LE GUIDE 2022-2023 CYBERSÉCURITÉ

FRENCH DIRECTORY

6e édition

Protection endpoint, Cloud, Supply-Chain : pour tout savoir



LES SOLUTIONS / LES SERVICES

700 ÉDITEURS, CONSEILS, PRESTATAIRES, DISTRIBUTEURS, FORMATEURS

En partenariat avec numeum

Hors-série Solutions numériques

Prix : 30 € - ISSN 2606-2860


kaspersky
25 ans
Plus efficace.
Déploiement simplifié.
Sécurité dans le cloud.
Kaspersky Optimum Security,
votre protection contre
les cybermenaces.
Dans le cloud.
Kaspersky
Optimum
Security
2022 AO KASPERSKY LAB

SOMMAIRE

Introduction

- **Editorial : Ransomwares : la bourse ou la vie !** 4
- **Tribunes**

ANSSI – Gestion de crise d'origine cyber : se préparer sereinement avant la tempête 7

Campus Cyber - Le défi du Campus Cyber pour renforcer la sécurité numérique de tous 8

Cybermalveillance.gouv.fr - Un Référentiel Formation Cybersécurité pour répondre aux besoins de compétences du marché 12

Clusif - Sécurité de l'information : Adapter les indicateurs pour mieux convaincre 14

Cesin - Numérique et sécurité : quel futur ? 16

Hexatrust - Pourquoi la France a besoin d'une nouvelle ambition numérique ? 18

Cigref - Sécurité numérique : les enjeux de la résilience 20

Numeum - Ensemble pour un numérique de confiance 22

AFCDP - Sanction de la CNIL à l'encontre d'ACCOR : Une décision riche d'enseignements pour les DPD/DPO 24

Les tendances de la cybersécurité

- Cybersécurité : on accélère 27
- A la pointe de l'innovation ! 30
- Protection endpoint : EDR et XDR redonnent l'avantage aux RSSI 32
- Le secteur cyber s'organise face à la crise des talents 34
- Peur sur la Supply Chain 38
- La cybersécurité bascule dans le Cloud 40
- Cybersécurité industrielle : vers une convergence IT/OT ? 42

Les acteurs de la Cybersécurité : Qui fait quoi ?

Editeurs, Conseils, Intégrateurs, formateurs etc. : présentation détaillée de 80 spécialistes incontournables 43

Fiches alphabétiques des entreprises spécialisées

- Fournisseurs de solutions 154
- Prestataires de services 168
- Consultants 180
- Formation 181
- Hébergeurs 182
- Avocats spécialisés 183
- Distributeurs 184

→

SOMMAIRE

Panorama : tableaux comparatifs

- Tableau des fournisseurs de Solutions 187
- Tableau des prestataires de services 201

Comprendre la technologie

Ramsomware, Zero Trust 214

BugBounty, Chiffrement post-quantique 215

Gestion du risque cyber, Red/Blue/Purple Team 216

Ingenierie sociale, SASE 217

Cyberassurance, Cybersécurité industrielle 218

Attaque par déni de service 219

Contrôle d'accès et gestion des identités 220

Threat Intelligence 222

DevSecOps, la transformation digitale des DSI 223

Protection du poste de travail 224

Protection des terminaux mobiles 225

Protection de la donnée 226

Protection applicative, Audit d'architecture 228

Soc 229

Tableaux de bord de sécurité, Siem 230

L'Ecosystème

Les organismes de référence : 232

ANSSI, AFCDP, CAMPUS CYBER, CESIN, CIGREF, CLUSIF, CNIL, CYBERMALVEILLANCE.GOUV.FR, HEXATRUST, NUMEUM

Hors Série de Solutions Numériques - Directeur de la publication & rédaction : Jean Kaminsky - Ont collaboré : Alain Clapaud, Jérôme Saiz (Conseiller de la rédaction) - redaction@solutions-numériques.com - Publicité tel. : 01 41 77 16 03 - publicité@solutions-numériques.com - Maquette : réalisation, Pierre Sandré - Siège social : K-Now SAS, 21 rue de Fécamp 75012 Paris - Impression : Mordacq, 62120 Aire-sur-la-Lys - Dépot légal à parution. Photo de couverture : ©Unsplash

L'éditeur ne peut être tenu responsable d'éventuelles erreurs ou omissions. Le reproduction partielle ou totale du contenu est interdite sauf autorisation expresse de l'éditeur.
Copyrigt : reproduction interdite

EDITORIAL

Ransomwares : « la bourse ou la vie ! »

Dans une guerre classique, les hôpitaux sont paralysés par l'afflux de blessés, dans une cyberguerre ils le sont par des ransomwares.

Le blocage informatique que subit depuis 5 semaines -le jour où j'écris ces lignes-, le centre hospitalier sud-francilien à Corbeil-Essonnes est le plus long feuilleton sans doute autour d'une prise d'otage. Un piratage opéré par des *« "criminels"…pour en rester là »,* indique d'un air entendu le ministre de la santé et médecin urgentiste, François Braun qui les qualifiera sur Europe 1 un autre jour de « cyber-terroristes ». Le détail est important : les maîtres chanteurs seraient-ils de simples braqueurs sans scrupule ou des mercenaires opérant pour un état ? Des pirates ou des corsaires ?

La question est, du reste, presque tranchée, quand on sait que les experts désignent comme auteur de l'attaque le trop fameux groupe criminel russophone Lockbit 3.0, auteur du cyber-piratage de près de 150 organisations, essentiellement européennes, sur les 3 premières semaines de septembre seulement. On peut donc soupçonner la Russie, sans en avoir la preuve.

« Il est hors de question de payer la rançon, la santé des français ne sera pas prise en otage » a déclaré, bravache, le ministre de la santé, aux côtés du ministre du numérique. C'est donc le gouvernement qui est à la manœuvre dans un bras de fer devenu affaire d'état, mais à l'issue incertaine… A ce jour, le montant de la rançon demandée -en échange de la clé de chiffrement et de la destruction des données volées - est divisé par 5 par rapport à la revendication initiale (2 millions au lieu de 10). Mais un échantillon d'une douzaine de gigaoctets de données personnelles sensibles a été mis en ligne dans le darkweb par les pirates, pour montrer leur pouvoir de nuisance.

Cependant, le bénéfice collatéral est l'augmentation de 20 millions du budget en cybersécurité du secteur de la santé, le portant à 45 millions.

Faut-il payer les cyber-rançons, et les assurances doivent-elles les indemniser ?

Un projet de loi présenté en Conseil des ministres autorise l'indemnisation, sous condition de déposer une plainte. Mais le débat fait rage.

Le Cesin (Club de Experts de Sécurité de l'Information et du Numérique) a sondé ses membres sur ces dispositions réglementaires, le résultat révèle que 82% des 249 répondants se positionnent contre. L'association explique : *« Cette annonce provoque de vives réactions dans la communauté des professionnels de la cybersécurité, et soulève de nombreuses questions, comme le risque d'encourager le cybercrime, les pressions que pourraient exercer les assureurs auprès de leurs clients pour payer la rançon si celle-ci s'avère moins élevée que les coûts de remédiation, les risques accrus de récidives pour l'entreprise quand celle-ci a été estampillée « bon payeur » par la communauté des cybercriminels (…). Quant aux réserves concernant les indemnisations sur les attaques lorsqu'elles sont d'origine étatique, elles ne sont simplement pas applicables tant les questions d'assignation sont complexes et les frontières floues.(…) Le CESIN est cependant bien conscient que certains dirigeants de PME-PMI, qui n'ont pas suffisamment anticipé le risque cyber, sont tentés de payer les rançons pour pouvoir récupérer l'accès à leurs données lorsque la pérennité de leur entreprise est en jeu. »*

La cybersécurité et la résilience deviennent en effet un impératif de survie pour les entreprises. Et au moins une garantie de santé économique. *« La cybersécurité est partie intégrante de la compétitivité de toute entreprise et de la confiance de ses clients »* nous expliquait Farid Illikoud, Ciso groupe de Décathlon. Après l'ère des directions commerciales et des Daf, le RSSI deviendrait-il le nouvel homme fort des organisations ?



Jean Kaminsky - *Directeur de la publication*



pradeo

PROTÉGEZ VOS
TERMINAUX

SÉCURITÉ **MOBILE**

PROTÉGEZ VOS
APPLICATIONS



Découvrez nos solutions sur
www.pradeo.com

FRANCE CYBER SECURITY

CYBERSECURITY™
MADE IN EUROPE

Tous droits réservés - Pradeo - 2022

LA 23

LES ASSISES

11.10.23 →→ 14.10.23 /MONACO///

Retrouvez les incontournables
et les pépites de la cyber !

→ lesassisesdelacybersecurite.com

DG CONSULTANTS

COMEXPOSIUM

Gestion de crise d'origine cyber
Se préparer sereinement avant la tempête



Par Yves Verhoeven, Sous-directeur Stratégie de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)

La transformation numérique s'est accompagnée d'une interconnexion croissante de l'ensemble des acteurs de la société, faisant ainsi évoluer le risque numérique du champ purement technique vers un risque de plus en plus prégnant pour l'activité des organisations. Ce nouveau paradigme oblige dorénavant les entreprises, les collectivités et les institutions à reconsidérer leur modèle de gestion des risques afin que le numérique soit intégré au même niveau que les préoccupations stratégiques, économiques et juridiques.

Face à des acteurs malveillants dont l'arsenal ne cesse de se perfectionner, les investissements, pourtant massifs, des entreprises dans la protection et la défense de leurs systèmes d'information et de leurs services numériques, demeurent insuffisants. A l'ANSSI, nous constatons que les attaques les plus sophistiquées ou ciblées qui touchent notamment les entreprises exploitent l'écosystème de la victime pour contourner les mécanismes de protection déployés. Le risque numérique devient ainsi systémique et non transférable, avec la nécessité absolue de se préparer à être un jour, à son tour victime, et de prévoir le dispositif permettant de se relever.

Impérative, la résilience d'une entreprise face à une crise d'origine cyber exige une bonne préparation à tous les niveaux, afin d'adopter, le moment venu, les bons réflexes et de maintenir l'activité. Source de stress, la crise d'origine cyber complique la prise de décision rapide, pourtant vitale pour en limiter les impacts. L'anticipation et la préparation des entreprises s'avèrent impérieuses. Afin d'appréhender pas à pas cette gestion et de faciliter la prise de décision, nous avons choisi d'élaborer une collection de guides de crise, complémentaires et destinés à chaque acteur, qui est également disponible en anglais :

- « *Crise d'origine cyber : les clés d'une gestion opérationnelle et stratégique* » - réalisé en partenariat avec le Club des directeurs de sécurité des entreprises (CDSE), ce guide fait le « pont » entre la gestion stratégique et opérationnelle avec le partage de recommandations grâce aux témoignages de bénéficiaires ayant subi une attaque.
- « *Anticiper et gérer sa communication de crise cyber* » - fruit d'un partenariat avec Cap'Com – ce guide démontre qu'une bonne communication de crise cyber reprend avant tout une stratégie de communication de crise, avec des conseils et recommandations prodigués très opérationnels.
- « *Organiser un exercice de gestion de crise cyber* », réalisé en partenariat avec le Club de la continuité d'activité (CCA), ce guide vise ainsi à accompagner les entreprises dans la mise en place d'un exercice vraisemblable et formateur, pour les joueurs comme pour les organisateurs avec un scénario « clé en main ».

La gestion de crise cyber doit devenir un véritable pilier de la stratégie de résilience des entreprises, qu'il soit question d'un grand groupe ou d'une TPE/PME. Lorsque la crise survient, les entreprises se retrouvent forcées de s'adapter et de fonctionner de manière inhabituelle face aux déséquilibres engendrés - vol de données, paralysie partielle ou totale des services numériques – et dont les impacts, souvent critiques, peuvent être opérationnels, juridiques, financiers et réputationnels.

L'objectif est donc de gagner en fluidité et d'adopter des automatismes qui permettront de réagir efficacement sur le temps long et de redonner confiance aux équipes ainsi qu'à l'écosystème (clients, partenaires, fournisseurs, régulateurs, etc.), qu'ils soient concernés ou non par les conséquences de l'incident. A cet égard, la communication de crise joue un rôle déterminant.

Seules les entreprises ayant une pleine maîtrise du risque numérique auront la capacité de se relever d'une crise d'origine cyber. Une bonne préparation permettra d'enrayer efficacement les cyberattaques et leurs conséquences ! ■

Rassembler les acteurs au-delà des concurrences économiques

Le défi du Campus Cyber pour renforcer la sécurité numérique de tous



Par Michel Van Den Berghe, Campus Cyber

Recherche, industriels, formation, startups, services de l'Etat, PME / ETI et associations sont autant d'acteurs qui forment le Campus Cyber. Ce dernier met en place des actions visant à fédérer la communauté de la cybersécurité et à y développer des synergies : il est la porte d'entrée de la cybersécurité en France et rassemble désormais plus de 240 acteurs nationaux et internationaux.

Si la transformation numérique est autant un remède qu'un poison selon Bernard Stiegler, le Campus Cyber est né du constat suivant : l'écosystème de la cybersécurité est fragmenté et insuffisamment préparé pour faire face à une menace multiforme et croissante. En 2022, pour la première fois, la cybersécurité a été classée dans le top 10 des risques business par le forum économique mondial.
En juillet 2019, le premier ministre m'a missionné afin de concevoir le lieu totem en matière de cybersécurité, inspiré de Beer-sheva. Trois ans plus tard, le Campus Cyber est une réalité, une tour de 26 000m² située à la Défense, rassemblant 1 800 experts au plus proche de l'écosystème.

Le Campus Cyber, une approche écosystème innovante

Représentant de l'écosystème, le Campus Cyber repose sur plusieurs spécificités. Nous avons eu à cœur d'assurer une forte collaboration privé-public : il n'est aujourd'hui plus possible de penser la cybersécurité sans embarquer l'ensemble des acteurs et leur complémentarité. De la même manière, nous avons fait le choix de distinguer l'apport en capital du pouvoir de décision afin que tous les acteurs soient présents dans les instances de gouvernance. Nous défendons ainsi un écosystème fertile et équilibré ! Enfin, la présence des bénéficiaires assure une cohérence et pertinence entre les besoins et les productions en matière de cybersécurité.



Former, innover et opérer : les enjeux de l'écosystème

Le Campus Cyber organise ses activités autour de trois piliers, qui correspondent aux défis de l'écosystème de la cybersécurité.



Espace de travail

Chiffres clefs

- **26 000m²** répartis au cœur de La Défense sur 13 étages
- **6 000m²** de plateaux projets et d'innovation
- **3 000m²** consacrés à la formation
- **4** espaces événementiels

- **167** Membres
- **40** Partenaires
- **120** Résidents

Sur les 6 premiers mois d'ouverture :
- **+2 300** experts on-boardés
- **+ 150** événements

Formation. La filière cybersécurité manque d'attractivité : 15 000 postes étaient à pourvoir en 2021 en France. Cette pénurie des talents met à risque le pays car elle correspond à une incapacité à répondre aux besoins du secteur bien que la menace augmente fortement. A peine 10% des professionnels actuels sont des femmes : c'est donc de la moitié du vivier des talents que nous nous privons ! Il est essentiel et urgent de travailler sur les imaginaires collectifs afin de casser les codes et de favoriser l'émergence de rôles modèles pour les jeunes et les moins jeunes. Le Campus Cyber a la capacité de jouer ce rôle de catalyseur : il rassemble des acteurs de la formation publics et privés, ce qui permet de déployer des initiatives ludiques, informatives, audiovisuelles tout en favorisant le partage de ressources.

Innovation. Les acteurs français et européens peinent encore à trouver suffisamment de fonds pour développer leurs solutions innovantes en matière de cybersécurité. En 2020, les Etats-Unis ont concentré plus de 75% des 7,8 milliards de dollars investis dans les sociétés cyber mondialement. Nous voulons que le Campus Cyber devienne le fer de lance de l'innovation en France : un startup studio accueille déjà 20 startups pré-incubées et il sera bientôt couplé à un incubateur/accélérateur. C'est donc toute la chaine de l'innovation qui est développée au Campus Cyber. La recherche est également au cœur des activités : de nombreux projets mêlant industriels et académiques vont être accueillis dans le cadre d'un programme de transfert de façon à assurer la corrélation des projets aux besoins réels du marché.

Opération. Au regard de l'augmentation des menaces, le Campus Cyber se donne comme objectif de fédérer les acteurs pour protéger efficacement les Français, notamment les PME et les collectivités qui sont les publics les plus exposés aux risques cyber. Plus de 80% des cyberattaques visent les PME ! Manquant de moyens financiers, de temps et de connaissance sur l'état réel de la menace, les PME sont davantage exposées aux attaques que les grands groupes. Pour anticiper et affronter cette massification des attaques, nous nous devons d'éduquer et sensibiliser les dirigeants et collaborateurs en les sensibilisant aux bonnes pratiques à adopter pour limiter les risques.

Fédérer les acteurs autour des communs de la cybersécurité : un pari réussi

Il y a deux ans, 60 acteurs se réunissaient pour co-designer les locaux du Campus Cyber. Aujourd'hui, plus de 500 experts participent à des groupes de travail afin de construire ensemble des communs de la cybersécurité utiles et accessibles à l'ensemble de la communauté.

Cette approche permet de résoudre des sujets complexes ne pouvant être résolus par un acteur unique lié aux niveaux d'investissement nécessaires ou à l'incertitude des débouchés marché. La participation de l'ANSSI a rendu les groupes de travail



très attractifs ! En un an, nous avons publié plusieurs livrables : une base de renseignement CTI, une matrice compétences / métiers, un livrable anticipation... et de nombreux autres sont à venir !

Le Campus Cyber organise des réflexions sectorielles, pour que les membres échangent sur des problématiques communes afin de renforcer leurs systèmes et mieux faire face à la menace. En effet, la cybersécurité concerne tous les secteurs économiques et transcende les concurrences existantes.

L'exemple le plus avancé est celui des banques et assurances : de leurs discussions préalables ont émergé trois sujets qui seront traités au sein de groupes réunissant des acteurs au-delà de cette communauté. De nombreux sujets seront lancés dans les prochains mois tels que le zero trust et le quantique. La forte participation à ces groupes de travail est révélatrice du changement de culture en cours au sein de l'écosystème : co-construire pour mieux protéger et mieux faire rayonner l'excellence française.

Enfin, un exercice de gestion de crise co-organisé avec l'ANSSI est en cours de préparation : plus de 110 organismes sont déjà inscrits et participeront en décembre à cet exercice grandeur nature au sein du Campus Cyber.

Développer un réseau, l'enjeu des mois à venir

Nous nous réjouissons du fort intérêt porté par toutes les régions au projet : il va permettre à un réseau de se développer, permettant de faire équipe afin de devenir un acteur de poids en France et en Europe.

Ce réseau visera à propager la culture et savoir-faire cyber sur l'ensemble du territoire, créer de la proximité et du dynamisme pour les écosystèmes régionaux, développer des liens et synergies sur les sujets de pointe.

Outre ce réseau français, de nombreuses initiatives devraient voir le jour en Europe et au-delà avec des acteurs de confiance. Le Campus Cyber a d'ores et déjà été sélectionné par la Commission Européenne comme EDIH (European digital innovation hub) pour les trois prochaines années afin d'offrir des services aux PME et des collectivités territoriales, premières victimes des attaques. A suivre ! ■

DOCAPOSTE

Vérification de l'identité à distance : un impératif dans les parcours digitaux

S'assurer de l'identité d'un utilisateur à distance est le fondement de tout service numérique. Mais avec quelle solution et quel niveau de garantie ? Le point avec Docaposte, acteur majeur de la confiance numérique en France.

Entrée en relation, signature électronique d'un contrat engageant, accès sécurisé à un service en ligne, parcours patient… L'explosion de la digitalisation des parcours clients et des échanges s'accompagne d'une augmentation des cas de fraudes numériques identitaires et documentaires. Pour faire face à ces nouvelles menaces, les réglementations sur la protection des données et des usagers, ainsi que sur les exigences en termes de sécurité, se durcissent. Devant cet état des lieux, les entreprises privées et publiques ont un intérêt majeur à mettre en place des solutions d'identification pour sécuriser leur activité et rassurer leurs clients et usagers. Si les professions fortement réglementées y étaient déjà confrontées, ce sont aujourd'hui tous les secteurs d'activité qui sont concernés par l'intégration de solutions d'identification fiables et capables de répondre aux exigences réglementaires. Face à l'inventivité des cybercriminels et au renforcement régulier de la législation, vos parcours digitaux doivent pouvoir intégrer les bons niveaux de sécurisation, sans pour autant alourdir les démarches pour les utilisateurs.

Pour répondre à ces enjeux, Docaposte, filiale numérique du Groupe La Poste, a créé ID360. Cette plateforme innovante propose, en une seule intégration et à partir d'une console d'administration, toutes les solutions de vérification d'identité à distance et tous les niveaux de sécurité existants.

Les forces d'ID360 : son exhaustivité, sa simplicité et son ouverture

Docaposte vous propose une plateforme unique, intégrant ses propres solutions d'identification comme L'Identité Numérique La Poste, des parcours en ligne automatiques ou hybrides, mais aussi des solutions tierces telles FranceConnect et FranceConnect+.

Tous les niveaux de sécurité sont ainsi accessibles. Solution évolutive, ID360 vous garantit la mise à jour des exigences réglementaires et l'ajout de toute nouvelle modalité d'identification pertinente. Au-delà des frontières de la France, ces solutions sécurisent aussi les échanges en Europe. Il est en effet possible d'identifier tout Européen grâce à son moyen d'identification électronique en cours dans son pays (*via* FranceConnect+). ID360 intègre également des solutions de renforcement d'authentification, de contrôle d'autres documents qu'identitaires, et traite les personnes agissant pour le compte de personnes morales.

Une seule intégration pour l'ensemble des solutions

Vous bénéficiez ainsi de la globalité des solutions à disposition sur ID360. **Une console d'administration simple et intuitive** vous permet de paramétrer et d'adapter le niveau de garantie de vos parcours en ligne selon les réglementations, les usages de vos clients et vos risques métier. Chaque identification ou authentification donne lieu à la génération d'un dossier de preuves archivé dix ans dans un coffre-fort à valeur probatoire. Parce que la confiance est importante aussi pour l'utilisateur final, **ID360 adopte les codes visuels de votre parcours : vos couleurs, votre logo**.

ID360, la référence de l'identification à distance

PROJET LABELLISÉ

ID360 vient d'obtenir sa conformité à la norme ETSI EN 319 401, fondement de tout service qualifié eIDAS, pour son haut niveau sécuritaire. Répondant aux enjeux clés des évolutions de l'économie digitale, ID360 de Docaposte a reçu le label **« Finance Innovation 2022 »**. Une reconnaissance du caractère novateur et stratégique de la solution de la part des acteurs de l'écosystème bancaire et financier.

Pour en savoir plus sur la solution ID360, rendez-vous sur **docaposte.com/solutions/id360**

Un Référentiel Formation Cybersécurité pour répondre aux besoins de compétences du marché



Par Jérôme NOTIN,
Directeur Général
Cybermalveillance.gouv.fr,

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

Cybermalveillance.gouv.fr, est le dispositif national d'assistance aux victimes d'actes de cybermalveillance, de sensibilisation des publics aux risques numériques et d'observation de la menace en France. Ses publics sont les particuliers, les entreprises et les collectivités territoriales.

Le travail en flux tendu dans l'IT n'est hélas ni une vue de l'esprit ni un nouveau concept. C'est un constat inéluctable qui existait bien avant la pandémie et qui s'est renforcé depuis son apparition il y a 2 ans.
En effet, en réponse à la crise que nous avons traversée, les organisations se sont davantage numérisées. Celles qui étaient peu présentes sur Internet ont considérablement développé leur visibilité, avec en parallèle une augmentation de l'utilisation des outils numériques en interne, pour par exemple permettre le télétravail. N'oublions pas qu'auparavant, à peine plus d'une PME sur 3 disposait d'une « vitrine » sur le web*, quant aux autres, elles ont vite saisi l'urgence à s'imposer sur Internet, levier de croissance indéniable.

Oui mais, au-delà de ces effets vertueux, la crise a aussi eu d'autres conséquences … Si les TPE-PME se sont numérisées à grands renforts de sites web, de nouvelles applications, de nouveaux services, de serveurs dans le Cloud et autres postes de travail en dehors du périmètre d'origine, cette transformation n'a pas été systématiquement accompagnée par la mise en œuvre de moyens en termes de cybersécurité. Et c'est bien-là le paradoxe.

Autrement dit, cette nouvelle exposition, du reste indispensable pour garantir leur compétitivité, voire leur activité économique, les a rendues encore plus vulnérables face à la menace.
Menace qui entre temps, n'a fait que croître, se sophistiquer et se professionnaliser…
Témoins les derniers chiffres de notre plateforme Cybermalveillance.gouv.fr qui affichait, fin 2021, + 143% de hausse pour l'hameçonnage, première menace, tous publics confondus et 95% pour les rançongiciels, sur les professionnels.

Alors comment faire pour combattre un tel fléau ? Toutes les entreprises ne sont pas préparées de la même façon pour faire face à une cyberattaque. Peu d'entreprises disposent d'une politique de cybersécurité et lorsqu'elles en ont une, la cybersécurité est encore trop souvent perçue comme une contrainte.

Et la plupart d'entre elles ne savent absolument pas par quel bout prendre le sujet et encore moins à qui s'adresser.

Or, en matière de cyber comme ailleurs, l'essentiel est bien d'apporter clarté et transparence aux organisations qui en ont besoin sur la qualité de l'offre de services proposée, en termes d'assistance mais aussi de prévention. Par ailleurs, si le marché de la prestation informatique s'est considérablement développé ces dernières années, il n'en reste pas moins extrêmement hétérogène, tout autant que le niveau de compétences.
La protection informatique et la sécurité des données est sans aucun doute l'un des principaux

défis que ces prestataires spécialisés se doivent de savoir relever pour répondre aux besoins de leurs clients.

ExpertCyber : Un label pour reconnaître l'expertise

C'est précisément dans ce cadre que Cybermalveillance.gouv.fr a créé début 2021 le label ExpertCyber en collaboration avec Cinov Numérique, la fédération EBEN, NUMEUM, France Assureurs et l'AFNOR.
L'objectif ? Reconnaître l'expertise en sécurité numérique d'un prestataire informatique dans 3 domaines : la sécurisation, la maintenance et l'assistance.
Ce label est non seulement un gage de sérieux mais aussi de confiance pour l'entreprise cliente. Il constitue une vraie valeur ajoutée pour le labellisé, dont l'expertise en cybersécurité est démontrée.
20 mois après son lancement, Cybermalveillance .gouv.fr compte plus de 200 prestataires labellisés répartis sur l'ensemble du territoire national.
C'est une première étape. Il nous faut aujourd'hui aller encore plus loin, et compléter ce maillage territorial en accompagnant la montée en compétences des prestataires qui ne disposent pas encore du bon niveau d'expertise en cybersécurité.

Un Référentiel Cyber pour former le plus grand nombre

Afin d'augmenter le nombre de prestataires disposant de fortes compétences en cybersécurité, nous avons décidé de créer un Référentiel Formation. Les organismes de formation pourront ainsi, sur la base de ce référentiel, créer des formations capables d'offrir au plus grand nombre un socle d'apprentissage en cybersécurité commun pour les prestataires.
Nous en sommes convaincus, les prestataires de proximité constituent aujourd'hui le relai de confiance des TPE-PME, collectivités et associations. Il est donc de notre responsabilité de nous assurer qu'un maximum de professionnels seront demain en mesure de les accompagner face à une menace croissante,
Après la création du label ExpertCyber, le Référentiel est la deuxième étape de notre démarche développée en partenariat avec l'AFNOR, le centre de formation de l'ANSSI (CFSSI) et la Région Nouvelle-Aquitaine, qui s'intègre parfaitement dans notre mission d'intérêt public.
Une mission, qui, ne nous y trompons pas, commence avant tout par la sensibilisation des collaborateurs au sein des différentes structures, parce que l'humain reste au coeur du dispositif de lutte contre la cybermalveillance.
En 2022, plus que jamais, la cybersécurité est l'affaire de tous.

---

* Source France Num
https://www.francenum.gouv.fr/guides-et-conseils/strategie-numerique/barometre-france-num-2021-le-numerique-dans-les-tpe-pme-0



Sécurité de l'information
Adapter les indicateurs pour mieux convaincre



Benoît Fuzeau
Président du Clusif

Le panorama de la cybercriminalité du Clusif l'a encore montré cette année : la menace cybercriminelle est en expansion et ne compte pas disparaître. C'est désormais un véritable écosystème qui met la survie même des organisations privées et publiques en péril.

Nous avons tous à l'esprit les attaques récentes sur les hôpitaux, par exemple. Or toutes les victimes potentielles des cybercriminels n'ont pas nécessairement accès à l'information suffisante pour se prémunir de ces attaques.
C'est dans ce contexte de risque accru et d'incertitude qu'une loi portant sur la création d'une certification en cybersécurité a vu le jour. Cette loi veut répondre au besoin d'une meilleure lisibilité des outils numériques en mettant en place un audit sous la forme d'un « système d'information coloriel », soit une sorte de déclinaison du désormais bien connu « nutriscore » appliqué à la cybersécurité.

Les avantages et les risques du "cyberscore"

Beaucoup de spéculations ont entouré l'élaboration du texte depuis son dépôt en 2020, pointant les avantages et également les risques que représentent une notation du type du « cyberscore ». Quelle sera la durée de validité de l'audit ? Dans quelles conditions et selon quelles modalités sera-t-il réalisé ? Devrait-il être renouvelé à chaque évolution technologique de la plateforme ? Quid de la localisation des données hébergées par l'application ? En définitive, cette loi, adoptée le 3 mars 2022, laisse à ce jour un certain nombre de questions sans réponse.
Mais pour nous, professionnels de la cybersécurité, ce concept reste porteur et j'ai la conviction que nous pouvons utilement nous saisir des principes de cet outil.

Le Clusif s'attache à voir le côté opérationnel du cyberscore en tant que véritable levier de sensibilisation potentiel.

Parce que notre culture entrepreneuriale est celle-ci, nous produisons des indicateurs quantitatifs très techniques. Le besoin de rationaliser nos messages mais aussi de faire entendre les enjeux cyber nous poussent à une technicité du discours telle que nous avons du mal à nous faire comprendre et entendre, notamment des dirigeants. Or qu'attendent-ils vraiment de nous ? Selon mon expérience, ils ont davantage besoin d'un éclairage sur le risque que d'un indicateur qui fixe un nombre de vulnérabilités restant à corriger. Nous devons aider à la prise de décision, mais comment faire ?
C'est dans cette perspective que le cyberscore est une idée à saisir et c'est ce que je travaille à mettre en place en tant que RSSI. Tout le monde est sensibilisé par le nutriscore. Il est simple, voire naturel d'appréhender le risque de cette façon pour les utilisateurs comme pour nos dirigeants. Mais au-delà du visuel, reste à définir comment le construire et quelles sont les données à prendre en compte pour le calculer. Mes équipes et moi-même avons opté pour une vision applicative mais d'autres options tactiques sont possibles. Ce qui est important est de fournir des règles de calcul transparentes en interne et d'utiliser des données simples à collecter par l'équipe SSI.
Rendre compte du risque cyber de manière plus lisible, c'est l'objectif de départ du cyberscore. Mais cela doit nous interpeller sur la nécessité d'innover en matière de sensibilisation et de savoir tirer parti des outils innovants quand ils se présentent. ■

blue. cyber

La sécurité de vos données au cœur de nos châteaux forts.



- Réseau privé SD-WAN managé
- Accès sécurisé (MFA) Bastion
- Cloud privé / hybride Backup & snapshot
- SOC : SIEM & SOAR Pentest

Certifications

ISO 27001 Certified

ITIL FOUNDATION

vmware CLOUD VERIFIED

bt-blue.com

Services proposés par blue.

Numérique et sécurité : quel futur ?



Alain Bouillé,
Délégué Général du CESIN

Pas encore sortis de la crise sanitaire qui nous a apporté de nouvelles organisations du travail où beaucoup de salariés aspirent désormais à davantage de liberté sur le lieu où exercer leurs missions, nous voici plongés dans une guerre en Europe inimaginable il y a encore quelques mois. Les catastrophes climatiques de l'été sont venues rajouter une nouvelle couche à ces crises qui n'en finissent pas !

Au moment de la crise sanitaire, on s'est soudain rendu compte combien nous étions dépendants de puissances étrangères comme la Chine où lorsque l'usine du monde s'est arrêtée de tourner, on s'est brutalement aperçu qu'il y avait plein de choses que l'on ne fabriquait plus près de chez nous ! Le conflit en Ukraine, au-delà des horreurs qu'il engendre, souligne notre extrême dépendance en particulier énergétique aux pays en guerre et enfin les crises climatiques nous rappellent également notre dépendance à certains produits affectés par le réchauffement climatique. N'a-t-on pas découvert de manière quasi anecdotique que la majorité des graines destinées à fabriquer la fameuse moutarde de Dijon n'est plus cultivée à Dijon mais au Canada ? Et lorsque la production est affectée par la sécheresse qui a sévit dans ce pays et que le plan B qui consiste à se fournir en Ukraine n'est plus d'actualité, on ne trouve plus de moutarde dans les magasins !

Nous sommes une colonie numérique des Etats-Unis

Cette dépendance est depuis longtemps de mise dans le monde numérique. Nous savons depuis longtemps que nous sommes une colonie numérique des Etats-Unis avant peut-être que la Chine ne prenne le lead en ce domaine. Si beaucoup d'entreprises sont restées insensibles aux questions de souveraineté depuis le « move to cloud », le resteront-elles encore longtemps face à la dépendance qu'elle engendre ?

Pendant ce temps le numérique voit son empreinte environnementale gonfler chaque année. Si le numérique était un pays, celui-ci aurait une empreinte carbone équivalente à 2 à 3 fois celle de la France (source EDF). L'ADEME, l'Agence de la transition écologique, rappelle que le secteur est responsable d'environ 4 % des émissions mondiales de gaz à effet de serre et d'ici 2025, cette part est prévue de doubler.

Et plutôt que de mettre le paquet sur la sobriété numérique, au lieu des mesurettes annoncées pour faire bonne figure, de quoi nous parle-t-on en 2022 ? De Metaverse, de NFT, de blockchain, tous plus consommateurs d'énergie les uns que les autres ! Sans parler des appareils électroniques possédés par les ménages et des objets connectés que l'on comptabilise par milliards (19 en 2020, 48 en 2025 !).

Si tout cela est une véritable catastrophe pour la planète, en matière de cybersécurité cette gabegie numérique représente une véritable calamité avec des surfaces d'attaque qui ne cessent d'augmenter de manière exponentielle. Comment alors s'étonner que les dépenses sécurité augmentent en flèche pour le plus grand bonheur de l'industrie cybersécurité ?

Face à ce constat, il n'est plus possible de faire de la cybersécurité « à la papa » avec les approches du 20ème siècle. Un des premiers commandements de l'ANSSI est de connaitre ses assets afin de mieux en maitriser ses vulnérabilités. Qui connait aujourd'hui l'étendue de son patrimoine lorsque

qu'il se crée des applications et des sites par dizaines chaque jour sur le cloud pour chaque entreprise ?

1000 nouveaux avis de sécurité à mi-2022

En matière de gestion des vulnérabilités, le CERT IST, avec lequel le CESIN est partenaire, publie des avis de sécurité qui regroupent plusieurs CVE (Common Vulnerabilities and Exposures). On en était à 1000 en 2014, nous en sommes pratiquement à 2000 en 2021 et on en est déjà à plus de 1000 à mi-année 2022. D'après le NIST (National Institute of Standards and Technology), on plafonnait à 6000 CVE jusqu'en 2016, on en est à plus de 20 000 en 2021 et pour 2022 on atteint les 18 000 à mi-année. Cette situation où le seul remède est d'automatiser le gestion de la médiocrité logicielle, n'est plus supportable pour les entreprises. Puisque les bonnes pratiques ne sont pas suffisantes en la matière, il faut légiférer. Le Cyber Resilience Act ira-t-il jusque-là ?

> *« Qui connait aujourd'hui l'étendue de son patrimoine lorsque qu'il se crée des applications et des sites par dizaines chaque jour sur le cloud pour chaque entreprise ? »*

En matière de gestion des identités et des accès, tout a été bouleversé depuis les premiers projets des années 2000 consistant à rassembler les accès des utilisateurs d'une entreprise au sein d'un même outil destiné à mieux gérer les accès aux applications mais surtout de savoir à tout moment qui accède à quoi, information précieuse lorsque l'utilisateur quitte l'entreprise surtout de façon précipitée.

Aujourd'hui ce sont les accès à des centaines d'applications en mode SaaS qu'il faut rassembler avec des outils de nouvelle génération. A cela s'ajoute le problème quasi insoluble des accédants sous-traitants à qui on donne souvent « les clés du camion » avec des turnovers souvent inconnus du client !

La promesse d'une meilleure sécurité une fois la migration dans le cloud réalisée n'a pas été tenue

Près de 9 entreprises sur 10 estiment que sécuriser des données dans le cloud nécessite des outils spécifiques autres que ceux proposés par le Cloud Provider selon le dernier baromètre du CESIN. Cela souligne que la promesse d'une meilleure sécurité, une fois la migration dans le cloud réalisée, n'a pas été tenue. La sécurité du cloud et surtout du multicloud est devenue un vrai casse-tête pour les RSSI et n'est pas près de s'arranger au rythme des migrations en cours.

Et comme si tout cela, qui ne représente qu'une faible part des défis auxquels est confronté le RSSI , ne suffisait pas, la cyber-assurance refait parler d'elle avec la position du Trésor au sujet du paiement des rançons. Au final, avec des primes de plus en plus élevées, des couvertures amoindries et des exigences de la part des assureurs de plus en plus élevées, on peut se poser la question de l'intérêt de se cyber-assurer lorsque l'on est une grande entreprise alors que pour les ETI et le PME, une cyber assurance est la plupart du temps salutaire. Il faudrait que le marché s'inverse.

Une nouvelle gouvernance est nécessaire

Tous ces sujets doivent interroger les directions générales sur la meilleure manière de piloter un programme cyber. Une nouvelle gouvernance est nécessaire et le CESIN reste convaincu que cette mission est beaucoup trop sérieuse pour être confiée à un généraliste. Un sachant de haut niveau capable d'appréhender tous ces défis avec une parfaite maitrise des enjeux et des risques est indispensable. Ce sont des thèmes sur lesquels le Club va travailler dans le futur, à commencer lors de son Congrès annuel en décembre prochain. ■

L'actu, les dossiers de la
CYBERSÉCURITÉ
www.solutions-numériques.com/securite
Abonnez-vous à la Newsletter *du lundi*

Pourquoi la France a besoin d'une nouvelle ambition numérique ?

Jean-Noël de GALZAIN, Président d'HEXATRUST



HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

En France, on n'a pas de pétrole mais on a des idées. Si la France repense désormais sa politique énergétique dans un contexte géopolitique instable, force est de constater qu'elle possède l'or noir du XXIème siècle : des données !

Il ne s'agit pas simplement d'un enjeu technologique mais sociétal. Le CSF Industries de Sécurité a d'ailleurs rappelé dans un courrier adressé aux intégrateurs que le risque cyber est considéré comme le 1er de tous les risques par les chefs d'entreprise. Les crises qui se suivent soulignent nos dépendances critiques et la nécessité de renforcer notre autonomie par la souveraineté. La cybersécurité n'est plus seulement une question d'experts autour de sujets de sécurité. C'est une filière qui s'intègre dorénavant dans l'éducation, l'enseignement, la recherche, l'emploi, l'économie, le fonctionnement de nos villes, notre mobilité, notre santé et nos rouages démocratiques.

Emmanuel Macron a annoncé en février 2021, une stratégie nationale de cybersécurité française ambitieuse de plus d'un milliard d'euros. L'objectif pour 2025, c'est le triplement du chiffre d'affaires de la filière, soit 25 milliards €, le doublement des emplois soit 75 000 personnes, et faire émerger 3 licornes. Dans ce contexte, la filière s'est mobilisée en Équipe de France pour transcender les défis et se mettre dans l'état d'esprit de la gagne !

Pouvoirs publics, utilisateurs, industriels, PME, ETI, start-ups, décideurs, tous ensemble, nous devons nous mobiliser autour d'une nouvelle ambition numérique pour faire de la France la terre européenne du numérique et de la cybersécurité, résiliente et indépendante de ses choix.

Cette ambition se structure autour de mesures très concrètes pour les utilisateurs et pour notre société toute entière : un catalogue de solutions souveraines, le levier de la commande publique, la mise en place de la cyber assurance pour les PME et les ETI, la mobilisation de financements pour accompagner l'équipement de nos organisations et entreprises les plus fragiles, la création d'un European tech Business Act et d'un Small Business Act pour servir de tremplin à notre industrie au service de notre transformation numérique. Ce sont les bases d'une politique industrielle stratégique au service de la souveraineté numérique.

Pour mener à bien cette ambition, il nous faut démontrer une qualité technologique compétitive vis-à-vis de nos alliés et compétiteurs internationaux. Cette compétence, nous l'avons, ainsi que l'excellence de nos talents reconnue dans le monde entier.

Nous sommes donc dans le « momentum », avec une équipe de France rassemblée autour de son Capitaine Jean-Noël Barrot, le nouveau Ministre de la transformation numérique. Et comme le disait Victor Hugo *« Il n'est rien au monde d'aussi puissant qu'une idée dont l'heure est venue ».*

Le succès de notre filière sera collectif ou ne sera pas. L'écosystème en est la clé. Hexatrust continuera par conséquent à s'investir dans l'émergence d'une filière Cyber France d'excellence, au service des utilisateurs à la recherche de solutions souveraines et de services de confiance pour bâtir un futur numérique souhaitable.

OUTSCALE Cloud Santé

Le plus haut niveau de sécurité pour vos données de santé

Certifié Hébergeur
de **Données de Santé**

fr.outscale.com/hds-cloud-sante/





OUTSCALE × NetApp

Sécurité numérique : les enjeux de la résilience



Par Jean-Claude LAROCHE,
DSI du groupe Enedis
Vice-président du Cigref

Cigref
RÉUSSIR LE NUMÉRIQUE

Dans le contexte actuel de forte croissance de la menace, il apparaît indispensable de changer les paradigmes de la sécurité dans l'espace numérique. Il est en effet illusoire de penser que les instruments juridiques et technologiques actuels, mis en œuvre pour assurer la protection des produits et des services numériques, des systèmes d'informations, des infrastructures numériques, permettront de juguler la cybercriminalité.

Le Cigref propose depuis plusieurs années de rénover en profondeur cette approche collective que nous devons avoir de la sécurité dans l'espace numérique, ce qui impose une action vigoureuse à tous les niveaux, y compris celui des Etats et de l'Union européenne. Nous appelons à développer des politiques publiques cohérentes entre elles et ambitieuses, en les articulant autour de quatre axes principaux susceptibles de constituer les fondements d'une stratégie nationale et européenne de sécurité numérique.

Le premier axe concerne les technologies de cybersécurité qu'il est nécessaire de continuer à développer. Ces technologies permettent de renforcer la sécurité des systèmes d'information et des infrastructures numériques qui les portent. Entre 2017 et 2021, les grandes organisations, publiques et privées, membres du Cigref, en fonction de leur secteur d'activité, de la criticité de leurs infrastructures numériques, de la sensibilité des données qu'elles manipulent, de leur statut d'opérateur d'importance vitale ou de service essentiel, ont toutes augmenté de manière plus ou moins drastique les budgets consacrés à l'acquisition de ces technologies, à leur intégration et à leur mise en œuvre. Le 18 février 2021, le Président de la République présentait un plan ambitieux d'accélération pour la cybersécurité. Ce plan mobilise des financements importants, d'un montant d'un milliard d'euros, pour identifier et réduire les vulnérabilités des systèmes d'information et des infrastructures numériques de nombreux organismes publics et privés, notamment les hôpitaux publics qui paient un lourd tribut à la hausse de la cybercriminalité. Pour autant, une stratégie nationale pour la sécurité dans l'espace numérique ne peut se limiter à un tel plan, aussi nécessaire soit-il.

Le deuxième axe d'une telle stratégie de sécurité numérique concerne l'adaptation des moyens de police et de justice à la situation de dégradation constante de la sécurité dans l'espace numérique. Dans un avis publié le 29 avril 2021, la Commission supérieure du numérique et des postes, organe parlementaire bicaméral, publiait un avis qui pointait une véritable carence de l'Etat dans les moyens dédiés à la lutte contre la cybercriminalité. Cette commission pointait le décalage croissant entre la réalité de la criminalité dans l'espace numérique et les moyens dont dispose l'institution judiciaire et les forces de police pour traiter cette cyber-délinquance mon-

dialisée et industrialisée. Cette commission recommande notamment la création d'un parquet national cyber, disposant des ressources et des expertises suffisantes pour instruire les dossiers liés aux affaires de cyber-délinquance les plus complexes, et un renforcement significatif des moyens des services d'enquête pour lutter contre la cyber-délinquance internationale, en développant les capacités de coopération judiciaire européenne.

Le troisième axe concerne les capacités spécialisées, éminemment régaliennes, en matière de cyber-défense dans la profondeur. Ces capacités sont indispensables pour identifier et neutraliser les cyberattaquants situés dans des zones géographiques dans lesquelles ils ne peuvent être appréhendés par les moyens conventionnels de la police et de la justice. Plusieurs services de l'Etat peuvent contribuer significativement à cette mission. Il est cependant essentiel de maintenir et de renforcer dans la durée leurs compétences et leurs moyens.

Enfin, quatrième axe de cette stratégie globale de sécurité numérique, et c'est sans doute le plus complexe. Il apparaît désormais indispensable d'effacer une singularité de l'industrie du numérique sur le marché européen. Cette industrie est probablement la seule en Europe à n'être soumise à aucune norme de sécurité contraignante ni à aucune règle prudentielle pour la fabrication et l'exploitation de ses produits et de ses services. Il est inadmissible que cette industrie, quand bien même ce serait le fruit de son histoire, continue à opérer sur le marché européen sans que la responsabilité de ses acteurs puisse être engagée sur la base de telles normes de sécurité ou de règles prudentielles spécifiques. C'est dans cette logique que la Commission européenne a lancé une initiative législative, le 16 mars 2022, en proposant un futur règlement, le Cyber Resilience Act. Pour répondre aux besoins du marché européen et protéger les utilisateurs, professionnels comme particuliers, contre les produits et services non sécurisés, cette initiative visera à fixer des exigences de cybersécurité auxquelles les fabricants et les vendeurs de ces produits et services devront se conformer. La Commission devrait en principe publier son projet de règlement le 13 septembre 2022. Chacun des acteurs de l'écosystème numérique sera appelé à le commenter et à proposer des améliorations en vue de son examen par le Parlement européen et le Conseil. Ce travail est essentiel pour qu'il réponde aux préoccupations du plus grand nombre et pour ne pas laisser l'initiative aux seuls géants technologiques dont l'intérêt sera, sans nul doute, d'en restreindre la portée. Pour autant, ne nous faisons pas d'illusion, la marche à gravir est très élevée. Ce processus prendra probablement de nombreuses années, sans doute une dizaine, et les forces qui s'y opposeront seront virulentes. ■

> *« Le futur règlement, le Cyber Resilience Act, visera à fixer des exigences de cybersécurité auxquelles l'industrie du numérique, fabricants et vendeurs de produits et services devront se conformer. »*



Retrouvez le guide Cybersécurité en ligne

- Téléchargez le guide au format e-book et PDF
- Consultez les fiches des entreprises sur l'annuaire de la sécurité

Ensemble, pour un numerique de confiance



Etienne de Séréville, IBM,
pour la Commission Cybersécurité de numeum

Dans un contexte géopolitique où les tensions internationales sont très fortes, les actions dans le cyberespace se sont multipliées ces derniers mois, à destination des intérêts des États et aussi des entreprises.

Les attaques et les incidents se sont multipliés, tant pour les acteurs directs des conflits que pour les protagonistes alliés et leurs entreprises emblématiques, comme l'arrêt d'un réseau satellite privant des européens de service Internet, ou les attaques par ransomware sur des installations énergétiques : électrique en Ukraine, éolienne en Allemagne, gazière en Roumanie. L'extension hors des frontières des conflits hybrides rend plus que jamais d'actualité le thème de cette année « *façonner l'avenir numérique de l'Europe* » du Forum International de la Cybersécurité, comme le sont les évolutions réglementaires NIS 2 et DORA, pour la confiance numérique.

Nos convictions chez Numeum rejoignent cette volonté de travailler ensemble : la coopération et la collaboration doivent permettre d'accroitre la cybersécurité pour mieux répondre aux enjeux, offrir des services et des solutions toujours plus efficaces aux entreprises et services de l'État. Numeum est organisé en commissions qui permettent aux professionnels des entreprises de services du numérique, aux éditeurs de logiciels, aux plateformes, ainsi qu'aux sociétés d'ingénierie et de conseil en technologies, d'échanger et de construire des écosystèmes à même de répondre aux besoins de cybersécurité. Ainsi, en plus de du renforcement légal et réglementaire, cette volonté de travailler ensemble est un levier supplémentaire pour améliorer la défense de nos entreprises individuellement et collectivement, comme en témoigne la présence de Numeum comme membre associé du Campus Cyber.

> ***« La coopération et la collaboration doivent permettre d'accroitre la cybersécurité. »***

La commission Cybersécurité de Numeum a pour objectif de :

- favoriser les échanges entre ses membres et l'écosystème de la cybersécurité,
- faire connaître les solutions et les services de sécurité de nos membres,
- contribuer à rendre attractive la filière pour attirer les talents vers nos métiers,
- informer et sensibiliser les utilisateurs du numérique des risques potentiels pour contribuer à la confiance numérique.

Nos échanges entre professionnels traitent des sujets d'intérêt cyber, tant techniques que réglementaires ou normatifs, d'innovation et d'industrialisation des technologies, ainsi que de formation vers l'école et l'enseignement supérieur.

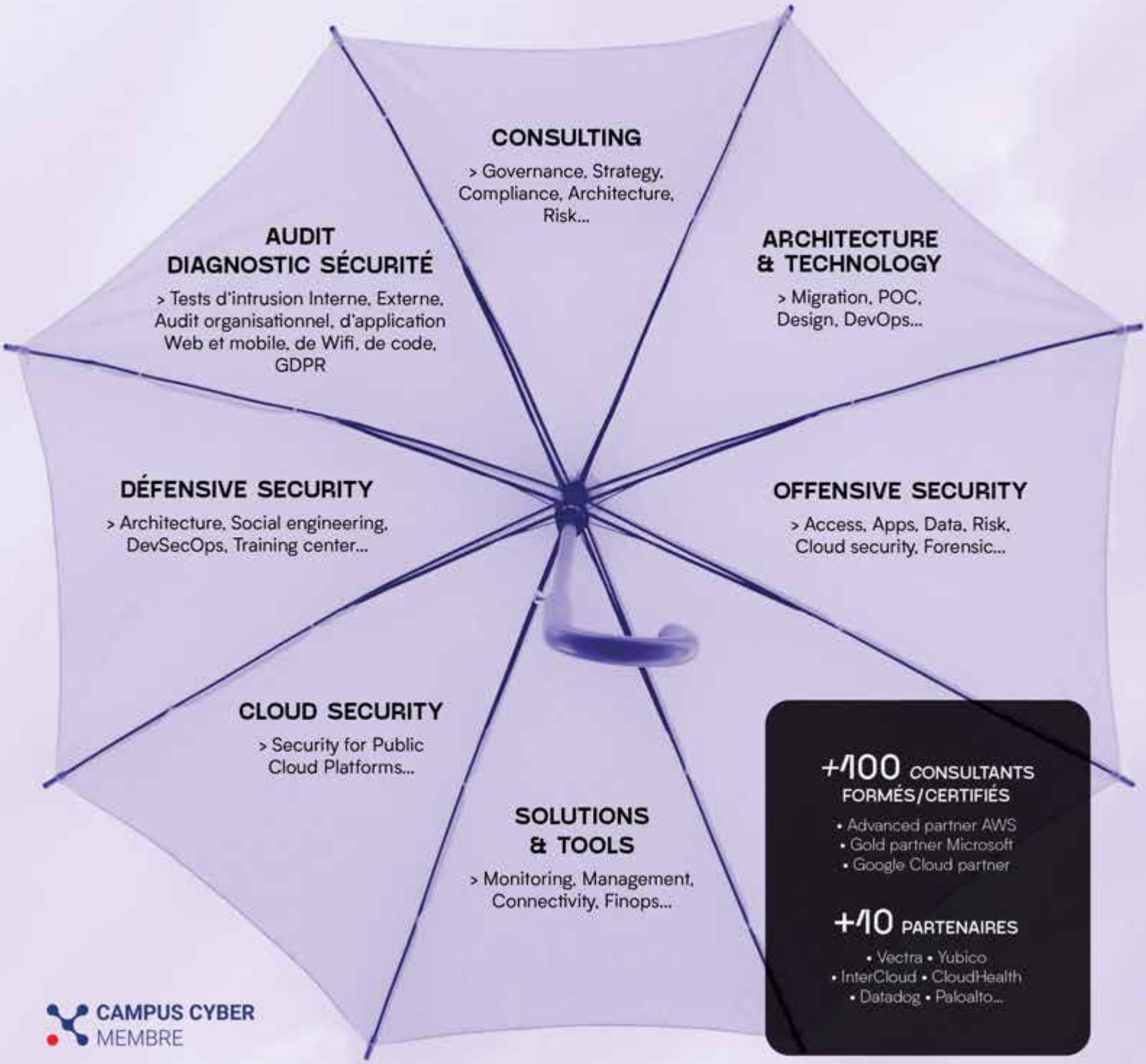
D'autre part, nous participons au rayonnement de la plateforme cybermalveillance.gouv.fr, sommes partenaire du mois européen de la cybersécurité piloté par l'ANSSI et nous formulons des propositions en matière de cybersécurité auprès des pouvoirs publics.

Toutes ces activités sur la cybersécurité au profit de la filière numérique française sont mues par des valeurs partagées : ensemble pour un numérique de confiance au service des hommes et des innovations au service de la société.

GO CLOUD & SECURITY

by Micropole

Nous vous accompagnons dans votre migration vers le Cloud et dans la sécurisation défensive et offensive globale de votre système d'information.



CONSULTING

> Governance, Strategy, Compliance, Architecture, Risk...

AUDIT DIAGNOSTIC SÉCURITÉ

> Tests d'intrusion Interne, Externe, Audit organisationnel, d'application Web et mobile, de Wifi, de code, GDPR

ARCHITECTURE & TECHNOLOGY

> Migration, POC, Design, DevOps...

DÉFENSIVE SECURITY

> Architecture, Social engineering, DevSecOps, Training center...

OFFENSIVE SECURITY

> Access, Apps, Data, Risk, Cloud security, Forensic...

CLOUD SECURITY

> Security for Public Cloud Platforms...

SOLUTIONS & TOOLS

> Monitoring, Management, Connectivity, Finops...

+100 CONSULTANTS FORMÉS/CERTIFIÉS

- Advanced partner AWS
- Gold partner Microsoft
- Google Cloud partner

+10 PARTENAIRES

• Vectra • Yubico
• InterCloud • CloudHealth
• Datadog • Paloalto...

CAMPUS CYBER
MEMBRE

Contact :
Christophe Levier - contactgcs@micropole.com - micropole.com - 01 74 18 74 18

MICROPOLE

Cabinet de conseil spécialisé dans la transformation des entreprises par la Data

Sanction de la CNIL à l'encontre d'ACCOR : une décision riche d'enseignements pour les Délégués à la protection des données



Patrick Blum,
Délégué Général, AFCDP

La sanction prononcée par la CNIL à l'encontre d'Accor cet été (1) a pu surprendre par sa sévérité. Elle s'explique d'abord par un certain nombre de manquements relevés par la Commission, mais aussi par l'impact du mécanisme d'harmonisation européen, déclenché pour les affaires impliquant plusieurs pays, et doit attirer l'attention des délégués à la protection des données (DPD/DPO).

Des manquements cumulés

Saisie de plusieurs plaintes en France et en provenance d'autres pays européens, la CNIL, agissant comme autorité « Cheffe de file » en raison de la localisation dans l'Hexagone du siège d'Accor, a enclenché une procédure de contrôle.

Cette procédure a conduit la CNIL à relever plusieurs manquements au RGPD et à la législation française, portant sur :

- l'absence de recueil du consentement pour traiter des données à des fins de prospection commerciale (article L. 34-5 du Code des postes et des communications électroniques) : lors de la réservation d'une chambre d'hôtel, l'internaute était automatiquement abonné à la newsletter, la case de consentement étant précochée par défaut. De même, la création d'un espace client conduisait à l'envoi automatique de prospection commerciale.

- l'absence d'information des personnes à la création d'un compte client ou lors de l'adhésion au programme de fidélité : le formulaire permettant la création d'un compte client ou l'adhésion au programme de fidélité ne comportait pas les informations exigées par les articles 12 et 13 du RGPD.

- l'absence de mention du consentement comme base légale du traitement, pour la promotion de produits ou services de tiers ;

- des insuffisances sur le respect du droit d'accès des personnes aux données les concernant (art. 12 et 15 du RGPD) : la CNIL a observé que dans un cas, isolé, l'entreprise n'avait pas procédé dans les délais impartis à la satisfaction de la demande.

- des insuffisances sur le respect du droit d'opposition des personnes ne souhaitant plus recevoir de message de prospection commerciale (art. 12 et 21 du RGPD) : la CNIL a observé des dysfonctionnements dans les liens de désinscription et dans la synchronisation des fichiers, susceptibles d'avoir empêché de nombreuses personnes de s'opposer à la réception des messages de prospection, ceci concernant potentiellement plusieurs millions de personnes.

> ***« Le mécanisme de coopération et d'harmonisation européen a pour conséquence de rehausser les montants des sanctions décidées par la CNIL »***

- une sécurité insuffisante des données personnelles (art. 32 du RGPD) : la CNIL a relevé plusieurs anomalies comme l'insuffisance de certains mots de passe opérationnels. Mais elle a également observé qu'en cas de suspension d'un compte pour suspicion de connexion frauduleuse, le client devait envoyer par courriel une copie de sa pièce d'identité, sans chiffrement des données.

(1) https://www.cnil.fr/fr/prospection-commerciale-et-droits

Une sanction aggravée par la procédure d'harmonisation

S'agissant d'un dossier concernant des personnes issues de plusieurs pays européens, la CNIL a dû enclencher la procédure de coopération prévue par le RGPD.

Au cours de cette procédure, l'autorité de contrôle polonaise a formulé des objections qui ont fait l'objet d'un arbitrage au sein du CEPD/EDPB (le groupe des « CNIL » européennes). Il était en particulier reproché à la CNIL une sanction insuffisante au regard des manquements observés et de la taille de l'entreprise.

La décision contraignante du CEPD/EDPB(2) a conduit la CNIL à réviser le montant de l'amende à 600 000 euros.

Des enseignements utiles pour les Délégués à la protection des données

L'AFCDP observe que le mécanisme de coopération et d'harmonisation européen a pour conséquence de rehausser les montants des sanctions décidées par la CNIL en conduisant l'autorité française, souvent plus modérée et conciliante, à se rapprocher d'autorités historiquement plus « sévères ».

La décision rappelle aussi qu'une plainte, conduisant à un contrôle, peut déboucher sur des sanctions portant sur des manquements sans lien direct avec la plainte initiale.

Ainsi, la CNIL attache une grande attention au respect des droits des personnes (droit à l'information, droit d'accès, droit d'opposition), et elle n'hésite pas à sanctionner les cas de non-respect de ces droits.

L'AFCDP attire donc l'attention des DPD/DPO sur l'importance accordée par la CNIL à la sécurité des traitements. Elle alerte en particulier sur la pratique de transmission de pièces d'identité par email, sans chiffrement, encore couramment observée au sein des organismes, et sur la nécessité de sensibiliser les services opérationnels aux risques que cette pratique présente en termes de sécurité des données. ■

(2) https://edpb.europa.eu/system/files/2022-08/edpb_binding_decision_01_2022_accor_fr_redacted_fr.pdf

> *« L'AFCDP alerte en particulier sur la pratique de transmission de pièces d'identité par email, sans chiffrement, »*

ENTREPRISES SPÉCIALISÉES, RÉFÉRENCEZ-VOUS SUR L'ANNUAIRE EN LIGNE

**Les informations de ce guide sont issues de l'annuaire en ligne.
Les sociétés spécialisées en cybersécurité doivent se référencer et mettre à jour régulièrement leur fiche.**

***Attention, l'annuaire est réservé aux entreprises réellement spécialisées en cybersécurité.
La rédaction valide la création des fiches.***

Inscription et mise à jour :
https://www.solutionsnumeriques.com/securite/ annuaire-cybersecurite/

Les tendances

de la cybersécurité



Cyber-sécurité : on accélère !

Panorama des start-ups françaises de la cybersécurité

Protection endpoint : EDR et XDR redonnent l'avantage aux RSSI

Le secteur Cyber s'organise face à la crise des talents

Peur sur la Supply Chain

La cybersécurité bascule dans le Cloud

Cybersécurité industrielle : vers une convergence IT / OT ?

Cyber-sécurité : on accélère !

Entretien avec Thierry Auger, DSI et RSSI du groupe Lagardère,
Président des Assises 2022



Thierry Auger cumule les fonctions de DSI et de RSSI pour le groupe Lagardère. Cela lui confère un statut d'observateur exceptionnel sur les enjeux de l'IT et de la sécurité. Nous avons souhaité cet entretien car il est également cette année président des Assises de la sécurité. L'édition 2022 de cet évènement sera placée sur le signe de l'accélération, et Thierry Auger, présente les thèmes qui seront évoqués. Nous l'avons aussi interrogé sur les défis qui se posent aujourd'hui aux RSSI français : comment accroître la résilience de l'entreprise, hausser le niveau de protection tout en se plaçant au service du business.

L'édition 2021 des Assises avait été placée par Olivier Ligneul sous le thème du « Back to Fondamentals ». Quel est celui que vous avez choisi pour cette édition 2022 ?

« Les Assises 2022, on accélère », avec une ligne éditoriale qui assure la continuité en reprenant aussi dans ces thématiques celui du « Back to Fondamentals » mais avec l'idée qu'il faut désormais monter en puissance. Pour moi, cette idée regroupe deux choses : il faut d'une part augmenter la résilience et le niveau de protection, mais aussi accompagner l'accélération de l'action des équipes de sécurité. Le socle sanitaire doit encore être consolidé face aux nouvelles menaces, la liste des projets à traiter par les RSSI reste longue, ce qui implique de prioriser ces chantiers. Pour que cette accélération se traduise dans les faits, il faut choisir ses priorités, revoir les solutions pour privilégier l'efficacité et replacer la protection de la donnée au cœur de la problématique.

Qu'est-ce que cela implique ce changement de posture de sécurité ?

Pour moi, la priorité numéro 1 doit être la protection de la donnée. Le RSSI doit se placer en capacité de restituer la donnée aux métiers quel que soit le type d'attaque subie, y compris si les sauvegardes sont visées par les attaquants. La guerre en Ukraine nous a montré que les techniques de destruction de données mises en œuvre peuvent être extrêmement intelligentes et efficaces. La résilience des sauvegardes est un impératif aujourd'hui. En parallèle, il est indispensable d'augmenter les surveillances actives et intelligentes afin de détecter une potentielle fuite de données le plus en amont possible afin de pouvoir réagir avant un incident, une divulgation, c'est aussi cela l'accélération. Une fois exfiltrées et divulguées, il devient quasiment impossible de les rattraper et de chercher à en contrôler la diffusion. Il est donc clairement préférable de les protéger et de

surveiller efficacement pour réagir immédiatement. En outre, la conformité nous pousse clairement dans ce sens.

La conformité est une thématique croissante à l'agenda des DSI et de leur RSSI.
La gestion de la conformité est une autre problématique appelée à fortement monter en puissance dans l'agenda du RSSI. Si on fait une projection à 5 ans, on voit que de nombreux pays cherchent à mettre en place des règlements spécifiques pour protéger les données personnelles de leurs citoyens mais aussi pour contrôler les exports de ces dernières vers l'extérieur. Cette volonté d'isolation sera clairement un challenge pour les entreprises présentes dans plusieurs pays. Depuis de nombreuses années, les DSI ont cherché à optimiser leurs SI en centralisant et en mutualisant les applications et le catalogue de services afin de minimiser les coûts et les charges, Ce modèle devra désormais tenir compte de ces nouvelles contraintes et donc s'adapter en conséquence.. Si on prend l'exemple des Etats-Unis, 4 à 5 états ont légiféré sur la question, une dizaine d'autres sont en cours. Si demain une vingtaine de pays imposent des règles de protection et de localisation des données différentes, il va falloir remettre le modèle centralisé à plat. Ira-t-on vers des hubs de données locaux et des mécanismes de transfert et de synchronisation ? Ce sont des architectures complexes que les DSI vont devoir imaginer afin de répondre à ces nouvelles contraintes de conformité.

> *« Il ne faut pas hésiter à innover et déployer les offres pertinentes de start-up. »*



Lorsque vous appelez au renforcement du socle sanitaire, sur quoi les entreprises doivent-elles porter leurs efforts selon vous ?
La priorité varie en fonction du contexte de chacun, mais les éditeurs et constructeurs doivent prendre leur part dans cette accélération. Depuis quelques mois, nous en avons vu plusieurs faire évoluer leurs offres pour aller vers une nouvelle approche qui nous parait très intéressante pour l'avenir. Les éditeurs comme Microsoft, Github, Firefox, Apple, embarquent de plus en plus de mécanismes de sécurité par défaut dans leurs offres qui participent par défaut à élever le niveau de sécurité global pour un RSSI. Ainsi, Windows 11 bloque automatiquement l'accès après une série de tentatives de connexion et impose une double authentification. Il faut pousser les éditeurs à aller de plus en plus vers ces approches « Secure by design » et embarquer des comportements de sécurité à toutes leurs offres. C'est un moyen de réduire d'une manière globale la complexité de la cybersécurité et de réduire le risque

Au sein du groupe Lagardère, vous n'hésitez pas à faire appel à des start-up pour renforcer votre socle technologique. Quel rôle doivent jouer ces start-up dans cette stratégie d'accélération ?
Pour réussir cette accélération dans un contexte où les moyens sont comptés et les effectifs restreints, les entreprises vont devoir miser sur l'innovation pour améliorer leur sécurité. Nous avons besoin de technologies intelligentes et sur ce plan il ne faut pas hésiter à innover et déployer les offres pertinentes de start-up. Pour prendre un exemple, le groupe Lagardère a fait le choix de s'appuyer sur les services de CybelAngel pour augmenter les surveillances et donc renforcer la protection de ses données. C'est un éditeur que nous suivons depuis 2014 lorsqu'ils ont reçu le trophée de la PME innovation au FIC. Ils n'étaient encore que 4, ils sont près de 200 aujourd'hui. Miser sur des technologies innovantes telles que l'IA dans la cybersécurité a un coût, c'est vrai, mais elles peuvent rendre d'énormes services. Forrester a estimé le retour sur investissement apporté par la solution de CybelAngel à 359% sur 3 ans ! Ce type d'informations permet de négocier auprès d'une direction générale afin d'investir dans l'innovation.

Quels sont les freins auxquels se heurtent les RSSI face à cette nécessaire accélération ?
Outre la part de la cybersécurité dans le budget IT qui doit rapidement s'accroitre, le manque de compétences disponibles est un frein important à la montée en puissance de la cybersécurité dans les entreprises. Ce problème RH n'est pas un problème français ou européen en soi. Tous les pays au monde y sont confrontés à plus ou moins grande échelle. La Chine a récemment lancé un plan de formation massif dans ce domaine. De notre côté, nous devons réfléchir à des dispositifs pour amener plus de personnel dans les métiers de la cybersécurité. Je pense qu'il faut notamment proposer aux ingénieurs informaticiens des parcours de reconversion vers nos métiers. Ce sont des gens bien formé qui, je pense, peuvent être progressivement amenés vers nos métiers. Il faut réfléchir à des dispositifs pour les faire monter en puissance directement au sein des équipes opérationnelles de sécurité. C'est une voie que les entreprises françaises devraient suivre pour faire face à une

pénurie de compétence qui n'aura de toute façon aucune issue à moyen terme.

L'externalisation et un recours massif aux services managés semblent une voie fréquemment empruntée par les RSSI pour contourner ce déficit de compétences disponibles…
Sur un certain nombre de services, le modèle managé permet de s'appuyer sur un spécialiste est bien plus efficace que ce que l'on peut faire seul dans son entreprise. Par nature, le terrain de jeu d'un fournisseur de services de sécurité est bien plus vaste et ces prestataires peuvent atteindre une efficacité opérationnelle impossible à atteindre par une entreprise dont la cybersécurité n'est pas le métier. L'exemple le plus évident est celui du monde des SIEM et des SOC externalisés. Une entreprise peut déployer elle-même un SIEM mais toute la valeur se situe dans les hommes qui vont le mettre en œuvre, dans les algorithmes de détection qu'ils vont mettre en place. Pour une entreprise isolée, il est très coûteux de monter en puissance et au final, quand survient un incident, on se rend compte que le SIEM ne l'a pas remonté. La détection est complexe, se transforme en permanence, si bien qu'au final, l'investissement est très important pour un système qui, souvent, ne détecte pas certaines attaques. Cela montre qu'il faut sortir de cette logique et accepter que si on a besoin de la technologie, ce n'est pas nécessairement à l'entreprise de la porter sauf contraintes ou priorités spécifiques à certaines activités particulièrement contraintes. Ce fut le cas des salles blanches il y a quelques années, toutes les entreprises se sont peu à peu tournées vers des spécialistes pour héberger leurs serveurs car disposer de ses propres salles performantes nécessite aujourd'hui d'investir des sommes astronomiques et que ce n'est pas la finalité d'une DSI. D'autant que l'aspect RSE est venu s'ajouter à cela ; il y a aujourd'hui une nécessité de réduire la consommation énergétique de l'IT, les hébergeurs professionnels savent faire cela bien mieux que ce que nous pouvons faire seuls de notre côté.

> *« Comment accroître la résilience de l'entreprise, hausser le niveau de protection tout en se plaçant au service du business ? »*

Quel va être le rôle du RSSI dans le futur ? Deviendra-t-il un « simple » gestionnaire de contrats de services ?
Le RSSI sera un super chef d'orchestre qui devra identifier quelles sont les solutions disponibles sur le marché et choisir celles qui sont le plus en adéquation avec l'environnement, les attentes de ses métiers, son exposition et les priorités de son entreprise. La tâche n'est pas simple car il doit avoir une visibilité sur les solutions technologiques et les offres, mais surtout évaluer leur niveau de maturité réel. Il s'agit d'un problème récurrent dans l'innovation : sur le papier, les éditeurs annoncent toujours des solutions 100% opérationnelles, mais une bonne idée demande à être développée. Au démarrage, une solution proposée par une start-up n'est pas encore industrialisée et il faut généralement beaucoup de temps pour aboutir à une solution réellement mature. C'est très compliqué d'estimer le niveau de maturité d'une nouvelle offre tant qu'on ne l'a pas déployée soi-même. Remonter ce type d'information implique un travail de concert entre les RSSI, un travail en réseau pour remonter des informations sur l'efficacité réelle des solutions. Il existe des outils intéressants comme le radar Wavestone des start-up de la cybersécurité par exemple, mais le rôle d'un événement comme les Assises de la sécurité est essentiel dans ce partage d'expériences. Le campus Cyber a sans doute aussi un rôle à jouer dans cette capitalisation d'expérience, nous verrons quelles seront les propositions qui émergeront de cette nouvelle structure qui s'organise actuellement sur ces sujets. ■



Propos recueillis par Alain Clapaud et Jean Kaminsky

A la pointe de l'innovation

Panorama des start-ups fra

Chaque année, le cabinet Wavestone réalise son « radar » des start-ups françaises du secteur de la cybersécurité. Une remarquable analyse des points forts et des points faibles de cet écosystème dynamique.

Par Jean Kaminsky

166 startups spécialisées en cybersécurité ont été analysées en 2022, dont 45 nouvelles. 150 étaient détaillées en 2021, ce qui prouve le dynamisme de l'écosystème. Mais l'étude relève que « *beaucoup de startups n'arrivent pas à passer à l'échelle : 13 sorties relevées en 2022 ...* »

Deux fois plus de Scale-ups

Le rapport indique : « *L'écosystème mûrit progressivement. Il donne naissance à de plus en plus de scale-ups (11 en 2021 vs. 24 en 2022), et à la première Licorne cybersécurité du marché : Ledger. Il faut aussi noter une acquisition majeure : celle de Ubble par la solution britannique de solutions de paiement, Checkout.com, un témoin de l'attractivité du savoir-faire français en cybersécurité.* »

Levées de fonds multipliées par 6 en un an

Le Radar analyse le nerf de la guerre : les levées de fonds. Après la période du Covid, elles ont été multipliées par six (100M€ en 2021) avec 630M€ en 2022. Même si cette progression doit être relativisée note Wavestone car « il faut prendre en compte l'effet Ledger (330 millions) ».

Le cabinet nous rappelle également notre place modeste par rapport aux levées de fonds des champions américains, 14Md€ environ, mais aussi britanniques (900M€ environ) ou israéliens (1,6Md€ environ).

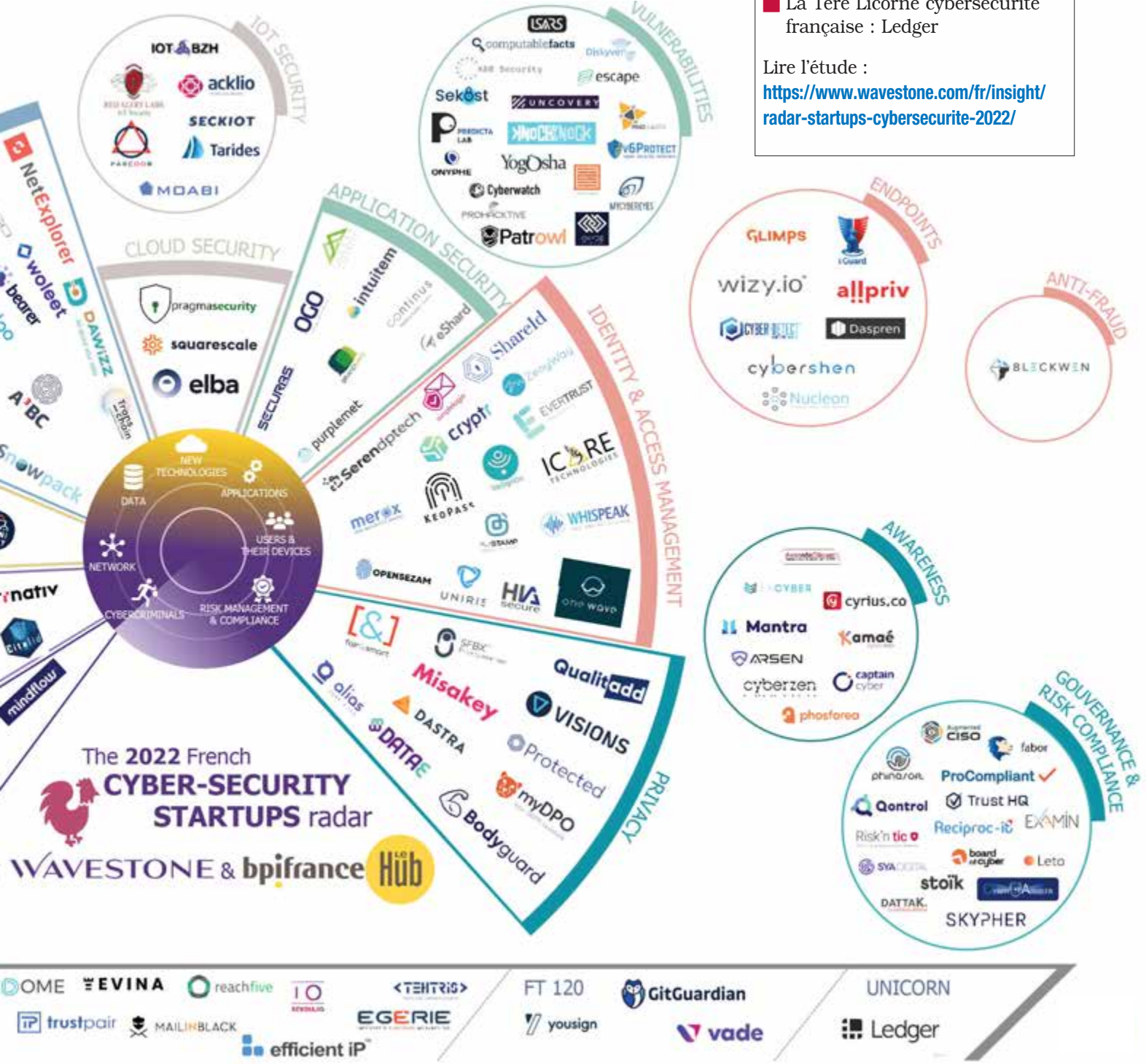
Gérôme BILLOIS, Partenaire chez Wavestone conclut : « *L'écosystème français confirme son dynamisme, sa richesse et sa solidité, aussi bien pour les start-ups que pour les scale-ups. Les prochains défis seront ceux d'être plus impactant en matière d'innovation et dans le développement à l'international pour rivaliser avec les autres écosystèmes.* »



nçaises de la cybersécurité

- 166 startups dans le radar vs. 150 en 2021, un chiffre relativement stable
- 24 scale-ups cybersécurité en France
- La 1ère Licorne cybersécurité française : Ledger

Lire l'étude :
https://www.wavestone.com/fr/insight/radar-startups-cybersecurite-2022/



Protection endpoint : EDR et XDR redonnent l'avantage aux RSSI

Plus que jamais, avec l'essor du télétravail et du BYOD, le poste client joue un rôle-clé dans la sécurité du système d'information. Alors que les attaques de ransomware ou phishing redoublent, les EDR et leurs algorithmes d'intelligence artificielle apportent une nouvelle arme aux défenseurs.

Par Alain Clapaud

Avec un taux de croissance supérieur à 25% pour la période 2021-2027(1), le marché des solutions de protection endpoint de type EDR (Endpoint Detection & Response) connait son âge d'or. Celles-ci font passer la protection des endpoints d'une défense de type statique à une détection active, s'appuyant notamment sur l'intelligence artificielle pour détecter des attaques non encore répertoriées. Les algorithmes de Machine Learning sont aujourd'hui suffisamment matures pour se livrer à une analyse comportementale sur les postes sans multiplier les faux positifs. En outre, l'EDR fournit au RSSI une capacité de réaction rapide et de remédiation en cas d'attaque avérée. Il est possible d'enrayer la diffusion latérale d'une attaque et de circonscrire celle-ci à quelques postes. 1

Le Covid-19 a indirectement boosté l'adoption des EDR

Les solutions de type EDR ne sont pas totalement nouvelles. L'idée remonte aujourd'hui à une dizaine d'années. Néanmoins, le surcoût du déploiement de solutions considérées comme un complément aux logiciels d'EPP (Endpoint Protection Platform) plus classiques a poussé les RSSI à différer leur investissement. La vague de ransomware à laquelle les entreprises ont dû faire face lors de la pandémie de Covid-19 a sans doute précipité les choses. L'EDR a profité des rallonges de budget Cyber accordées aux DOSI pour faire face à ce défi de sécuriser des organisations dont le personnel était massivement en télétravail. Ces solutions de nouvelle génération se sont imposées comme un moyen pour les entreprises de contrer efficacement cette avalanche d'attaques et bon nombre ont franchi le pas et commencé à déployer des EDR dans leur système d'information. Si les éditeurs poussent naturellement vers une couverture à 100% des endpoints, l'argument étant que le pirate exploite le maillon de sécurité le plus faible pour attaquer une entreprise, les entreprises ont souvent préféré couvrir leurs assets les plus critiques avant d'étendre plus avant ces déploiements.

De facto, le marché des EDR a gagné en maturité. De nombreuses start-up ont investi en R&D pour prendre position et les grands éditeurs de la cybersécurité ont multiplié les acquisitions pour étoffer leurs offres. Outre la prise de contrôle de Carbon Black par VMware, de Secdo par Palo Alto Networks, celle de Darkbytes par Sophos ou encore de ReaQta par IBM, tous les grands éditeurs répondent aujourd'hui présents et affichent une offre EDR à leur catalogue. Depuis Broadcom/Symantec, Cisco, FireEye, Palo Alto, Trend Micro, VMware Carbon Black, les grands éditeurs luttent désormais avec les quelques pure players de la protection endpoint comme Crowdstrike, Cybereason, Sentinel One. La couverture fonctionnelle des plateformes EDR de chacun s'est beaucoup élargie et seules des évaluations très élaborées et des Proof-of-Concept peuvent permettre de départager des offres qui, sur le papier, semblent toutes très proches.

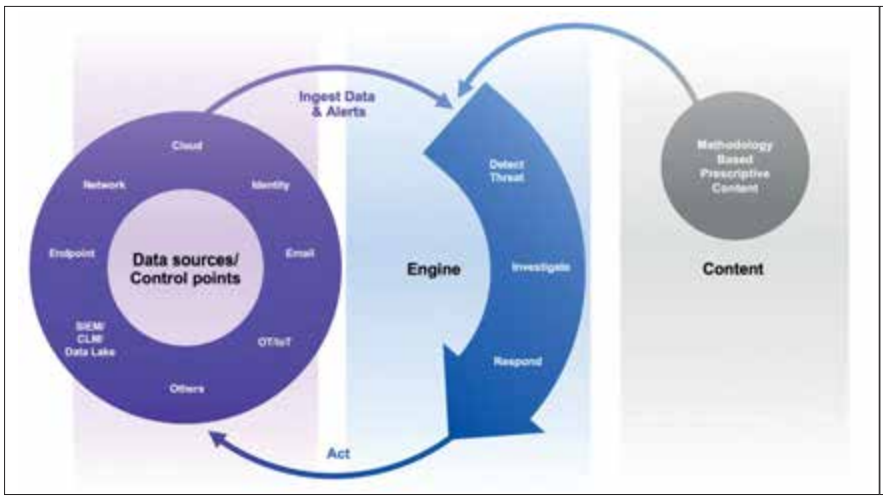
Une évolution « naturelle » vers le XDR

Face à une approche SIEM qui va multiplier les sources de données au sein du système d'information et corréler ces informations pour trouver des schémas d'attaques complexes, la limite de l'EDR est de s'appuyer sur les données collectées au niveau des agents déployés sur les endpoints. Le cheval de bataille des éditeurs est désormais d'alimenter leurs plateformes EDR de nouvelles sources de données afin d'accroitre encore leurs capacités de détection, notamment afin de déceler

(1) *Endpoint Detection and Response Market – Growth, Trends, Covid-19 impact, and Forecasts (2022 – 2027), Mordor Intelligence, 2022*



1 Le télétravail a été perçu par les pirates comme une opportunité à saisir pour attaquer les entreprises via leur talon faible, les postes de travail distants.
(Source : Etat de la cybersécurité en 2022, Splunk)

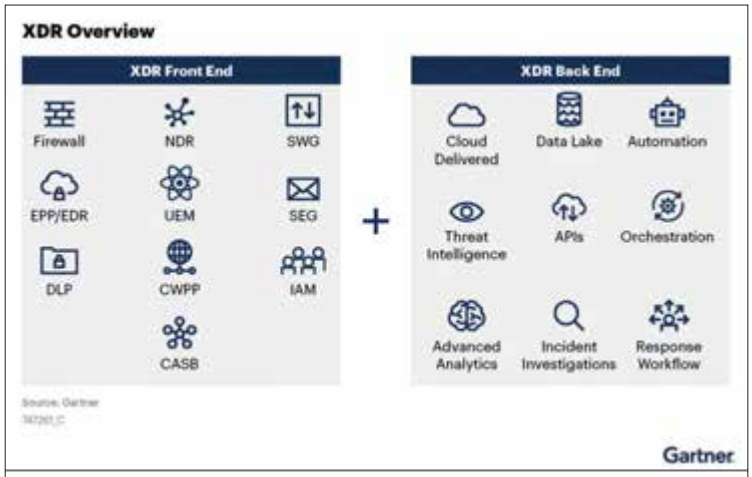


3 Un écosystème de solutions articulées autour de l'XDR tel que l'ont imaginé les membres de la XDR Alliance.

les mouvements latéraux des attaquants. 2 Une nouvelle génération d'EDR est ainsi apparue, celle des XDR. Là-encore, tous les éditeurs se sont mis au diapason et proposent une plateforme de ce type, l'idée étant d'interconnecter un écosystème de solution de sécurité afin d'alimenter un Data Lake sur lequel faire tourner les algorithmes de détection. Les éditeurs de cybersécurité « généralistes » interconnectent ainsi leur portefeuille de solution à leur offre XDR, mais on a aussi assisté à l'émergence d'alliances entre éditeurs à l'image de l'Open XDR Platform des éditeurs français SEKOIA, Harfanglab, Pradeo, Glimps, Vade et Gatewatcher et de l'XDR Alliance. On retrouve dans cette dernière, entre autres, Exabeam, Cyberark, Netskope, SentinelOne et VMware. Il est à noter que Google Cloud qui édite le service Chronicle (issu de l'acquisition Siemplify en janvier 2022) participe à cette alliance. L'américain est aussi un solide allié pour Cybereason : celui-ci à injecté 50 millions de dollars dans l'éditeur d'EDR et les deux partenaires se sont associés pour délivrer une offre XDR portée par Google Cloud. L'éditeur Crowdstrike a lui aussi entrepris de créer un écosystème autour de son offre ; la CrowdXDR Alliance dans laquelle on retrouve plusieurs membres de la XDR Alliance, dont Google Cloud, Netskope mais aussi Claroty, Cloudflare, Okta, PingIdentity, Proofpoint, ServiceNow et Zscaler. Plus qu'une simple solution de sécurité supplémentaire qui va venir s'ajouter à un bestiaire déjà bien rempli, l'XDR se présente comme un véritable écosystème de sécurité. Choisir un XDR apparaîtra de plus en plus comme un choix d'écosystème pour le RSSI.

L'XDR bouscule l'ordre établi

Ce passage de l'EDR vers l'XDR constitue un changement de nature de la solution beaucoup plus profond qu'il n'y parait. Alors que l'EDR n'était perçu que comme une extension à l'arsenal des solutions de protection endpoint, le XDR s'impose de plus en plus comme une alternative technologique aux SIEM qui motorisent tous les SOC actuels. C'est une aubaine pour les entreprises dont l'équipe sécurité et le budget ne sont pas assez étoffés



2 L'architecture fonctionnelle d'un XDR telle que la définit le Gartner.

pour constituer un véritable SOC. Toutefois les analystes du Gartner mettent en garde les DOSI : les XDR n'ont pas encore la couverture fonctionnelle suffisante pour répondre aux besoins de l'équipe SOC d'une grande entreprise. Sur le haut du marché, le XDR va clairement jouer un rôle de complément au SIEM en attendant plus… D'ici 2027, les analyses du Gartner estiment que 40% des entreprises utiliseront un XDR. 3

Faut-il y voir un premier effet de l'action des EDR et XDR ? Une étude réalisée chaque année par Mandiant(2) fait apparaitre en 2022 une diminution du « dwell time », ce délai entre le moment où l'attaquant s'infiltre dans le système d'information et celui où il est détecté. Réduire cet indicateur est capital pour contrer une attaque en préparation. Ce délai moyen est passé de 78 jours en 2018 à 21 jours « seulement » en 2022, une progression très significative. Pour rappel ce délai était de 243 jours il y a 10 ans et de 416 jours en 2011 ! Nul doute que l'adoption massive des EDR/XDR devrait permettre d'améliorer encore ce résultat.

AC

(2) Mandiant M-Trends 2022

Le secteur Cyber s'organise face à la crise des talents

Depuis quelques années, les entreprises comme leurs prestataires sont confrontés à une pénurie de talents, une pénurie particulièrement sévère dans le domaine de la cybersécurité. Faute de personnel, les entreprises se tournent vers les MSSP.

Par Alain Clapaud

Guillaume Poupard, directeur général de l'ANSSI l'expliquait clairement lors de l'édition 2022 du FIC (Forum international de la cybersécurité) : « *Le sujet RH est ce qui va nous limiter dans les années à venir* ». Si les directions générales ont débloqué des budgets ces derniers mois afin de renforcer la sécurité, force est de constater qu'embaucher des experts en cybersécurité reste un exercice difficile et... coûteux. Un benchmark publié par Wavestone fait état de 15 000 postes vacants en France. Cette pénurie est globale, avec 3 millions de personnes qualifiées qui manquent à l'appel dans le monde, dont 700 000, rien que pour les Etats-Unis. L'administration Biden a lancé un plan sur 120 jours pour mettre en place de nouveaux programmes de formation en cybersécurité, un plan qui s'inscrit dans un programme plus large, le "Good Jobs Challenge" qui vise à drainer de nouvelles populations de candidats, dont les femmes, les minorités vers les métiers plus qualifiés

En France, ce déficit de talents a été bien identifié et de nombreux cursus de formation ont été créés ces dernières années. Le plus emblématique est celui de Microsoft qui, sur le modèle de ce qui avait bien fonctionné pour les métiers du Big Data et de l'intelligence artificielle a créé l'Ecole Cyber Microsoft by Simplon.

Le choix pragmatique de l'externalisation

Néanmoins les écoles en cybersécurité ont bien du mal à faire le plein et les entreprises vont devoir vivre encore longtemps en situation de pénurie. Le recours à la prestation externe est le passage obligé dès lors que l'on souhaite créer puis faire croitre une équipe cyber interne. Ce recours à la prestation à un coût et ne fait que transférer cette problématique RH à un tiers qui se retrouve, lui aussi, confronté à un vivier de candidats bien trop restreint. Une autre approche consiste à privilégier les services managés de sécurité. L'exemple du CyberSOC, le SOC (Security Operations Center) géré par un tiers, est emblématique de ce mouvement. Monter un SOC demande d'investir énormément en technologies et surtout embaucher

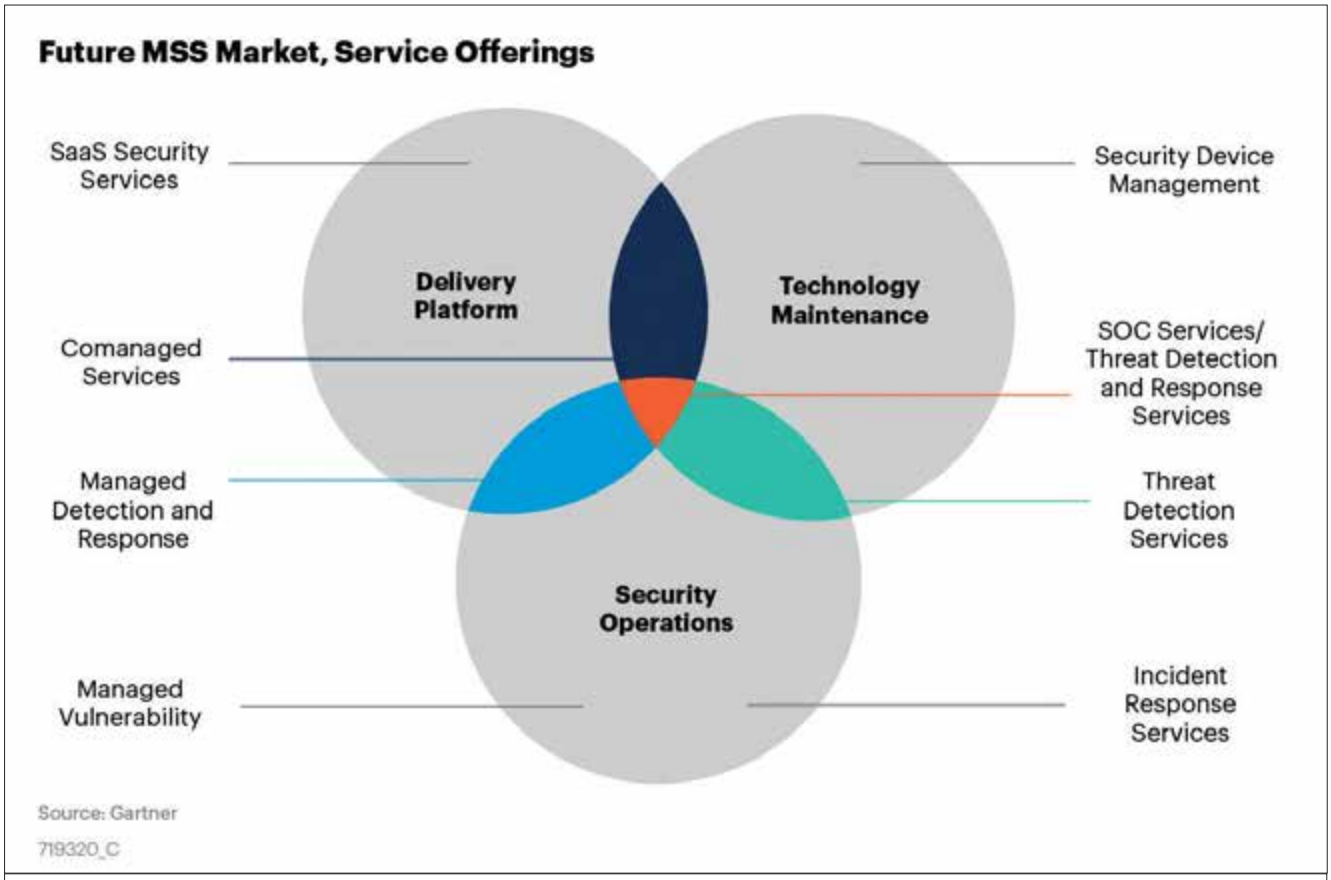


Outre des budgets encore insuffisants, la cybersécurité souffre en France d'un manque cruel de talents. Guillaume Poupart, directeur général de l'ANSSI soulignait encore cette problématique lors du FIC 2022. La course à la technologie ne palliera sans doute qu'en partie ce manque chronique de main d'œuvre.

(Photo : Olivier Bellin, Solutions-Numériques)

énormément de personnel si on vise un fonctionnement en 24/7. Même les entreprises les plus prestigieuses ou du mal à garnir leurs salles de supervision, d'autant que le turn over est élevé sur les postes d'analystes de niveau 1.

S'appuyer sur l'offre SOC d'un prestataire spécialisé est clairement un moyen pour des entreprises du midmarket de disposer d'un tel service en 24/7, ce qu'elles ne pourraient faire en s'appuyant sur leurs propres moyens. Si les grandes entreprises peuvent prescrire les solutions mises en œuvre par leur prestataire, pour les petites entreprises, le CyberSOC se présente plutôt comme un service

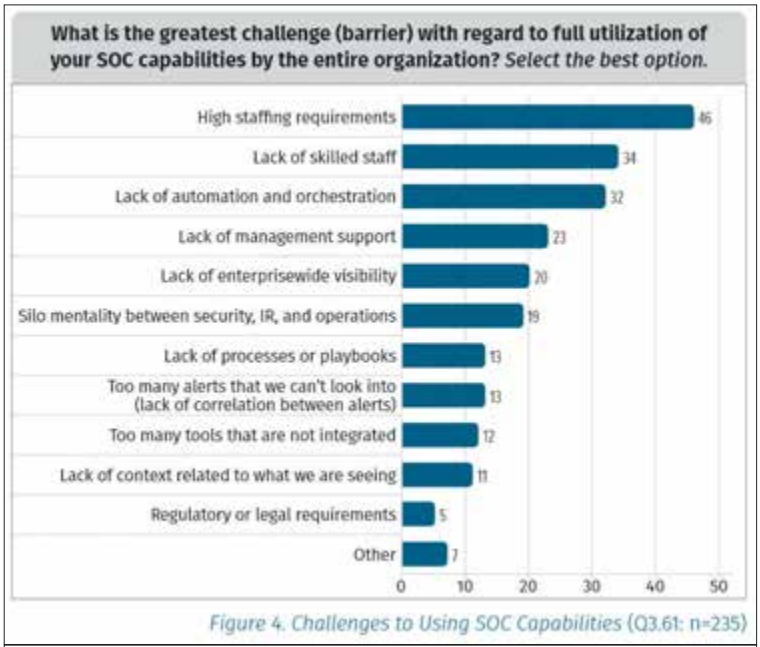


2 L'éventail des services managés en sécurité tel que le formalise le Gartner.

clefs en main beaucoup plus accessibles financièrement. De facto, les MSSP (Managed Security Services Provider) français, qu'il s'agisse des grosses ESN, des acteurs spécialisés ou de prestataires régionaux offrent un large panel de services de sécurité externalisés qui ciblent les grandes entreprises pour les uns, les marchés midmarket et PME pour les autres. Fortune Business Insight estime à +12,6% par an la croissance du marché mondial des services MSSP sur la période 2021-2028. 2

Outre le monitoring temps réel de la sécurité, une étude Forrester(1) pointe logiquement les audits de sécurité et la Threat Intelligence parmi les domaines les plus fréquemment confiés à un tiers. Pour les responsables interrogés, la gestion des systèmes de sécurité reste le service qui présente le plus de valeur à leurs yeux, devant les données d'intelligence sur les vulnérabilités, l'audit cyber et encore la réponse à incidents. Le marché des MSP et des MSSP évolue avec de plus en plus d'acteurs, des concentrations et de plus en plus

(1) « *Improve Your Cybersecurity (With A Little Help From Your MSSP)*", *Enquête Forrester Consulting réalisée pour CyberProof, Janvier 2019*



1 L'embauche d'experts de haut niveau et le recrutement des équipes figurent parmi les principaux défis à relever dans la mise en place d'un SOC. Une problématique RH qui pousse de nombreux responsables à opter pour des SOC managés externes.



3 Le recours a un MSSP est fréquent pour réaliser un audit de sécurité, la surveillance en 24/7 ou bénéficier d'un service de Threat Intelligence ou encore confier la gestion d'un système de sécurité à un tiers.



4 Les solutions étudiées par les entreprises afin de faire face à la crise des talents dans la cybersécurité (Source : Splunk, Etat de la cybersécurité en 2022)

de services packagés. L'exemple du décollage des services MDR illustre bien le dynamisme du marché. Il existe une foison d'offres EDR/XDR managées par un tiers, avec des MSSP qui se retrouvent parfois en concurrence avec les éditeurs eux-mêmes. Les solutions de sécurité étant de plus en plus proposées en mode Cloud, il peut sembler « naturel » pour un éditeur de monter une offre packagée exploitant sa technologie. Il s'agit souvent de services généralement ultra packagés et industrialisés auxquels répondent les MSSP par une plus grande personnalisation et une proximité géographique souvent appréciée en cas d'incident. 3

De l'intelligence artificielle pour remplacer les cerveaux manquants ?

L'autre réponse possible au manque de bras dans la cybersécurité est technologique. Elle passe par une automatisation des processus de réponse à incident, notamment par un recours de plus en plus fréquent au SOAR pour traiter les incidents de sécurité bien connus. Tous les opérateurs de SOC managés ne peuvent espérer améliorer la rentabilité de leurs infrastructures que grâce à une industrialisation à outrance des process techniques et à l'automatisation d'une partie de la réponse à incident. Estimé par ReportLinker à environ 1 milliard de dollars en 2021, le marché des solutions de SOAR (Security Orchestration, Automation and Response) est amené à doubler d'ici 2027. IBM, Palo Alto, Google Chronicle (ex-Siemplify), Swimlane, Rapid7 ou Splunk, il existe de nombreux éditeurs qui proposent des solutions d'orchestration matures. Reste aux DOSI et aux RSSI a placer le curseur de l'automatisation en fonction de leurs propres impératifs business. Il n'est jamais facile de devoir expliquer à une direction générale la mise hors ligne de serveurs de production critiques à cause d'une suspicion d'attaque... 4

L'autre solution souvent évoquée pour pallier les bras manquants consiste à recourir aux algorithmes d'intelligence artificielle. Outre la détection d'intrusion, l'analyse des signaux faibles, l'IA sera amenée à intervenir dans de très nombreux cas d'usage, depuis la détection de fraude, le DLP (Data Loss Prevention), la gestion des identités et des accès, la conformité. Pour autant, une IA omniprésente aura bien du mal à réduire le déficit chronique de talents dont va souffrir le secteur tout au long de cette décennie.

AC



HS2

Hervé Schauer Sécurité

Formation cybersécurité technique

INTRODUCTION • RÉSEAUX
INFRASTRUCTURES • DÉFENSE

PROGRAMME

Introduction à la cybersécurité

ESSCYBER
Essentiels techniques de la cybersécurité
SECUCYBER
Fondamentaux techniques de la cybersécurité

Sécurité des réseaux et des infrastructures

SECUARCH
Sécurité des architectures
SECUWIFI
Sécurité et Red Team Wi-Fi moderne
SECUPKI
Infrastructures de clés publiques
SECUPKIWIN
Infrastructures de clés publiques Windows

Sécurité défensive

SECUWIN
Sécurisation des infrastructures Windows
SECULIN
Sécurité Linux
SELinux
Comprendre SELinux et savoir modifier la politique de sécurité
SECUWEB
Sécurité des serveurs et des applications Web
SECUINDUS
Cybersécurité des systèmes industriels
SECUOBJ
Sécurité des objets connectés
SECUMOBILE
Audit sécurité d'applications mobiles Android et iOS

+ 33 974 774 390

www.hs2.fr

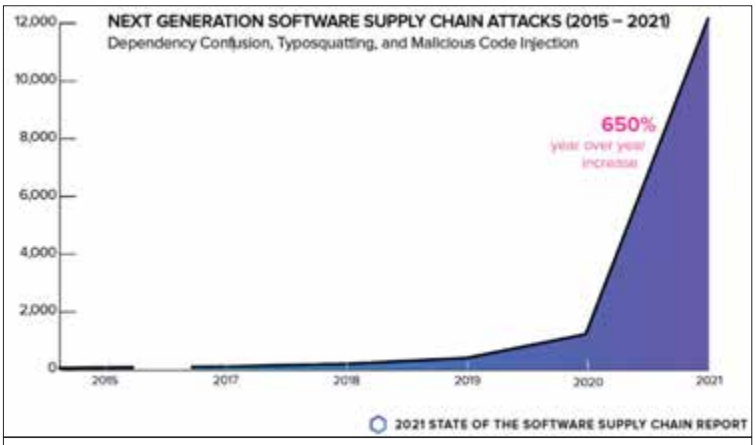
formation@hs2.fr

Peur sur la Supply Chain

Dans une économie ou chaque entreprise s'appuie sur une myriade de prestataires et de partenaires, où les systèmes d'information sont hyperconnectés, la sécurité devient l'affaire de tous. Néanmoins s'assurer de la sécurité des tiers est une problématique qui reste complexe à intégrer dans une stratégie de sécurité.

Par Alain Clapaud

Attaquer le maillon le plus faible d'une chaine de sécurité pour la briser, c'est le B.A. BA de l'attaque informatique. Attaquer un prestataire, un sous-traitant pour rebondir et pénétrer le système d'information de la véritable cible n'est pas une idée nouvelle. L'attaque d'un casino de Las Vegas en 2017 via le système de maintenance connecté de son spectaculaire aquarium est entrée dans les annales. Ce type d'attaque a été répété par la suite sur le système de climatisation pour accéder au système d'information de la célèbre enseigne de distribution américaine Target. 1



1 Les attaques sur la Supply Chain sont un phénomène en accroissement rapide qui nécessite des mesures spécifiques, tant organisationnelles que techniques. (Source : State of the 2021 Software Supply Chain, Sonatype)



2 : Si un tiers des DOSI ont obtenu une rallonge budgétaire pour traiter le risque lié à la Supply Chain, aucune solution unique ne se dégage vraiment face à une problématique complexe. (Source : Splunk, Etat de la cybersécurité en 2022)

Les éditeurs de logiciels et services sont devenus des cibles de haute valeur

Plus récemment, l'attaque sur SolarWinds découverte en 2020 a montré que certains logiciels très prisés des entreprises et des administrations sont devenus une cible de choix pour les attaquants. En s'infiltrant dans le logiciel Orion de l'éditeur, ceux-ci se sont ouvert la voie à 18 000 entreprises, et notamment une écrasante majorité du Fortune 500 avec 425 entreprises impactées.
Ce coup de semonce doit non seulement pousser l'ensemble des éditeurs de logiciels et de services Cloud à muscler la protection de leurs infrastructures, mais elle doit aussi les pousser à intégrer la composante sécurité au cœur de la conception de leurs produits, aller vers une démarche DevSecOps et ne publier plus que des solutions « Secure by Design ».

L'attaque du ver Stuxnet contre les centrifugeuses du programme nucléaire iranien en juin 2010 a poussé Siemens, dont les automates avaient été visés, à investir massivement dans la cybersécurité et s'inscrire dans une démarche « Secure by Design » pour redorer le blason de ses produits. Tous les éditeurs doivent aujourd'hui suivre cet exemple et revoir leurs processus de développement d'autant que la faille découverte dans la librairie Log4J a récemment mis en avant la présence de vulnérabilités dans bon nombre de logiciels, y compris certains qui sont très largement présents dans le système d'information d'une entreprise classique.

Répertorier et patcher lorsque c'était possible toutes les solutions mettant en œuvre cette librairie fut un travail colossal pour de nombreux responsables et, outre les traditionnelles certifications ISO avancées par les éditeurs, le besoin de solution « Secure by Design » est plus que jamais nécessaire. 2

De leur côté, les entreprises doivent agir afin de réduire le risque lié à leur supply chain IT. Celles-ci vont devoir rapidement monter en puissance sur le volet de la gestion des vulnérabilités afin d'améliorer leur capacité à patcher rapidement leurs systèmes en cas d'alerte et ne plus passer des jours à analyser leurs logiciels pour savoir

s'ils contiennent une librairie potentiellement dangereuse. Devant la complexité de la tâche, plus de 20 000 nouvelles vulnérabilités sont découvertes chaque année, il est impossible pour une entreprise de disposer d'un système d'information qui ne soit pas entaché de multiples vulnérabilités.
Beaucoup ne sont pas exploitables directement par un attaquant car protégés par de multiples protections périphériques, d'autres font courir un danger direct à l'entreprise. Prioriser l'action de l'équipe de sécurité est donc vital et la mise en œuvre de solution de type CSAM (CyberSecurity Asset Management) va permettre aux RSSI de disposer d'une vue synthétique de la situation, identifier rapidement les points où il faut intervenir en urgence.
L'outil va permettre de s'attaquer à la dette technique que représente la multitude de vulnérabilités du système d'information, tout en sachant qu'il restera illusoire de vouloir la réduire à 0 un jour.

Une gestion « administrative » du risque ne suffit plus

Jusqu'à aujourd'hui, les DSI des grandes entreprises ont traité ce risque avec leur direction juridique à coup de clauses contractuelles et de questionnaires envoyés aux prestataires, seuls les plus critiques d'entres-eux faisant l'objet d'un audit technique.
Cette approche « administrative » du risque cyber présente des limites évidentes : dans ses réponses, le fournisseur va être tenté de surévaluer ses efforts en termes de sécurité pour ne pas perdre son client et si le donneur d'ordre est parfaitement protégé du point de vue juridique d'une attaque via son prestataire, si celle-ci survient, ces documents signés et contresignés n'auront été d'aucune aide pour protéger l'entreprise et pour aider à la remédiation de cet incident.
Il est techniquement et financièrement impossible d'auditer réellement les centaines voire les milliers de fournisseurs d'une grande entreprise et vérifier à distance les réponses à un questionnaire de sécurité simple reste très coûteux en temps et d'une efficacité discutable. Des solutions de « screening » permettent de mener une évaluation automatisée de chaque prestataire.
Cet audit technique mené via Internet permet d'avoir une indication sur le niveau de sécurité des ressources IT d'un partenaire, du moins celles qu'il expose sur Internet. Bien évidemment, un score CVSS (Common Vulnerability Scoring System) est une vue relativement succincte de la sécurité IT d'une entreprise puisqu'il ne lève pas le voile sur les processus de sécurité internes.
Des prestataires se sont positionnés pour assurer toute cette gestion administrative de la diffusion et de la collecte des questionnaires de sécurité et d'une première analyse des résultats. Tout comme les agences de notation financière attribuent une note de solvabilité aux Etats et aux organisations, ces prestataires proposent un système de notation qui permet de benchmarker les entreprises sur ce critère cyber.
Si la valeur absolue de la note attribuée est un indice quant à la posture de sécurité de l'entreprise, suivre sa valeur dans la durée est intéressant pour voir si l'entreprise a bien pris conscience des enjeux et investit en conséquence.
La composante cybersécurité s'impose peu à peu comme un critère de sélection des fournisseurs et prestataires de l'entreprise. Le Gartner estime qu'en 2025, 60% des organisations considèreront le risque cyber comme un critère significatif dans toute transaction avec un tiers.

AC

Les 3 bonnes pratiques à appliquer face aux risques liés à la Supply Chain, selon le NIST (National Institute of Standards and Technologies) :

1. Mettre en place des défenses sur le principe que tous les systèmes sont piratés un jour. Il ne s'agit pas seulement de prévenir une attaque mais de prévoir comment y remédier et redémarrer.
2. La cybersécurité ne porte pas que sur la technologie, mais les gens, les processus. Ne pas oublier la composante humaine : l'erreur humaine est bien plus fréquente que la défaillance d'une technologie.
3. La sécurité reste la sécurité. Il ne devrait pas y avoir de frontière entre sécurité physique et cybersécurité. Un pirate peut initier son attaque en exploitant une faille de la sécurité physique de l'entreprise visée.

La cybersécurité bascule dans le Cloud

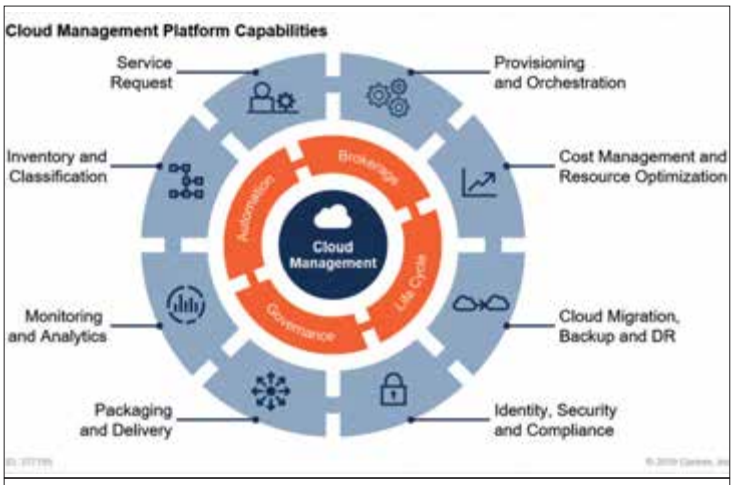
Rares sont aujourd'hui les entreprises à ne pas s'appuyer en partie sur le Cloud public. La cybersécurité se met au diapason avec de plus en plus de solutions Cloud-native et la nécessité de sécuriser les workloads Cloud des entreprises.

Par Alain Clapaud

Le Cloud public, moi jamais ! ce genre de discours était encore fréquent il y a une dizaine d'années, mais aujourd'hui plus aucun DSI ne se risquerait à tenir un tel discours. Le Cloud public est désormais une réalité bien implantée dans toutes les entreprises. Même certains acteurs du secteur de l'armement et de la défense n'hésitent plus à confier certaines workloads à des CSP. Sans revenir sur la pertinence ou pas d'un tel choix, le DOSI et les RSSI doivent se mettre au diapason et à la fois sécuriser ces applications et données hébergées hors des murs de l'entreprise, mais aussi bénéficier des apports des solutions Cloud.

De plus en plus de briques de sécurité deviennent « Cloud-natives »

De nombreux services de sécurité gagnent à être délivrés par des services mutualisés : Threat Intelligence, solutions de protection endpoint de type EDR/XDR, systèmes anti-phishing, jusqu'à des solutions traditionnellement bien enfouies au cœur des systèmes d'information comme la gestion des identités et des accès. Des services tels que les SWG (Secure Web Gateway) ont offert une alternative séduisante aux VPN traditionnels qui se sont vus engorgés lors des phases de confinement imposées par la pandémie de Covid-19.



Les principales capacités d'une plateforme CSPM telles que le Gartner les a définies dès 2019.

S'il reste encore des versions on-premise pour la grande majorité des solutions, certaines seront de plus en plus difficiles à trouver en monde on-premise.

Si la cybersécurité « traditionnelle » glisse peu à peu vers le Cloud public, les RSSI ont rapidement été mis au pied du mur par les métiers : ceux-ci ont besoin de plus en plus de solutions SaaS, de services IaaS et PaaS pour rester innovants, à la DSI de suivre le mouvement et de sécuriser ces workloads.

Les CWP, des outils pour gérer la sécurité des infrastructures Cloud

Outre le portefeuille de solutions des fournisseurs Cloud, les RSSI ont rapidement vu les éditeurs de cybersécurité investir les marketplaces. Ils ont ainsi pu retrouver leurs solutions habituelles dans des versions « As a Service ». Les WAF en sont l'exemple le plus évident, avec des solutions disponibles sous forme d'instances virtuelles facturées à l'usage, puis de véritables services managés. On a aussi assisté au développement des solutions de CWP (Cloud Workload Protection) qui ont pour vocation d'apporter un peu de cohérence, de centralisation et d'efficacité dans la panoplie d'outils de sécurité Cloud. Multi-Cloud, supportant les architectures hybrides et les conteneurs logiciels, ces solutions offrent une vue centralisée des ressources Cloud, une surveillance des assets placés sur le Cloud.

Ces solutions ont des capacités de découvertes des ressources utilisées ainsi que d'auto-remédiation en cas d'alerte. Ces solutions sont aujourd'hui de plus en plus complétées par ce que l'on nomme le CSPM (Cloud Security Posture Management). Ces logiciels contrôlent en permanence que l'usage des ressources Cloud reste dans les clous vis-à-vis de la politique de sécurité définie par l'entreprise, vérifie la conformité aux standards liés à la protection des données, dont le fameux RGPD. Si on y ajoute les CASB, ces solutions logicielles viennent chapeauter l'ensemble des usages cloud d'une entreprise, depuis la simple utilisation d'applications SaaS jusqu'aux architectures de conteneurs les plus complexes en passant par les services PaaS.

AC

Mira

La gestion des risques pragmatique

Cochez les cases **s'appliquant** à votre cas :

- ☐ J'ai des analyses de risques fragmentées et hétérogènes
- ☐ Je produis beaucoup d'analyses et je veux automatiser le contrôle de qualité
- ☐ J'ai du mal à suivre les mitigations associées à mes analyses
- ☐ Je trouve Excel peu adapté mais je veux éviter un format propriétaire
- ☐ J'ai des besoins spécifiques à mon organisation (modèle, authentification, workflow, etc.)
- ☐ J'ai besoin d'une solution qui m'aide sans m'imposer une méthodologie spécifique
- ☐ J'aimerais inclure plusieurs utilisateurs tout en maitrisant mes coûts

Si vous avez coché **plus de deux** cases, la solution **Mira** pourrait vous aider !



Centrée sur la donnée
et la productivité



Déployable en mode
cloud ou sur site



Personalisable
et évolutive sur mesure

Offre gratuite FREE
pour les acteurs de la santé et de l'éducation

intuitem
disruptive simplicity

8 rue des Frères Caudron, Vélizy 78140, France | https://intuitem.com/mira

Cybersécurité industrielle : vers une convergence IT / OT ?

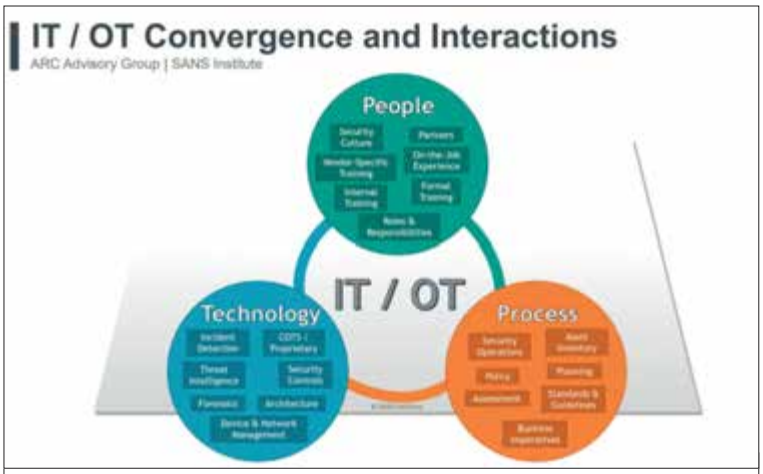
La cybersécurité des installations industrielles est un enjeu capital tant du point de vue économique que de sécurité du personnel. Les industriels en prennent conscience, mais les synergies avec la cybersécurité IT restent rares.

Par Alain Clapaud

Qu'il s'agisse de « simples » ransomwares qui obligent les sites industriels à fonctionner en mode papier ou des attaques très élaborées visant à détruire une installation ou immobiliser un réseau de distribution d'énergie, l'industrie est désormais une cible à haute valeur ajoutée pour les attaquants. Or ceux-ci disposent d'un atout maître dans leur manche : l'Industrie 4.0, avec des installations industrielles de plus en plus connectées. 1 Cette problématique de la sécurité OT (Operational Technology) n'est pas nouvelle : la Loi de Programmation Militaire de 2013 a contraint les industriels classés OIV (Opérateurs d'Importance Vitale) à accroître le niveau de sécurité de leurs installations critiques et les directives NIS et NIS 2 ont élargi le nombre d'industriels concernés avec les OSE (Opérateurs de Services Essentiels). De facto, l'aspect réglementaire a porté l'essor du marché de la cybersécurité OT : Firewall, sondes, antivirus adaptés, les éditeurs spécialisés puis les grands éditeurs se sont positionnés sur une niche de marché en expansion rapide. Le cabinet d'études MarketsandMarkets(1) l'estime à 15,5 milliards de dollars au niveau mondial pour cette année. Il sera de 32,4 milliards de dollars en 2027, soit une croissance annuelle proche de 16%. Si les grands industriels, cible de choix pour les attaquants, doivent continuer à investir pour muscler encore leur posture de sécurité, c'est du côté des ETI que beaucoup reste à faire. Les difficultés sont nombreuses : Outre une capacité de financement limitée par le faible niveau de marge des industriels, il est souvent complexe de déployer des solutions et de patcher des logiciels sur des installations dont les périodes d'arrêt sont très limitées. 2



1 La prise de conscience des industriels vis-à-vis du risque cyber reste partielle. Beaucoup doit encore être fait du côté des ETI notamment. (Source : « SANS 2019 State of OT/ICS Cybersecurity Survey », SANS Institute, 2021)



2 Outre le volet technique, le rapprochement entre l'IT et l'OT passera par de gros efforts en termes humains et dans la mise en place de processus adaptés aux contraintes de chaque camp. (Source : ARC Advisory Group/SANS Institute, 2021)

Pour de nombreux offreurs de solutions, l'heure est à la convergence entre IT et OT. Un SOC commun devra être capable de gérer les alertes issues des systèmes bureautiques, mais aussi des systèmes de production. Reste que la sécurité des installations industrielles est du ressort des directions industrielles et il existe des différences culturelles majeures entre ces deux mondes. L'action de la DSI vise avant tout à la protection des données et le traitement rapide des incidents de sécurité pour éviter toute propagation de l'attaque. Pour l'industriel, la priorité numéro 1 est la résilience : la production doit continuer coûte que coûte. Les équipements sont durcis, redondés autant que possible pour que la production puisse se poursuivre et expliquer à un responsable de production qu'il doit stopper ses machines pour patcher quelques ordinateurs en raison d'une attaque informatique qui pourrait se produire à tout d'une gageure… Plus qu'une convergence technique, c'est avant tout une compréhension des enjeux des deux camps qui va s'avérer nécessaire pour mutualiser les moyens et générer les synergies nécessaires à la compétitivité d'un industriel. ■

AC

(1) « Operational Technology (OT) Security Market », MarketsandMarkets, Juillet 2022

Fiches Sociétés

Fournisseurs

Qui fait quoi ?

Une sélection de 80 entreprises incontournables, spécialistes de cybersécurité. Leaders ou challengers, ils sont éditeurs, prestataires, hébergeurs, distributeurs ou formateurs.

Sociétés		Solutions	Services	Conseil	Formation	Distribution
6CURE	p.45	●				
ABBAKAN	p.46	●				●
ACCEIS	p.48			●	●	
Groupe ACESI	p.49		●	●	●	
ACRONIS	p.50	●				
ALGOSECURE	p.51	●	●	●	●	
ADVENS	p.52		●	●		
ALLISTIC	p.54		●	●	●	
ARMIS	p.55	●				
ALMOND	p.56			●	●	
ATEMPO	p.58	●				
AVAST BUSINESS	p.59	●				
AVANT DE CLIQUER	p.60	●				
BOARD OF CYBER	p.62	●				
BITDEFENDER	p.64	●				
CHAMBERSIGN France	p.65	●	●			
CONSCIO TECHNOLOGIES	p.66	●			●	
CyberRes (Microfocus)	p.67	●				
CS NOVIDY'S (CS GROUP)	p.68	●	●	●		
EGE (Ecole de Guerre Economique)	p.70				●	
EIFFAGE Energie Systèmes	p.73		●	●	●	
ESET	p.74	●				
FORTINET	p.76	●	●			
GATEWATCHER	p.78	●				
GLIMPS	p.80	●				
HEADMIND PARTNERS	p.81			●		
HELPSYSTEMS	p.83	●				
HOLISEUM	p.84	●	●	●		
HS2	p.86				●	
ILLUMIO	p.88	●				
INFOCLIP	p.89	●	●	●		

Sociétés		Solutions	Services	Conseil	Formation	Distribution
IN GROUPE	p.90	●				
I-TRACING	p.92		●	●		
ITRUST	p.94	●	●			
KASPERSKY	p.96	●				
KEYSIGHT TECHNOLOGIES	p.98	●				
KUDELSKI SECURITY	p.100	●	●	●		
LUXTRUST	p.101	●	●			
LASTPASS	p.102	●				
MAKE IT SAFE	p.104	●	●	●		
MENAYA	p.107	●				
METSYS	p.108		●	●		
MIEL	p.110				●	●
NAMESHIELD	p.112	●	●	●		
NEOWAVE	p.114	●				
NOZOMI NETWORKS	P.115	●				
OODRIVE	p.116	●				
OPENTEXT SECURITY SOLUTIONS	p.118	●				
PARSEC (SCILLE)	p.120	●	●			
PALO ALTO NETWORKS	p.121	●	●	●		
QUALYS TECHNOLOGIES	p.122	●				
QUERY INFORMATIQUE	p.123	●				
RUBYCAT	p.124	●				
SAILPOINT TECHNOLOGIES	p.126	●	●	●		
SANS INSTITUTE	p.128				●	
SCASSI Cybersecurity GROUP	p.130	●		●	●	
SECKIOT	p.132	●				
SECUSERVE	p.134	●				
SERMA SAFETY & SECURITY	p.137	●	●	●		
SIEMENS	p.138	●	●			
STORMSHIELD	p,139	●				
SYSDREAM (HUB ONE)	p.140		●			
SYSTEMIS	p.142	●		●		
SYNETIS	p.144		●	●	●	
THALES	p.145	●				
TIXEO	p.146	●				
UBIKA	p.147	●	●	●		
WALLIX	p.148	●				
WITHSECURE	p.150	●				
YESWEHACK	p.152	●				

Annonceurs Publicité

LES ASSISES	p.6
BT BLUE	p.15
DOCAPOSTE	p.11
HS2	p.37
IN GROUPE	4e couverture
INTUITEM	p.41
KASPERSKY	2e couverture
MICROPOLE	p.23
3 DS OUTSCALE	p.19
PRADEO	p.5

Notre métier : la protection de vos infrastructures réseaux et de vos DNS

6cure est une société innovante, spécialisée dans la sécurité des systèmes d'information, et reconnue pour ses activités de R&D dans le domaine des systèmes de détection d'intrusion et de réaction contre les cyberattaques. 6cure fournit des solutions pour la défense active contre les attaques DDoS sur les systèmes et réseaux d'information pour garantir la disponibilité et la qualité des services de ses clients. Ces solutions sont de nature à répondre aux problématiques des acteurs de l'internet que ce soit pour leurs propres besoins ou pour offrir un service à valeur ajoutée à leurs clients.



Société : 6CURE
Adresse : 701, rue Léon Foucault
14200 Hérouville Saint Clair
Tel : 09 71 16 21 50
Mail : **contact@6cure.com**
Site Web : **www.6cure.com**

Spécialisations :

- **Détection/Réaction/Mitigation des attaques DDoS**
- **Protection des infrastructures DNS**
- **Audit DDoS**

Chiffres clés :

Effectifs : 20-25

Historique :

Création : 2010



Dirigeant
Fabrice CLERC
CEO

Contacts
Direction Commerciale
sales@6cure.com

Direction Technique
ddos-mitigate@6cure.com



Produits / Services

Protection anti-DDoS

6cure Threat Protection® s'appuie sur une logique algorithmique brevetée, permettant d'identifier et de filtrer en temps réel les attaques DDoS les plus complexes, jusqu'au niveau applicatif, et ainsi de préserver l'intégrité et la performance des flux légitimes. Elle s'intègre nativement dans une architecture de protection sur site, en amont (niveau opérateur ou cloud) ou hybride.

Sécurité DNS

6cure DNS Protection® est une solution de sécurité DNS « tout-en-un », qui permet de garantir la disponibilité et la qualité de service, de manière totalement transparente et agnostique, d'offrir une visibilité complète de la menace aux équipes opérationnelles et de fournir des services à valeur ajoutée pour les utilisateurs et les clients. Elle garantit la disponibilité et la performance des infrastructures DNS, grâce aux fonctions embarquées de protection contre le DDoS et les amplifications, l'empoisonnement de cache, et les attaques applicatives. Elle assure également une protection temps réel, transparente et supervisée des services DNS, offrant une visibilité précoce et le moyen de réaction le plus rapide face à des menaces d'infections, l'exfiltration de données par des canaux cachés, ou la fuite d'informations indésirables.

Audit DDoS

DDoS Assessment permet d'évaluer la résilience des infrastructures réseau et services face à la menace DDoS dans un contexte maîtrisé. Notre expertise DDoS et notre plate-forme de test est à votre service pour réaliser un audit de vos moyens humains et techniques de protection pour une analyse de risques complète.

Certifications

Label France Cyber Sécurité
Label ECSO
Référencement : Fournisseur OTAN

Références Clients

Opérateurs Télécom, FAI, Hébergeurs en France, DROM, à Monaco, en Afrique du Nord et en Afrique de l'Ouest ;
OIV OSE
Organismes publics, soit directement, soit via un réseau de partenaires…

abbakan
an Ingram Micro Company

INGRAM MICRO



Quelle visibilité pour lutter contre l'augmentation de votre surface d'attaque ?

Scannez ce QR Code pour retrouver nos éditeurs partenaires :

www.abbakan.com

ARMIS

Avec sa solution de Cyber Asset Management et de Sécurité des devices non managés, sans agent, Armis fournit :

- ✓ Un inventaire complet des actifs, et monitoring de leurs activités,
- ✓ Une analyse des vulnérabilités et facteurs de risques,
- ✓ Une détection des menaces et réponses automatisées grâce à des intégrations tierces.

Attack Surface Management solution 100% Cloud en mode SAAS sans agent, détecte et analyse les ressources Internet dans les environnements dynamiques, distribués et partagés d'aujourd'hui. Cette solution fournit une visibilité complète sur votre surface d'attaque, évalue les risques et les vulnérabilités.

GROUP-IB

ProHacKtive
CYBER SERENITY

Solution 100% française proposant le premier auditeur cyber automatisé plug&play, la solution ProHaktive offre :

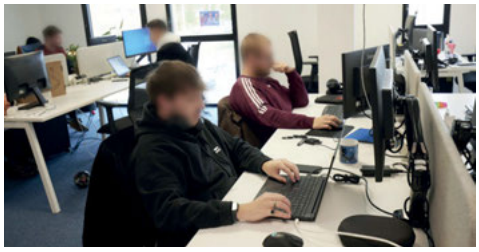
- ✓ Un audit complet et permanent de tous les appareils,
- ✓ Des données sensibles uniquement accessibles en local,
- ✓ Une interface synthétique et intuitive.

Jizô NDR détecte les menaces là où c'est le plus pertinent :
au coeur de votre réseau, avant même qu'elle atteigne vos endpoints. La détection s'opère en temps réel, avec des capacités d'analyse uniques sur le marché. Elle s'opère grâce au meilleur des moteurs de détection, IT ou OT, appuyés par de l'intelligence artificielle. **Visa de sécurité ANSSI pour sa qualification élémentaire en juin 2021.**

Sesame it

acceis
Centre d'expertises en cybersécurité

Pour la sécurisation réussie de vos activités



Créé à Rennes en 2015, ACCEIS est doté du visa de sécurité de l'ANSSI. ACCEIS possède l'agrément CESTI software et la qualification PASSI.

Pour asseoir sa notoriété et déployer son offre, ACCEIS centre d'expertises en cybersécurité, a ouvert une antenne à Paris en 2022. Son équipe d'experts pluridisciplinaires passionnés vous propose un accompagnement sur-mesure, complet qui se décline en trois grandes activités complémentaires : audits, accompagnement et conseil, études et évaluations.

Société : ACCEIS
Adresse : 12 rue du Bourg-Nouveau, 35000 RENNES
Tel : 06 64 59 15 50
Mail : christophe@acceis.fr
Site Web : www.acceis.fr

Spécialisations :

Audits techniques, accompagnement et conseil, gestion des incidents de sécurité, certification, gouvernance. L'équipe d'experts pluridisciplinaires en cybersécurité d'ACCEIS est capable d'intervenir à la fois sur des missions techniques exigeantes comme sur des sujets organisationnels et stratégiques à forts enjeux.

Chiffres clés :

CA : 2022 : 2 M€
2021 : 1,2 M€
Effectifs : 30, en pleine croissance.
Siège à Rennes et agence à Paris.

Dirigeants



Gwenn FEUNTEUN
Président, co-fondateur

Yves DUCHESNE
Directeur Général, co-fondateur

Christophe BEUCHARD
Directeur Commercial & Marketing Associé

Contact
Christophe BEUCHARD
Directeur Commercial & Marketing Associé
christophe@acceis.fr
06 64 59 15 50

Un **accompagnement global** pour vos projets de **cybersécurité**.

- **AUDITER** votre système d'information
- **RÉAGIR** face à un incident de sécurité
- **ÊTRE CONSEILLÉ** en cybersécurité
- **ÉVALUER** votre produit pour obtenir une certification CSPN
- **OBTENIR** une certification de services (iso 27001, hds,...)
- **FORMER** et sensibiliser vos équipes

ACCEIS a pour objectif d'accompagner de façon globale ses clients à la sécurisation de leurs activités en leur apportant les compétences hautement qualifiées grâce son équipe d'experts.

Intervenant sur le territoire national et à l'étranger, ACCEIS est impliqué auprès de tous secteurs d'activités, avec une présence marquée dans les domaines de l'industrie, de la santé, des services numériques et les institutionnels.

Qualification PASSI

VISA DE SÉCURITÉ — ANSSI

ACCEIS bénéficie de la reconnaissance des plus hautes instance étatiques. ACCEIS est prestataire qualifié par l'ANSSI pour la réalisation d'audits de sécurité des systèmes d'information (PASSI RGS), sur l'ensemble des portées proposées par le référentiel (tests d'intrusion, audits de code source, audits de configuration, audits d'architecture, audits organisationnels et physiques).

Cette qualification lui permet également d'intervenir sur des marchés réglementés.

Agrément CESTI

SÉCURITÉ CERTIFICATION

ACCEIS dispose également de l'agrément CESTI (Centre d'évaluation de la sécurité des technologies de l'information) délivré par l'ANSSI.

L'ANSSI s'appuie sur notre rapport d'évaluation pour délivrer une Certification de Sécurité de Premier Niveau (CSPN), permettant aux éditeurs et industriels d'attester du bon niveau de sécurité des produits et logiciels qu'ils développent et commercialisent.

Qualification PASSI LPM

ACCEIS a amorcé sa qualification PASSI LPM - Loi de Programmation Militaire.

Références Clients

ALE International, AriadNEXT, Biocoop, Bodet Software, Bouygues, Centre Hospitalier de Troyes, DGFIP, Eiffage, Euro-Information, Foliateam, Groupe Le Duff, Gruau, MV Group, Nehs Digital, Orolia, Ouest-France, PAPREC France, Roojaï Service Indonesia, Santélys, SERVIER MONDE, Shadow, SIB, SNEF, Softway Medical, TINGARI,...

GROUPE acesi

Conseil, intégration, services : La cybersécurité au cœur de votre stratégie informatique



Fondé en 2004, le groupe ACESI propose des services à fortes valeurs ajoutées et s'est spécialisé au fil des années dans les domaines de la cybersécurité et des infrastructures informatiques. Associés à une expertise de pointe, ses différents métiers lui permettent aujourd'hui de couvrir très largement l'ensemble des besoins informatiques des entreprises. Le groupe a lancé en 2021 un programme ambitieux ayant pour objectif de devenir le partenaire référent Cybersécurité du grand quart Nord-Est de la France et a fait l'acquisition en 2022 de la société lilloise Yourax qui devient ainsi le label cybersécurité du groupe. Avec son siège basé à Strasbourg, le groupe s'appuie sur 5 autres agences implantées à Bâle-Mulhouse, Besançon, Reims, Lille et Genève (Suisse).

Société : GROUPE ACESI
Adresse : Aeroparc 1, 8B rue Icare 67960 ENTZHEIM

Nom des marques :

VITA *VITA, offre de services managés*

yourax by acesi *Yourax by ACESI, label cybersécurité*

Tél : +33(0)3 90 64 80 00
Mail : **contact@ace-si.com**
Site Web : **www.ace-si.com**

Spécialisations :

Conseil sécurité, conformité RGPD, audit de contrôle, sécurisation de l'environnement utilisateur, infogérance, infrastructure, services Cloud, Télécoms & Réseaux

Chiffres clés :

CA : 22M€ de CA en 2021
6 agences
Effectifs : 130 collaborateurs

Historique

2004 : création d'ACESI France
2005 : création d'ACESI Suisse
2006 : création de VITA
2022 : rachat de Yourax It Security

Offres

- Conseil & Stratégie : direction de projets, audits, formation & sensibilisation, RGPD et conformité, gestion des risques, PSSI, externalisation DPO, RSI, DSI, etc.
- Infrastructure : virtualisation, PRA/PCA, sauvegarde, infrastructure hyperconvergée, hébergement, etc.
- Cybersécurité : gestion des vulnérabilités, gestion des droits et gouvernance de la donnée, sécurisation des postes de travail, outils collaboratifs, messagerie, sécurisation des flux et applications cloud, phishing, pentests, réponse à incidents, etc.
- Services Cloud : IAAS, SAAS, cloud privé, cloud hybride, cloud public, etc.
- Réseaux & Télécoms : intégration de projets LAN, WAN, Wifi, SD-Wan, gestion de la mobilité, internet sécurisé, ADSL, SDSL, fibre optique.

Yourax, la référence cybersécurité

L'offre Cybersécurité du Groupe ACESI propose une expertise haut de gamme permettant de mettre en place une politique de sécurité et des solutions techniques parfaitement adaptées. Le label cybersécurité Yourax est garant de la qualité de la démarche et se déploie sur l'ensemble des agences du groupe.

VITA, le service managé by ACESI

En 2006, ACESI crée VITA et permet aux entreprises d'externaliser partiellement ou en intégralité l'exploitation quotidienne de leur système d'information. Grâce à une expérience historique dans ce domaine et à de nombreuses références, le groupe propose une offre garantissant le respect des niveaux de services indiqués sur ses Plans d'Assurance Qualité, tout en gardant la souplesse nécessaire pour s'adapter à chacun des contextes clients.

Certifications

- Yourax by ACESI : prestataire référencé sur Cybermalveillance et label Expert Cyber en 2021.
- Certification ISO 27001 (Service Cloud : certification en cours) / Consultants certifiés Lead Auditor – Lead Implementor / Risks Manager

Points Forts

- Fort engagement RSE
- Création de VIT'EA en 2021 : entreprise adaptée permettant l'emploi de salariés en situation de handicap.

« Notre entreprise se caractérise par les valeurs fortes qui animent l'ensemble des collaborateurs. Vision long terme, expertise de pointe, respect, démarche responsable. Nos clients sont au centre de tous nos intérêts et notre objectif est de mettre en place une relation de confiance pour un partenariat long terme »

Jean-Marc PATOURET,
co-dirigeant du Groupe ACESI.

Dirigeants



Jean-Marc PATOURET
co-dirigeant
jmpatouret@ace-si.com



Manuel KIENTZY
co-dirigeant
mkientzy@ace-si.com



Jean-Michel VALY
co-dirigeant
jmvaly@ace-si.com

Contacts

Romain ZUCKER
Directeur commercial
rzucker@ace-si.com

Mickael RUVIO
Directeur des opérations Yourax
mruvio@ace-si.com

Acronis, société suisse, leader mondial de la cyberprotection

Société : ACRONIS
Adresse : 105 Rue Anatole France, 92300 Levallois-Perret
Tel : 01 86 26 54 51
Mail : **sales_fr@acronis.com**
Site web : **https://www.acronis.com/fr-fr/**

Acronis unifie la protection des données et la cybersécurité pour délivrer une approche de cyberprotection intégrée et automatisée réunissant les conditions SAPAS de fiabilité des données, d'accessibilité, de confidentialité, d'authenticité et de sécurité. Par ses modèles de déploiement flexibles adaptés au fonctionnement des fournisseurs de services et des professionnels IT, Acronis garantit la cyber protection supérieure des données, applications et systèmes avec des solutions antivirus de nouvelle génération, de sauvegarde, de reprise après sinistre et de gestion de la protection des terminaux à base d'IA. Grâce à un antimalware avancé piloté par une intelligence artificielle de pointe et à ses technologies primées d'authentification par la blockchain, Acronis protège n'importe quel environnement, cloud, hybride, sur site, pour un coût prévisible et abordable.

Spécialisations :

Cyber Protection, Solutions de sauvegarde et protection de la donnée, Cyber Sécurité

Chiffres clés :

- *Croissance annuelle de 77 % du chiffre d'affaires cloud d'Acronis*
- *Effectifs : plus de 2000 employés dans le monde, 30 employés pour le territoire Français*
- *3.5 milliards la valeur de marché*
- *250 millions de dollars d'investissement en 2021*
- *250 millions de dollars d'investissement en 2022*

Dirigeants



Patrick Pulvermueller
CEO depuis 2021
https://www.linkedin.com/in/patrickpulvermueller/



Samy Reguieg
Managing Director France

Titulaire d'un exécutive MBA à HEC Paris, Samy Reguieg occupe depuis plus de 5 années, le poste de Directeur Général France. Avec plus de 15 années d'expérience dans l'informatique et particulièrement chez les éditeurs de logiciels, Samy Reguieg a en effet rejoint la société Acronis en 2011 au poste de Corporate Account Manager où il était en charge des clients finaux. Aujourd'hui il supervise, toutes les activités commerciales, marketing et channel sur le Territoire , plus particulièrement les opérations de ventes, les renouvellements de produits et abonnements, la génération de demandes, mais aussi le programme de partenariat de l'entité Française. Samy avait auparavant occupé le poste de commercial chez différents éditeurs de logiciels.

Offres :

Cybersécurité, Sauvegarde, reprise d'activité après sinistre et gestion des terminaux intégrées en une solution unique pour fournisseurs de services et entreprises.

Services :

Cloud et/ou sur site - Améliorez votre cybersécurité grâce à nos services d'évaluation des risques, de sensibilisation à la sécurité et d'intervention sur incidents.

Solutions :

Solution de cybersécurité et de protection des données intégrées - Plateforme axée MSP pour la fourniture de services de cyberprotection. Hébergée et/ou dans le Cloud.

Certifications :

Data Center Strasbourg

Références Clients :

Sanofi / Engie / Williams Racing / LMB Martin Freres

« Chez Acronis, nous sommes passés d'une société de sauvegarde à une société de cyber sécurité. Acronis propose une gamme de solutions pour une cyber protection moderne et de nouvelle génération à la pointe de la technologie. Les solutions de cyber protection Acronis, (sauvegarde et antimalware entièrement intégrés et optimisés par l'IA), s'appuient sur les cinq vecteurs SAPAS (Safety, Accessibility, Privacy, Authenticity, Security) de la cyber protection qui apportent ainsi le plus haut degré de protection aux données, garanties infalsifiables. Acronis a une approche holistique qui combine la protection des données et la cybersécurité. Reconnu comme un visionnaire par Gartner, nous voyons cette reconnaissance comme une validation de l'interdépendance critique entre la sauvegarde et la cybersécurité. »

Samy Reguieg

Historique :

- *Fondée en 2003 à Singapour*
- *Siège social à Schaffhouse, en Suisse, depuis 2008*
- *Siège social international à Singapour*
- *Plus de 2000 employés*
- *34 sites dans le monde entier*
- *Les produits sont disponibles dans plus de 150 pays en 26 langues*
- *Plus de 20 000 MSPs utilisent les solutions Acronis*

Contacts

Nora Moumni, *Distribution Manager France*	***Christopher Géraud,*** *Partner Account Manager Cloud*	***Jérôme Carletti,*** *Partner Account Manager*	***Grégory Laroche,*** *Senior Solution Engineer*	***Samy Reguieg,*** *Managing Directeur, France*

algosecure
Keep It Safe and Secure

Société : ALGOSECURE
Adresse : 57 boulevard Marius Vivier Merle – 69003 LYON
Tél : 04 26 78 24 86
Mail : contact@algosecure.fr
Site Web : www.algosecure.fr

*Créé en 2008, AlgoSecure est un cabinet conseil **français indépendant pure player de la cybersécurité.***
*AlgoSecure accompagne les entreprises et les organismes publics dans la **sécurisation de leurs systèmes d'information** en proposant un accompagnement complet : **Évaluer – Conseiller et Sécuriser – Sensibiliser et Former – Réagir en cas d'incidents de sécurité.***

Les engagements :

- *Bénéficier d'une **forte expertise technique** avec une équipe de consultants hautement qualifiés, passionnés et bénéficiant de formations en continu.*
- *Être conseillé en toute **impartialité** par un acteur indépendant (vis-à-vis des constructeurs et éditeurs).*
- *Créer de la valeur ajoutée grâce à une **approche pragmatique et transparente.***

Spécialisations :

- **Missions offensives**
- **Missions défensives**
- **Missions RGPD**
- **Accompagnement Pack SSI**
- **Missions forfaitaires et en assistance technique/régie.**

Chiffres clés :

Effectifs : 45 collaborateurs
Date de création : 2008



Dirigeant
Hicham BEN HASSINE
Dirigeant et directeur technique d'AlgoSecure

Après plusieurs années dans la cybersécurité, Hicham a fondé AlgoSecure en 2008 avec comme objectif de sécuriser les SI tout en agissant positivement sur son écosystème. Il s'inspire notamment du fonctionnement des entreprises libérées en plaçant au centre l'humain et l'expertise technique.

Offres

ÉVALUER

Audits Techniques
- Audit d'application web (PASSI)
- Audit d'application mobile (PASSI)
- Audit interne - LAN (PASSI)
- Audit Red Team
- Audit d'infrastructure cloud
- Audit de configuration (PASSI)
- Audit d'architecture (PASSI)
- Audit de code source (PASSI)
- Audit SWIFT
- Audit système industriel
- Audit environnement IoT
- Reverse Engineering

Audits Gouvernance
- Audit de conformité RGPD
- Audit organisationnel et physique (PASSI)

PROTÉGER

Conseils Techniques
- AMOA Cybersécurité
- Supervision
- Accompagnement RGPD
- DPO externalisé
- Sécurisation Active Directory

Conseils Gouvernance
- Accompagnement PSSI
- Certification ISO 27001
- Certification HDS
- Analyse de risques
- RSSI externalisé
- Algo Centre de Compétences

RÉAGIR
- Analyse forensique
- Réponse incidents de sécurité
- AlgoCert* : Pack Sérénité

SENSIBILISER ET FORMER
- Campagne de phishing
- Sensibilisation SSI
- Formation Cybersécurité

*__AlgoCert__ : 3 formules pour anticiper, se préparer et/ou être assisté rapidement en cas d'__incidents de sécurité__.

Certifications

- Qualifié PASSI
- Certifié ISO 27001
- Expert Cybermalveillance
- CERT

Nos principaux marchés

- Energie
- Transport / Logistique
- Organismes publics
- Santé
- Industrie
- Finances
- Information / Communication

Contacts
Nancy Ly
Responsable Marketing et Communication
Nancy.ly@algosecure.fr

Service Commercial :
+33 4 26 78 24 86
commercial@algosecure.fr

Advens
Security for the greater good

Société : ADVENS
Adresse : 16 Quai de la Mégisserie, 75001 Paris
Tél : 01 84 16 30 25
Mail : contact@advens.fr
Site Web : www.advens.fr

Spécialisations :

- **SOC-as-a-Service & MDR**
- **CERT, CSIRT, CTI**
- **Gouvernance, risque, conformité**
- **Audits & Red team**
- **Intégration et management des technologies de sécurité**
- **Sécurité OT & IoT**
- **Sécurité des clouds**

Chiffres clés :

CA : 50 M€
Effectifs : 400 collaborateurs



Dirigeants
Alexandre FAYEULLE
Président
alexandre.fayeulle@advens.fr



David BUHAN
CEO
david.buhan@advens.fr

« Face à la diversité et à la professionnalisation des attaquants, il est nécessaire de faire front commun pour toujours être plus cyber résilient ! Nous le faisons aux côtés de nos clients, en protégeant leur organisation jour après jour, dans une logique de partenariat, via notre expertise globale et un service de SOC dernière génération. Nous le faisons avec tout l'écosystème au travers de nos engagements et nos initiatives pour une Cyber plus inclusive. » David Buhan, *Directeur Général, Advens*

Cybersécurité. Impact. Collectif.

Advens est un leader français de la Cybersécurité, indépendant et souverain. Nos 400 experts sont présents partout en France, ainsi qu'à Montréal et prochainement en Europe. Notre mission : protéger les organisations publiques et privées, toujours plus dépendantes du numérique et toujours plus exposées à des attaquants de plus en plus professionnels.
Cette mission de protection nous guide et nous anime au quotidien. Mais elle ne nous suffit pas. Si la cybersécurité permet de faire tourner le monde, notre performance doit participer à le changer. Notre croissance s'accompagne d'un partage de la valeur au service de cette ambition sociétale. Pour la financer, jusqu'à 40% de notre valeur financière sera redistribuée au fonds de dotation Advens for People & Planet, qui accompagne des initiatives à impact, en faveur de l'inclusion sociale, de l'éducation et de l'environnement.

Offres

- **mySOC** : SOC-as-a-service et service de détection et de réaction 24/7 pour tous les environnements
- **CISO Office :** Centre de services Cyber à 360° et à la demande
- **myCERT :** Réponse à incident, gestion de crise et analyse de la menace

Services

- **Risques & Stratégie :** Gouvernance, maitrise de risques et animation de la filière Cyber, sensibilisation
- **Conformité Cyber :** Maitrise des exigences externes (RGPD, HDS, ISO27001, LPM, NIS, etc.)
- **Sécurité offensive :** Audit, tests d'intrusion et red team
- **Technologies de sécurité :** Intégration et management des technologies de sécurité
- **Cyber OT :** Protection des environnements industriels
- **Sécurité des clouds :** Maitrise de l'externalisation et sécurisation des clouds publics et privées

Projets

Outre ses ambitions dans la cybersécurité Advens a un projet d'entreprise fort, qui a mené à la création d'un fonds de dotation, en faveur de l'inclusion sociale, de l'éducation et de l'environnement. Les premiers projets du fonds portent sur l'inclusion dans la Cyber (via un partenariat avec Microsoft et Simplon), l'accompagnement Cyber des ONG et des acteurs de l'ESS et des actions de sensibilisation à destination des jeunes. Cela a été initié avec le sponsoring sportif et le soutien au projet LinkedOut.

Certifications

La société est qualifiée PASSI et PASSI LPM. Nous avons également initié une démarche pour le PDIS et pour le PRIS.

Références Clients

AG2R La Mondiale, AMF, AP-HM, AP-HP, Auchan, CAIH, Danone, Decathlon, Doctolib, EFS, HCL, Ile de France Mobilités, Ingredia, Intech, Malakoff Humanis, Mediametrie, Oodrive, Sodebo, Systeme U, Tessi, TF1, UGAP, Vinci, Wakam…



Contacts
Benjamin LEROUX
CMO
benjamin.leroux@advens.fr,
03 20 68 41 81

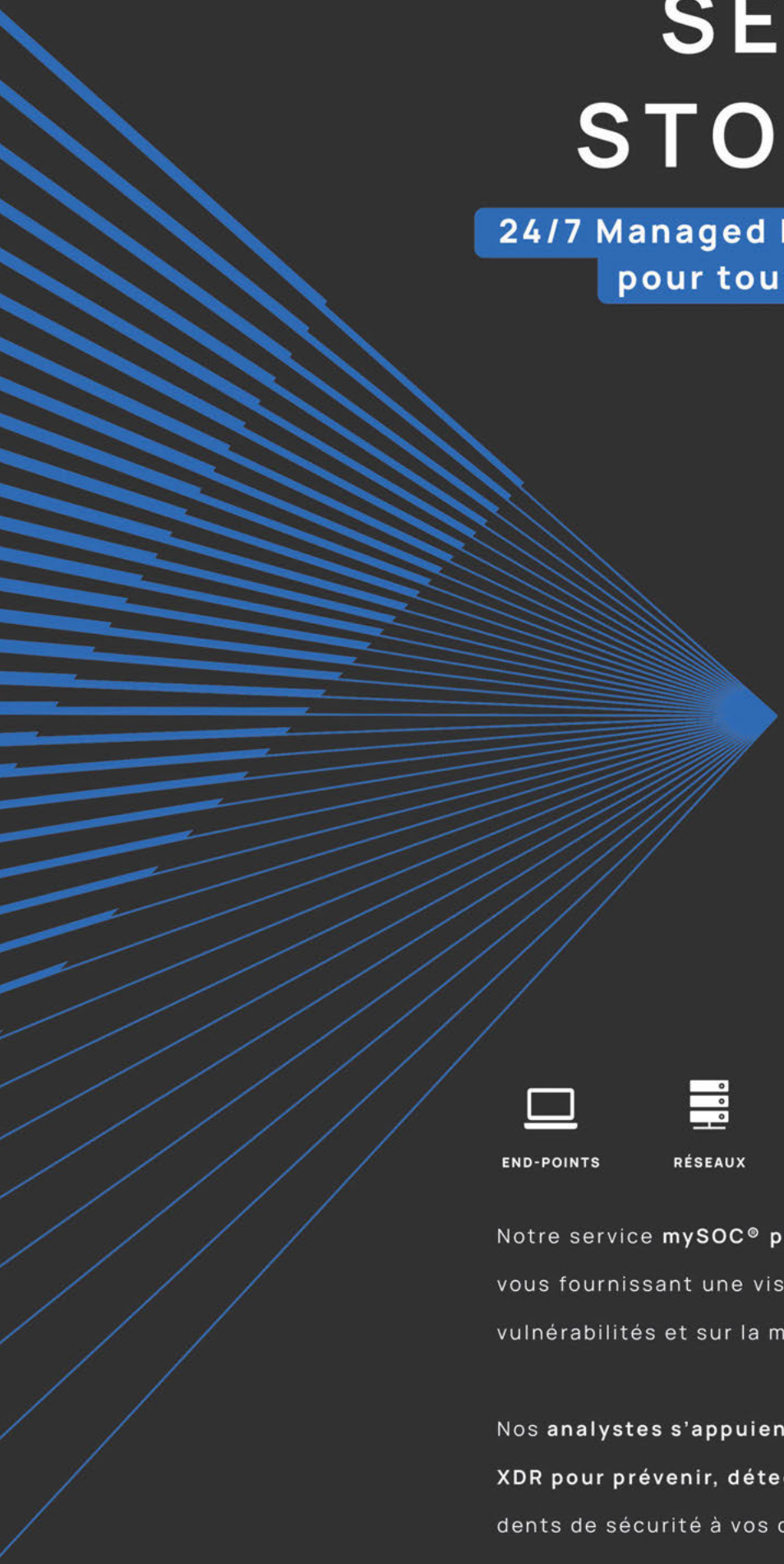
Historique :

Créé en 2000 à Lille, Advens s'est vite déployé en France, à Paris en 2010 puis partout sur l'hexagone - et désormais au Quebec. En 2016 Advens lance mySOC, son offre de SOC externalisé de nouvelle génération. En 2019 Advens est retenu par le ministère des armées au sein d'un consortium de PME d'excellence. Et en 2020 l'UGAP confie à Advens son marché de prestations de services. Advens protège désormais plusieurs centaines de clients publics et privés.

En 2017 la société a commencé à soutenir Thomas Ruyant, skipper professionnel, en cherchant à allier sponsoring sportif et impact. Cette initiative a été accélérée en 2020 avec le choix de soutenir LinkedOut, en faveur du retour à l'emploi. En 2021 Advens crée le fonds de dotation Advens For People & Planet pour concrétiser l'ambition sociétale de son projet d'entreprise.

SEE MORE.
STOP MORE.

24/7 Managed Detection & Response pour tous vos environnements



mySOC®
by ADvens



Notre service **mySOC® protège tous vos environnements** en vous fournissant une visibilité complète sur vos risques, vos vulnérabilités et sur la menace externe.

Nos **analystes s'appuient sur notre plateforme mySOC Open XDR pour prévenir, détecter et réagi**r en temps réel aux incidents de sécurité à vos côtés.

Découvrez nos services sur **www.advens.fr**

allistic

Société : ALLISTIC

Lille :
165 Avenue de Bretagne,
59000 LILLE
Tel : 03 74 09 61 00

Paris :
24 rue Louis Blanc
75010 PARIS
Tel : 01 88 336 336

Mail : **contact@allistic.fr**
Site web : **https://www.allistic.fr/**



Spécialisations :

- **Gouvernance, Risques et Conformité**
- **Sécurité Opérationnelle**
- **Sensibilisation et Formation**

Historique :

Créée en 2018, Allistic compte plus d'une vingtaine de collaborateurs qui cumulent savoir-être et savoir-faire pour améliorer votre cybersécurité.



Dirigeant
Jean-Michel DOS SANTOS
Fondateur et dirigeant
jmdossantos@allistic.fr

« La meilleure protection pour une entreprise est celle qui tient compte de son contexte et de ses enjeux. C'est la raison d'être d'Allistic. En abordant la problématique de la protection de l'entreprise dans sa globalité, Allistic permet à ses clients d'aligner les investissements et les efforts sur une ambition de sécurité.

Nous avons constitué une équipe disposant des compétences nécessaires à la prise en charge des problématiques de cybersécurité pour les entreprises et collectivités. »

Partant du constat que la meilleure protection pour une entreprise est celle qui tient compte de son contexte et de ses enjeux, Allistic accompagne les sociétés et collectivités dans leur transformation digitale en répondant à leurs enjeux de sécurisation.

Offres

Risques et Conformité

Soyez accompagné dans la définition de votre stratégie cybersécurité et dans sa mise en oeuvre.

- **RSSI On-Demand :**

Nous accompagnons nos clients à atteindre un niveau cybersécurité adapté à votre business model.

- **Audit organisationnel et accompagnement aux certifications :**

Nous vous accompagnons dans l'évaluation et l'atteinte de certifications cyber : ISO27001, PCI-DSS, HDS, RGPD, etc.

- **Gestion des risques :**

Nous vous accompagnons dans l'identification, la remédiation et la mise en place de référentiels vous permettant d'accroître la résilience de votre structure.

Sensibilisation et Formation

Aidez vos collaborateurs à comprendre les enjeux de cybersécurité et adoptez les bons réflexes.

- **Solutions intra-entreprise**
- **E-learning**

Sécurité Opérationnelle

Soyez accompagné dans l'élaboration d'une défense contre les cyberattaques et risques SI.

- **Conseil en architecture sécurisée :**

Nous vous accompagnons dans le design, le déploiement ou l'évaluation de la sécurité de vos architectures IT.

- **Intégration et management de solutions de sécurité :**

Nous intégrons les solutions de cybersécurité les plus adaptées à votre SI afin d'améliorer sa robustesse, sa résilience et son pilotage.

- **Audits techniques et Pentests :**

Nous évaluons vos différents périmètres techniques pour vous proposer les meilleurs remédiations possibles :

- Test d'intrusions interne / externe
- Audit d'applications, web
- Audit de configuration, Audit de code
- Red Team (Phishing, Vishing, Intrusions physique, etc.)

PROFESSIONNEL RÉFÉRENCÉ
CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

CAMPUS CYBER
ACTEUR ENGAGÉ

Pour en savoir plus :

Société : ARMIS

Mail : **sales-france@armis.com**
Site Web : **www.armis.com**

Spécialisations :

- **Inventaire des actifs gérés et non gérés IoT, OT, BioMed, ICS, IT**
- **Analyse des vulnérabilités et Gestion des risques avec hiérarchisation des priorités**
- **Remédiation**

Chiffres clés :

40 entreprises du Fortune 100 font confiance à ARMIS

Plus de 2 Milliards d'actifs suivis

Effectifs : 750 personnes dont 14 en France



Dirigeants
Jean-Michel TAVERNIER
Directeur régional
jeanmichel.t@armis.com
+33 06 04 11 11 06



Mathieu RICHARD
responsable du réseau partenaires
mathieu.richard@armis.com
+33 06 73 83 00 75

La plateforme de sécurité Armis® Asset Intelligence offre un inventaire unifié de tous les actifs d'une organisation, et permet trois capacités importantes :

1 Un inventaire complet et unifié des actifs, qui fait autorité, et qui corrèle les informations clés des nombreuses solutions technologiques existantes. Identifiez et classez chaque appareil, y compris l'informatique, l'IoT, l'OT, l'IoMT, le cloud et le cellulaire-IoT, géré ou non-géré.

- Améliore le temps et la précision de l'audit des actifs.
- Réduit les heures-personnes
- Réduit les problèmes de non-conformité
- Fait évoluer les contrôles 1 et 2 basés sur l'inventaire CIS
- Permet de synchroniser la CMDB

2 Évaluation des vulnérabilités et des risques et hiérarchisation des priorités : Effectuez une analyse des vulnérabilités et des risques sur chaque actif pour aider à identifier, hiérarchiser et gérer les risques pour votre organisation.

- En temps réel et en continu.
- Réduit l'impact des incidents de sécurité en améliorant la posture de sécurité.
- Identifie les dettes techniques* dans le matériel, les OS et les applications.
- Accroît la valeur des investissements en matière de sécurité tels que l'EDR, l'évaluation des vulnérabilités et l'ITAM.
- Diminue les frais opérationnels lors du traitement des risques, des vulnérabilités et des incidents. Supprime les fichiers Excel.

3 Intelligence décisionnelle et automatisée : Menez un programme d'amélioration continue en utilisant des actions basées sur des politiques pour générer des tickets, prendre des mesures correctives ou déclencher des contrôles compensatoires dans les produits de sécurité ou informatiques existants. La plateforme Armis applique les politiques avec des actions automatisées qui peuvent :

- Bloquer ou mettre en quarantaine les actifs à risque avec des contrôleurs WiFi ou des NAC.
- Réconcilier les données relatives aux actifs dans les solutions ITAM
- Actionner les scans via l'évaluation des vulnérabilités technologiques
- Générer des alertes vers les SIEM
- Déléguer des activités via ITSM

Quels sont les problèmes clients résolus par Armis ?

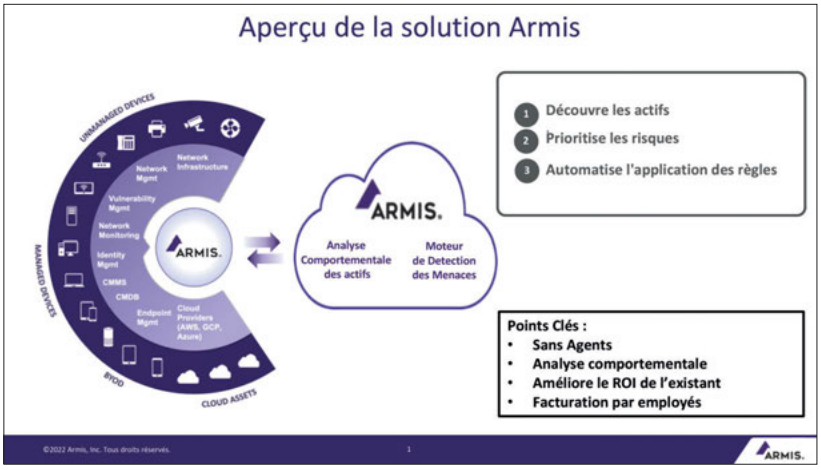
- Absence d'un inventaire centralisé faisant autorité de leurs actifs et des attributs de sécurité associés.
- Difficulté à identifier les scénarios à risque ou de non-conformité.
- Difficultés à faire face à la vélocité des vulnérabilités et à comprendre le contexte et l'impact métier des CVE.
- Impossibilité d'identifier avec précision la dette technique* dans l'ensemble de l'organisation.

Points Forts

- Source unique de confiance des actifs
- Analyse comportementale des actifs
- 100% Sans agent
- 100% passif : Aucun impact réseau. Pas de scanning des actifs
- Facile à déployer : en quelques minutes en utilisant l'infrastructure existante.
- Plateforme SaaS : Retour sur investissement en quelques heures, pas en semaines ou en mois.
- La plus grande base de connaissances d'actifs au monde, plus de 2 milliards d'actifs par jour.

Références Clients

Colgate Palmolive, Allegro Microsystems, Takeda Pharmaceuticals, Mondelez, PepsiCo, DocuSign, le Groupe Booking, et bien d'autres.



** dette technique : Suivi du Cycle de vie des produits, de façon à maintenir le parc des actifs à jour et opérationnel. La dette technique étant le retard de maintenance et de mise à jour*

almond

Société : Almond
Adresse : Bâtiment CRISCO DUO
7 avenue de la Cristallerie
92310 Sèvres
Tel : 01 46 48 26 00
Mail : **contact@almond.consulting**
Site web : **https://almond.consulting**

Spécialisations :

Audits de sécurité :
Tests d'Intrusion, Audits de code source, Audits de configurations, Audits d'architecture, Audits de sécurité physique et organisationnelle, Social engineering, Forensic

SOC / CERT CWATCH :
Réponse à incidents de sécurité, Services managés de détection d'incidents, Scan et gestion de vulnérabilités, Threat intelligence Conseil et audit en organisation du SOC / C-SIRT, certification PCI Forensic Investigator

Sécurité des infrastructures :
Architecture sécurité et réseau : hébergement, accès internet, défense en profondeur, Gestion des identités et des accès (IAM et IDaaS), Contrôle et sécurisation des applications SaaS, Sécurisation des terminaux dans toutes les situations de mobilité

Accompagnement RSSI – analyse de risques – sensibilisation – gouvernance de la sécurité – résilience – gestion de crise – certification PCI DSS – ANJ – conformité ISO27001 – HDS – RGPD – LPM – RGS – SWIFT

Chiffres clés :

CA 2021: 26,3M€
Effectifs : 200 collaborateurs
Paris, Nantes, Strasbourg, Lyon, Genève

Almond est un acteur majeur français indépendant de l'audit et du conseil, en cybersécurité, cloud et infrastructures. De l'innovation technologique à la modernisation du Système d'Information, sa mission est d'accélérer l'évolution de ses clients en apportant une vision stratégique pragmatique. Almond les accompagne sur toutes les phases de leurs projets, de la définition de la stratégie IT et métier jusqu'à la mise en œuvre de plans de transformation et l'intégration de solutions. Les équipes Almond développent pour chaque client une approche sur-mesure et garantissent un total engagement pour la réussite de leurs projets.

Offres

Almond est un des acteurs majeurs de la sécurité en France, en accompagnant ses clients de façon transverse sur les volets organisationnels (conformité, gouvernance) et opérationnels (audit et tests d'intrusion, infrastructure de sécurité, SOC – CERT) :

Offensive Security – Utiliser les techniques des cybercriminels avec pragmatisme et méthodologie : tests d'intrusion, audits sécurité de code source, d'architecture, de configuration, physique, reverse engineering, social engineering, forensic.

Governance & Risk management – Organiser la défense du SI et maîtriser les risques : Gouvernance de la SSI, analyse de risques, sensibilisation, accompagnement à la mise en œuvre de solutions de sécurité, audits organisationnels, PCA, PRA, gestion, tests et exercices de cyber crise, RSSI as a Service

Infrastructure Security – Concevoir et déployer les infrastructures de Sécurité : conception d'architecture technique sécurité et réseau (Cloud et sécurité des données, IAM, IDaaS, etc.), gestion de projets sécurité (AO, choix de solutions, industrialisation et pilotage, etc.), expertise technique sécurité

Compliance – Atteindre, maintenir et démontrer la conformité : Mise en conformité PCI DSS, ANJ, LPM, ASIP, ISO27001, DCP : Cartographie et conformité au RGPD, audits de conformité aux référentiels internes et sectoriels, sécurité de l'entreprise étendue (audits des fournisseurs de services)

SOC CERT CWATCH – Détecter et agir contre les attaques : Services SOC/CERT, réponse à incidents de sécurité, services managés de détection d'incidents de sécurité internes et externes, service de protection (scan et gestion de vulnérabilités, gestion solutions EDR), threat intelligence tactique, conseil et audit en organisation du SOC/C-SIRT.

Solutions

Boost your cyber experience

BYCE (Boost Your Cyber Experience) est notre plateforme e-learning de sensibilisation à la sécurité de l'information, prête à l'emploi et disponible en SaaS.
Des modules courts qui vont susciter la compréhension et l'adhésion de vos collaborateurs, écrits par nos experts et customisés par des spécialistes de la psychologie cognitive.

Certifications

- qualifié PASSI pour les activités de tests d'intrusion, d'audits techniques (architecture, configuration, code source d'application), et d'audits de sécurité opérationnelle et physique,
- détenteur du « Label France Cybersecurity »,
- auditeur SWIFT : inscrit dans le répertoire de SWIFT listant les fournisseurs de services d'évaluation liés au CSP et CSCF,
- PCI QSA Company, qualifié pour mener les audits de certification du standard PCI DSS depuis 2010,
- certifié PFI : premier acteur français certifié pour ses activités d'analyse forensique,
- habilité en tant qu'auditeur par l'ANJ pour mener les audits de certification auprès des opérateurs de Jeux en Ligne.

Dirigeants



Olivier PANTALÉO
Associé en charge de la Cyber Sécurité
opantaleo@almond.consulting



Michael BRIQUET
Associé en charge du commerce
mbriquet@almond.consulting

Historique :

2022 – Spinoff de l'activité logiciel dans la société Board of Cyber qui développe et commercialise le Security Rating®, solution SaaS qui permet d'évaluer en continu, et automatiquement, l'exposition des organisations aux risques Cyber.

Almond

Transform, Secure & Beyond

Avec Almond, optez pour une maîtrise de vos opérations et de votre stratégie SSI

› Nos expertises

Information Security

Digital & Technology

Almond Institute

› Nos services & solutions

CWATCH

Boost your cyber experience

› Nos labels, certifications et habilitations

PRESTATAIRE RÉFÉRENCÉ CYBERMALVEILLANCE.GOUV.FR

VISA DE SÉCURITÉ

FRANCE CYBER SECURITY

CERT Authorized to Use CERT™ CERT is a mark owned by Carnegie Mellon University

SWIFT

PCI QSA Security Standards Council Company

ANJ

Paris | Nantes | Strasbourg | Lyon | Genève

https://almond.consulting

Société : ATEMPO
Adresse : 23, avenue Carnot
91300 Massy - France
Tel : 33 1 64 86 83 00
Mail : **info@atempo.com**
Site web : **www.atempo.com**

Spécialisations :

Editeur de solutions pour la protection et le management des données, Atempo dispose d'une expertise éprouvée pour sauvegarder, archiver, déplacer et gérer de très grands volumes de données dans les secteurs pétavores tels que la finance, l'assurance, les médias, le design industriel, les sciences de la vie et de la terre, les véhicules intelligents et les systèmes d'information géographique.

Contact :
Thanom MARI
Marketing Manager
thanom.mari@atempo.com



« Pour Atempo, l'autonomie numérique européenne n'est pas une option. Elle constitue l'indispensable condition à la mise en œuvre de nos choix politiques, à notre prospérité économique et à l'expression de nos libertés. Pour nos clients, c'est la garantie de la confidentialité et de la sécurité qu'ils sont en droit d'exiger pour leur principal actif : les données"

Luc D'Urso, *CEO Atempo*

Une entreprise engagée pour la souveraineté numérique européenne

Avec plus de trente années d'expérience, Atempo, éditeur de logiciels français, est le leader européen de la **Data Protection** et du **Data Management.** Ses solutions offrent à des milliers d'organisations publiques et privées dans le monde la sécurité et la confidentialité qu'elles sont en droit d'exiger pour leurs données et la continuité de leur activité. Agnostiques aux constructeurs et fournisseurs de cloud Computing, les solutions Atempo supportent un vaste éventail de technologies de stockage et d'applications.

Engagée dans la lutte contre la cybercriminalité, la société est membre d'**Hexatrust, de l'European Champions Alliances,** du groupement ACYMA qui soutient le programme gouvernemental **cybermalveillance.gouv.fr,** de l'association européenne **GAIA-X** et du **GINUM** (Groupement des Intervenants du Numérique).

Sélectionnée dans le cadre du programme gouvernemental **French Tech 120**-Alumni 2020 destiné à faire émerger 25 licornes d'ici 2025, l'entreprise dispose d'un puissant réseau de grossistes à valeur ajoutée, revendeurs, constructeurs, intégrateurs, et fournisseurs de services managés.

Offres de confiance et souveraines

Atempo propose une plateforme de Data Protection avec des solutions de sauvegarde et de reprise d'activité après sinistre et une plateforme de Data Management dédiée à la gestion de très grands volumes de données entre différents stockages sur site ou dans le cloud.





Continuity : nouvelle plateforme dédiée à la sauvegarde 360° des TPE / PME.

Lina : solution de protection en continu des données des postes fixes, portables, et des serveurs de fichiers.

Tina : solution de protection des serveurs physiques, virtuels et des données M365.

Miria : plateforme unique de Data Management dédiée à l'archivage, la sauvegarde, la migration, l'analytique et la mobilité de très grands volumes de données à l'échelle du pétaoctet.

Développées et supportées en France, les solutions Atempo bénéficient d'une solide réputation auprès des organismes publics et privés. Elles sont référencées au catalogue GouvTech de la **DINUM** (Direction interministérielle du numérique), véritable gage de qualité et de fiabilité en matière de protection des données et de conformité aux grands principes du numérique public. Les offres Atempo sont également répertoriées dans les catalogues des Centrales d'Achat Publiques, telles que UGAP, CAIH, ELODI, CNL, SIPPEREC.

Points forts des solutions Atempo

- Solutions conçues, développées et supportées en France
- Solutions adaptées aux environnements hétérogènes
- Déploiement sur site, en mode cloud ou hybride
- Solutions agnostiques aux constructeurs et fournisseurs de cloud computing
- Large catalogue de compatibilité avec les systèmes d'exploitation et applications du marché
- Tarification adaptée aux segments de marché : collectivités, hôpitaux, éducation, recherche, etc.
- Fonction de Disaster Recovery pour lutter efficacement contre la recrudescence des cyberattaques
- Solutions d'archivage déconnectées (Air-Gap) et de données immuables pour se prémunir des cyberattaques
- Solutions capables de répondre aux enjeux liés à l'explosion des volumes de données (à l'échelle du pétaoctet)
- Qualité et disponibilité du support, accessible 24/7

Certifications

- Certification ISO9001:2015
- Label France CyberSecurity
- Label « Utilisé par les Armées Françaises »
- FrenchTech 120 – alumni 2020

Avast Business

Société : AVAST BUSINESS

Nom des marques :
Avast Small Business Solutions :
Avast Essential Business Security /
Avast Premium Business Security /
Avast Ultimate Business Security

Adresse : Pikrtova 1737/1a, Prague 4, Nusle, Code postal 140 00, République tchèque
Tél : +41 79 322 52 05
Mail : **alexandra.alguazil@avast.com**
Site Web :
https://www.avast.com/fr-fr/business

Spécialisations :

Antivirus / Protection du poste de travail / Sécurité réseau / Patch Management

Chiffres clés :

CA : $ 941.1M
Effectifs : 1700 +



Dirigeant
Ondrej VLCEK
Président directeur général

O. Vlcek était précédemment Président d'Avast Consumer, et a dirigé le développement du réseau de sécurité cloud d'Avast basé sur l'Intelligence artificielle. Antérieurement, après avoir été Chef Développeur et dirigé l'équipe qui avait développé l'un des tout premier antivirus sous Windows, il a combiné les positions de CTO, directeur général et vice-président, pour transformer Avast en fournisseur leader d'un portfolio complet de produits performants de protection, de confidentialité et performance pour les consommateurs.



Contact
Alexandra
ALGUAZIL
Responsable de compte Distribution
+41 79 322 52 05
alexandra.alguazil@avast.com

Avast Business offre des solutions de sécurité intégrées pour les réseaux et les terminaux des PME et prestataires de services informatiques. Grâce au réseau de détection des menaces le plus important et le plus étendu au monde, le portefeuille de produits de sécurité Avast Business permet de sécuriser, de gérer et de surveiller les réseaux informatiques complexes en toute simplicité et à moindre coût. Résultat : Une protection de qualité supérieure sur laquelle les entreprises peuvent compter.

Offres



L'offre Avast Small Business Solutions est une offre de sécurité en ligne simple, puissante et abordable pour votre petite entreprise. Une offre efficace de protection sans besoin de maintenance importante.

Essential Business Security : La protection en ligne essentielle dont vous ne pouvez pas vous passer. Grâce à notre antivirus primé, Avast Essential Business Security défend votre entreprise contre les virus, le phishing, les ransomwares, les spywares, les menaces zero second, les vulnérabilités des réseaux Wi-Fi et bien plus encore.

Premium Business Security : La protection en ligne et la confidentialité Premium que méritent vos employés. Avast Premium Business Security réunit notre antivirus primé, un VPN et des outils de confidentialité pour assurer la protection et la confidentialité en ligne de vos employés.

Ultimate Business Security : Le nec plus ultra de la protection en ligne et de l'automatisation indispensable à votre entreprise. Avast Ultimate Business Security réunit notre antivirus primé, nos meilleurs outils de confidentialité ainsi qu'un logiciel d'automatisation de la gestion des correctifs qui tient à jour vos appareils et applications et en assure la protection.

Certifications

Elu « Top product » par AV-Test en avril 2022



« Cette année, nous avons concentré nos efforts pour fournir plus de valeur et de sécurité à nos produits pour les petites et moyennes entreprises. Nous avons ajouté de nombreuses nouvelles fonctionnalités à nos solutions pour petites entreprises, comme la protection USB (contrôle des périphériques), la protection mobile, et dernièrement la protection contre les rançongiciels avec la fonctionnalité Ransomware Shield, et bien d'autres encore. Ces nouvelles fonctionnalités offrent une protection renforcée afin de protéger votre entreprise contre les ransomwares et autres cyberattaques avancées. »

Alexandra ALGUAZIL
Responsable de compte Distribution

Historique :

1988 : Pavel Baudis neutralise le virus Vienna. Il crée avec Eduard Kucera à Prague la coopérative AWIL pour commercialiser leur nouveau logiciel.
2001 : Avast prend un tournant décisif et change le modèle commercial de l'antivirus traditionnel en offrant à tous un antivirus gratuit et complet.
2011 : Création de solutions pour entreprises
2016 : Rachat d'AVG par Avast, cette acquisition dote Avast du réseau de détection de menaces le plus étendu et le plus avancé, grâce à une vaste base d'utilisateurs.
2017 : Avast atteint les 811 millions de dollars et rachète Piriform, atteignant 435 millions d'utilisateurs.
2018 : Entrée en bourse

POUR EN FINIR AVEC LE PHISHING

Avantde Cliquer .com
L'humain au cœur de la cybersécurité

Société : Avant de Cliquer
Adresse : 129 rue Edouard Delamare Debouteville
76160 Saint-Martin-du-Vivier
Tel : 02 78 77 53 86
Mail : contact@avantdecliquer.com
Site Web : avantdecliquer.com

Spécialisations :

Avant de Cliquer permet aux DSI, RSSI, DPO et dirigeants de réduire le risque de cyberattaque de manière drastique à l'aide d'un programme de sensibilisation au phishing basé sur l'apprentissage par l'action, créé sur mesure pour chaque utilisateur et animé sur la durée. La solution est entièrement autonome.

Impact :

Plus de 500 000 utilisateurs actuellement sensibilisés.

Objectifs :

Diviser par 10 le risque de cyberattaques



Dirigeant
Carl HERNANDEZ
carl@avantdecliquer.com
Tél : 02 78 77 53 86

Conçu, créé et hébergé en France

L'audit de vulnérabilité

Réalisé en situation réelle, mesure le niveau de maturité de vos utilisateurs face à une attaque par phishing. Votre rapport de vulnérabilité présenté en visioconférence permet de définir votre stratégie de prévention cyber.

Sensibilisation en continu

- Parce que le mode opératoire des fraudeurs évolue, les simulations de phishing ne sont donc pas faites sous la forme de campagnes ponctuelles mais d'envois constants, ce qui est bien plus efficace.
- Parce que les fraudeurs ne préviennent pas, à chaque instant, chaque utilisateur est susceptible de recevoir un mail malveillant.

Personnalisation de l'apprentissage

Les utilisateurs peu vigilants sont sensibilisés autant de fois que nécessaire jusqu'à ce que chaque point de faiblesse détecté soit comblé.

Des mises en situation

Les mises en situation peuvent prendre plusieurs formes :

- mails comportant des liens
- fraude au président
- SMS
- Clé USB…

Amélioration des remontées d'information de vos utilisateurs

- En 1 clic, à l'aide d'un bouton "Alerte Phishing", intégré au client mail, vos utilisateurs signalent tout mail douteux.
- Le mail potentiellement frauduleux est automatiquement transmis pour analyse à votre équipe informatique.
- L'utilisateur est félicité pour son comportement positif.

Documentation des actions mises en place

Les actions de sensibilisation menées, les améliorations constatées, les axes de progression sont documentés. Ces actions sont conformes à l'article 32 du RGPD, imposant la mise en place de mesures organisationnelles de protection des données personnelles.

E-learning

Sensibilisation initiale, couvrant des éléments de contexte et techniques liés à l'hameçonnage (30 minutes sous forme de 15 modules).

Vous n'avez rien à faire. Tout est automatique.

Les envois ciblés sont réalisés sans action de votre part : vous n'avez pas à créer ou choisir des templates, à planifier des envois, à analyser les résultats pour sensibiliser les utilisateurs qui en ont le plus besoin.

Un accompagnement personnalisé

Chaque mois vous échangez avec un spécialiste sur les améliorations constatées et les axes de progrès, les menaces actuelles, de nouveaux modules d'e-learning et supports de communication personnalisés.

BPI France — Solution pertinente pour sensibiliser les utilisateurs à la cybersécurité
Référencé UGAP — L'achat public responsable
Finaliste du prix de l'innovation — Salon des Maire et des Collectivités Locales
Lauréat de l'innovation SANTEXPO — Transformation Digitale & Cybersécurité
Référencé CAIH — Centrale d'Achat de l'Informatique Hospitalière
Lauréat de l'intelligence économique — Trophée de l'agroalimentaire

AvantdeCliquer.com

L'humain au cœur de la cybersécurité

PROTÉGEZ-VOUS EFFICACEMENT DES CYBERATTAQUES



80% DES CYBERATTAQUES ONT POUR ORIGINE UN E-MAIL FRAUDULEUX

conçus / hébergés / développés en FRANCE

- Lauréat de l'intelligence économique
- BPI France — Solution pertinente pour sensibiliser les utilisateurs à la cybersécurité
- Finaliste du prix de l'innovation du Salon des Maires et des Collectivités Locales
- Lauréat de l'Innovation SANTEXPO — Transformation Digitale & Cybersécurité (santé)

FRANCE CYBER SECURITY

www.avantdecliquer.com

Board of Cyber *est une startup française avec pour mission de* **créer un écosystème de confiance.** *La cybersécurité commence par une connaissance fine et objective de ses propres performances mais également celle de ses partenaires. Concrètement,* **Board of Cyber** *développe et propose des solutions SaaS de cybersécurité dont le produit phare est* **Security Rating®.**
Board of Cyber *est d'abord une équipe de plus de* **20 passionnés** *qui œuvrent tous les jours pour faire de cette aventure un très beau succès.*

Société : BOARD OF CYBER
NOM DES MARQUES :
SECURITY RATING®

Adresse : 7 Avenue de la Cristallerie, 92310 Sèvres
Tél : 01 46 48 26 00
Mail : **contact@boardofcyber.io**
Site Web : **https://boardofcyber.io**

Spécialisations :

- **Notation cyber**
- **Analyse de risques**
- **Gestion des risques fournisseurs**

Chiffres clés :

1,2 million (exercice en cours/prévisionnel. Création de la société en février 2022)

Effectifs : 20 personnes

Historique :

Board of Cyber est une startup en cybersécurité lancée début 2022 par le startup-studio d'Almond, pure player du conseil en cybersécurité. Board of Cyber propose des solutions SaaS de gestion du risque cyber.



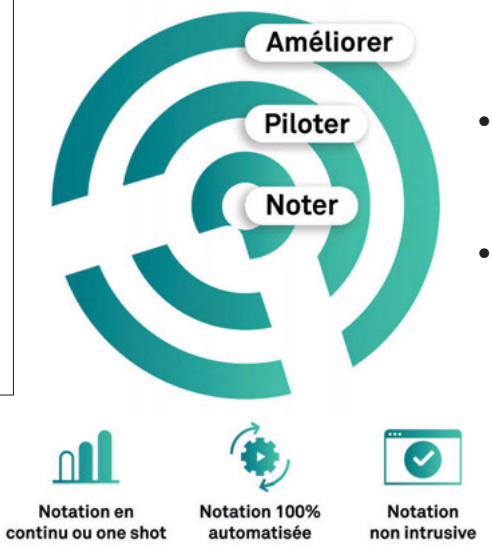
Contacts
Luc DECLERCK
Managing Director
06 60 72 39 23
ldeclerck@boardofcyber.io



François-Charles FACHON
Channel Manager
06 62 32 64 10
fcfachon@boardofcyber.io

Solution

Security Rating® est une solution **SaaS non-intrusive** qui évalue la maturité Cyber Sécurité d'une société ou d'une organisation à travers ses actifs publics. **'Noter', 'Piloter', 'Améliorer'**, au-delà de la notation, **Security Rating®** permet aux entreprises de disposer **de constats et de recommandations** pour une amélioration continue de sa performance cyber ou celle de son écosystème.



L'algorithme calcule une note en se basant **sur plusieurs tests découpés en 6 modules :**

- la surface d'attaque
- la messagerie
- la couche TLS/SSL des sites web de l'entreprise
- l'implémentation DNS sur les noms de domaines de l'entreprise (contrôle de sécurité)
- l'identification des vulnérabilités potentielles et la cadence de patching
- les incidents de sécurité (les évidences de compromissions identifiées)

En option, **nos questionnaires viennent enrichir la notation** en ajoutant une vision interne de l'entreprise évaluée : évaluation des besoins en cyber sécurité, évaluation de la maturité cyber, questionnaire RGPD. Les clients peuvent également intégrer leur propre questionnaire.

La plateforme est disponible en français, anglais, italien, espagnol et allemand.

CERTIFICATIONS

- **Board of Cyber** a obtenu le **Label France Cyber Security** qui certifie aux utilisateurs une garantie :
  - Sur un produit de **haute qualité**
  - Sur un service fourni par une **entreprise française indépendante** (actionnariat 100% français)
- **Board of Cyber** et sa solution **Security Rating®** sont référencés par l'UGAP dans le contrat cadre de l'offre multi-éditeurs.
- La notation cyber possède plusieurs points forts et permet de :
  - **Mesurer en continu la performance de la maturité cyber sécurité** des assets publics de l'entreprise
  - **Déterminer comment les investisseurs et partenaires voient l'entreprise** comme contributeur d'un risque
  - **Faciliter l'identification des axes de progrès** pour mieux gérer le risque cyber
  - **Positionner la performance de la maturité cyber sécurité** d'une entreprise vis-à-vis de son secteur d'activité
- Security Rating® se différencie avec une approche nouvelle de la cartographie des actifs évalués : nos utilisateurs **ont un accès complet** et peuvent **visualiser en temps réel les actifs analysés** par la solution.

Références Clients

Board of Cyber a déjà plus de 150 clients dont : Bessé, Bouygues, Conseil Départemental 06, CESIN, Eurazeo, Europ Assistance, Groupama, LCL, Région île de France, Somfy, Wendel

board of cyber

Beyond Rating.

Notez / Pilotez / Améliorez

en continu la performance cyber de votre organisation ou celle de votre écosystème avec notre solution SaaS

Security Rating®



www.boardofcyber.io

Bitdefender®
BUILT FOR RESILIENCE

Société : BITDEFENDER
Adresse : 49 rue de la Vanne, 92120 Montrouge, France
Tel : +33 1 47 35 72 73
Mail : **enterprise_france@bitdefender.fr**
Site Web : **www.bitdefender.fr**

Spécialisations :

Protection des endpoints physiques et virtualisés, sécurité du Cloud et des conteneurs, eXtended Detection and Response (XDR), SOC managé (MDR), Threat Intelligence, Forensics, Machine Learning

Chiffres clés :

Effectifs : 1 600

Historique : Société européenne créée en 2001

Bitdefender Labs : + de 30 milliards de requêtes de menaces chaque jour et +400 nouvelles menaces découvertes par minute

Le saviez-vous ? Les technologies Bitdefender sont utilisées par plus de 150 éditeurs sous licence



Dirigeant

Fondateur et PDG de Bitdefender, **Florin TALPES** *est un entrepreneur technologique visionnaire qui a fondé l'une des premières sociétés privées d'édition de logiciels, qui allait plus tard devenir Bitdefender. Sous sa direction, Bitdefender est devenu un leader mondial de la cybersécurité protégeant des millions de clients dans le monde.*



Contact

Laurent TOMBOIS
Country Manager France
ltombois@bitdefender.fr

Plateforme primée de prévention, détection, réponse aux menaces et services de sécurité managés

Bitdefender est un leader de la cybersécurité qui fournit des solutions de pointe en matière de prévention, de détection et de réponse aux menaces. Protégeant des millions d'environnements de particuliers, d'entreprises et de gouvernements, Bitdefender est reconnue comme étant un expert de confiance au sein de l'industrie pour l'élimination des menaces, la protection de la vie privée et des données, et la cyber-résilience. Grâce à des investissements importants dans la recherche et le développement, les Bitdefender Labs découvrent 400 nouvelles menaces chaque minute et répondent à 30 milliards de requêtes de menaces par jour. La société a été la première à innover dans le domaine des malwares, de la sécurité de l'IoT, de l'analyse comportementale et de l'Intelligence artificielle. Sa technologie est utilisée sous licence par plus de 150 éditeurs parmi les plus reconnus au monde. Fondée en 2001, Bitdefender a des clients dans 170 pays et possède des bureaux dans le monde entier.

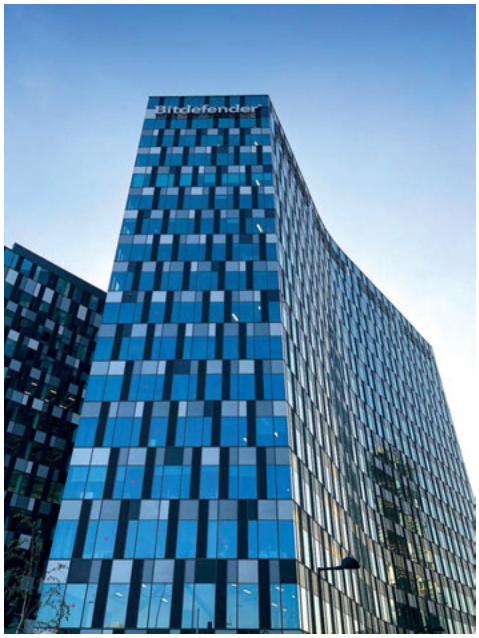
Offres

Bitdefender ambitionne de toujours mieux protéger ses clients entreprises en renforçant leur cyber résilience. Pour cela, Bitdefender répond à des besoins concrets en matière de cybersécurité.

• **Réduire le nombre d'outils utilisés et améliorer la visibilité.** Bitdefender GravityZone est une solution unifiée pour la protection et l'analyse des endpoints. Elle sécurise tous les endpoints de l'infrastructure et les charges de travail dans le Cloud via une seule console, un seul agent et un déploiement unifié (physique/virtuel/conteneurs, Cloud). Tous les modules de sécurité sont regroupés au sein d'un seul et unique outil : anti-malware Next-Gen, EDR, XDR, analyse des risques, contrôle des applications et du Web, Patch Management, chiffrement, sécurité contre les attaques réseau, sandbox cloud, Machine Learning, etc.

• **Bénéficier de la meilleure prévention possible.** Bitdefender est l'éditeur ayant été le plus grand nombre de fois à la première place des tests AV-Comparatives depuis 2018 en matière de Protection dans le monde réel, de Performances et de Protection contre les malwares. Bitdefender a aussi reçu la récompense « Best Protection 2020 » de la part d'AV-Test.

• **Résoudre les problématiques liées au manque de compétences internes.** Les organisations ne disposant pas des ressources nécessaires à la gestion quotidienne d'une solution de cybersécurité, à l'analyse des alertes et à l'investigation sur les attaques, elles peuvent se reposer sur le service Bitdefender Managed Detection and Response (MDR). Celui-ci exécute



24h/24, 7j/7, des mesures avancées de prévention et de remédiation des cyber-attaques, depuis le SOC Bitdefender.

• **Améliorer son ROI.** Bitdefender améliore le retour sur investissement de la cybersécurité en fournissant une solution unifiée qui intègre à la fois le renforcement, l'évaluation des risques, la prévention, la détection, la réponse et l'investigation.

Récompenses

« Strong Performer » Forrester Wave EDR (Q2 2022), «Top Player » Radicati Advanced Persistent Treat Protection (2021), «Best Protection» AV-Test (2021)

Certifications

SOC2 Type 2, ISO 9001, ISO 27001, Nutanix AVH/VMware/Citrix Ready.

ChamberSign
Autorité de certification

ChamberSign est une autorité de certification et un tiers de confiance. Elle propose un ensemble d'outils d'identités numériques et de signatures électroniques conforme aux réglementations en vigueur.

Société : ChamberSign France
Adresse : Le Cours du Midi
10 cours de Verdun Rambaud
69002 Lyon
Tel : 0892 230 252
(0,45 € TTC la minute France Métropolitaine uniquement)
Mail : commercial@chambersign.fr
Site Web : www.chambersign.fr

Spécialisations :

Acteur français incontournable en matière de sécurisation des échanges électroniques depuis plus de 22 ans, ChamberSign est une autorité de certification. Tiers de confiance, elle est qualifiée eIDAS par l'ANSSI et RGS par LSTI pour des certificats numériques professionnels à destination des personnes physiques et des entités morales.

Elle fournit un ensemble d'outils d'identités numériques et de signatures électroniques conforme aux réglementations en vigueur, afin de garantir les échanges électroniques authentifiés et sécurisés.

Chiffres clés :

Effectifs : + 25

+140 bureaux d'enregistrement répartis sur le territoire français (Guyane et Dom inclus)

+de 500 opérateurs habilités à délivrer des certificats électroniques



Dirigeant
Stéphane GASCH
Délégué général
sgasch@chambersign.fr
tél : 06 07 73 46 06

Experte dans son domaine, ses missions sont nombreuses :

- Fournir des certificats électroniques émis et délivrés dans le respect des normes les plus strictes de la réglementation (notamment RGS et eIDAS), garantissant ainsi l'identité numérique professionnelle de la personne physique ou de la personne morale ;
- Proposer des solutions permettant la gestion des identités numériques dans les applications métiers;
- Accompagner les organisations et les usagers à l'utilisation du certificat électronique dans leurs échanges dématérialisés sécurisés et adapter les processus et produits aux nouveaux usages ;
- Développer l'Identité Numérique Professionnelle des Entreprises. Cette solution a pour ambition de faciliter l'accès à divers services tout en utilisant une authentification forte professionnelle visant à fournir une identité substantielle.

Offres



Des certificats électroniques:

ChamberSign fournit des certificats électroniques pour les personnes physiques et morales.

Les certificats numériques personne physique offrent une multitude d'usages. Servant d'authentification forte, ils remplacent le login/mot de passe sur une session Windows ou tout autre compte utilisateur. Ils servent également à la signature électronique. C'est l'assurance d'une dématérialisation à valeure légale où l'identité du signataire, son engagement et l'intégrité du document sont prouvés de manière certaine.

Justifier de son identité est devenu indispensable pour toutes les organisations. Elles doivent utiliser des certificats électroniques de type cachet. Ils permettent de garantir la confidentialité et/ou l'intégrité des données transmises tout en garantissant leur origine et justifient de la propriété des machines.

Des outils d'authentification et de signature électronique :

ChamberSign a développé la solution "ChamberSign Connect" intégrant les certificats électroniques dans le système d'information des organisations. Cet outil permet aux utilisateurs de se connecter sur n'importe quelle application métier utilisant le protocole standard open ID Connect.

Par ailleurs, elle propose un ensemble de solutions de signatures électroniques et scellement, simple d'utilisation et facile à mettre en place, garantissant intégrité et origine des documents numériques.



L'identité numérique professionnnelle des entreprises:

ChamberSign travaille actuellement au déploiement de l'identité numérique professionnelle des entreprises permettant une connexion facilitée et universelle à divers services notamment France Connect. Cette authentifcation forte professionnelle, candidate à la certification, vise à fournir une identité numérique substantielle.

Qualifications et distinctions



ChamberSign s'est vu décerner le visa de sécurité de l'ANSSI pour ses services de certification électronique et a également obtenu le label France Cybersecurity.

- Ses certificats électroniques sont qualifiés eIDAS et RGS.
- Elle est certifiée ISO 9001 version 2015 pour ses procédures internes et celles de délivrance de certificats.

Conformément à ses obligations d'Autorité de certification, ses processus et son système d'information ont fait l'objet d'un audit de conformité RGPD conclu positivement et dont le renouvellement périodique est inclus dans sa politique interne.

Historique

ChamberSign fournit en France ses premiers certificats numériques en 2000. Elle participe depuis toujours à la réflexion et au développement des échanges électroniques sécurisés (membre de la FNTC, du club PSCO, ou encore de l'ACN).

Consciente des enjeux et soucieuses d'accompagner les organisations dans leurs nouveaux défis liés à l'instauration d'un environnement numérique fiable, de confiance et sécurisé, ChamberSign s'adapte et est en constante réflexion sur les besoins actuels et usages futurs des organisations.

Le dernier kilomètre de la cybersécurité : changer le comportement des utilisateurs

Société : CONSCIO TECHNOLOGIES
Adresse : 12 rue Vivienne, 75002 Paris
Tél : 01 84 80 82 00
Mail :
contact@conscio-technologies.com
Site Web :
www.conscio-technologies.com

Depuis 2007, nous travaillons avec les RSSI, DSI et DPO afin de les aider à développer une réelle culture cybersécurité. Notre objectif est de les aider à franchir le dernier kilomètre de la cybersécurité qui est celui du changement de comportements des utilisateurs. Conscio Technologies est éditeur de logiciels et de contenus conçus spécialement pour remplir notre mission.
Les logiciels Sensiwave et RapidAwareness sont conçus pour la mise en oeuvre de vos campagnes de sensibilisation et de tests phishing. Depuis près de 15 ans, Conscio Technologies a constitué un catalogue de plus de 80 modules, enrichi en permanence. Plus de 2 millions d'utilisateurs ont été sensibilisés au moyen des contenus et des solutions de Conscio Technologies, en accompagnant plus de 200 clients.

Spécialisations :

Sensibilisation cybersécurité

Chiffres clés :

CA : 1,7 M€
Effectifs : 17



Dirigeants
Michel Gérard,
CEO

« Notre mission peut se définir comme faire comprendre et adhérer le plus grand nombre à l'essentiel. A ce titre la cybersécurité est clairement l'un des enjeux majeurs du moment »

Solutions

Contenus Sensiware

- Catalogue de plus de 80 modules en évolution constante
- Etude de maturité
- Master quiz
- Microlearning interactifs
- Vidéos Funny But Serious
- Modules interactifs cyberhéros
- Interface chatbots
- Livres interactifs
- 13+ langues avec doublage des vidéos
- Nombreuses thématiques traitées (…)
- Modules sectoriels (santé…)
- Fiches thématiques téléchargeables

Plateforme de sensibilisation conçue dès le départ pour la mise en œuvre de votre stratégie de sensibilisation

- Un wizzard pour le lancement instantané de campagnes prépackagées
- Gestion des rôles administrateurs et managers
- Gestion utilisateurs multi critères
- Personnalisation et création de contenus avec les fonctions d'éditions intégrées
- Ciblage des campagnes multicritères
- Ciblage campagne en fonction des résultats précédents
- Pages d'accueil responsives
- Gestion des invitations et des relances
- Statistiques génériques
- Statistiques détaillées au moyen d'un requêteur
- Création de rapports
- Export scorm
- Gestion de certificats
- Espace utilisateur de sensibilisation
- Possibilité de création d'un opérateur de sensibilisation

Test phishing

- Catalogue de 60 scénarios en développement constant
- Lien dangereux
- Data entry
- Pièces jointes dangereuses
- Tirage aléatoire de scénarios
- Inscription automatique à une campagne de sensibilisation
- Bouton d'alerte
- Plus de 10 langues disponibles

Technique

- SSO/SAML
- Interface AD
- API OAUTH2
- Données chiffrées
- Base de données Big Data
- Puissance des performances (courbes montées en charge)

Sensiware



Certifications

BRETAGNE SUD · EFCTS · UGAP · HEXATRUST CLOUD CONFIDENCE & CYBERSECURITY · C.A.I.H. Centrale d'Achat de l'Informatique Hospitalière

CyberRes
Une ligne métier de Micro Focus

Renforcez votre cyber-résilience

CLUSIF Adhérent 2022

Société : CyberRes
Nom des marques :
FORTIFY, VOLTAGE, NETIQ, ARCSIGHT
Adresse : Tour Carpe Diem
31 Place des Corolles
92098 Paris La Défense Cedex
Site web : **www.cyberres.com**

CyberRes regroupe les solutions de Sécurité de Micro Focus. Nous apportons l'expertise de l'un des plus grands portefeuilles de sécurité au monde pour aider nos clients à faire face à l'évolution des menaces en renforçant la cyber-résilience de leurs équipes et organisation. Nous aidons les entreprises à renforcer la confiance, à gagner en fiabilité et à survivre en cas de conditions difficiles, de crise et de volatilité du marché.

Spécialisations :

- **DevSecOps**
- **Conformité RGPD**
- **Chiffrement**
- **Sécurité de l'information**
- **Collecte et traitement des logs**
- **SIEM & SOC**
- **IAM, IGA, Authentification forte**

Chiffres clés :

600 millions US$ de CA
14 000 clients
1800 employés
35 solutions
120 produits lancés chaque année
Siège social : Newbury, Royaume-Uni



Dirigeant
Christophe GAULTIER
Sales Director France & BeLux - CyberRes
christophe.gaultier@microfocus.com
Tel : +33 6 29 17 83 67

Offres

ArcSight

Next-Gen Security Operations & Analytics

Fort de plus de 20 ans d'historique dans le monde du SIEM et SOAR avec la plateforme ArcSight, CyberRes continue d'innover en proposant du contenu pertinent à des équipes de Sécurité Opérationnelle avec des outils de Threat Intelligence et de surveillance « mid-field » uniques sur le marché. Nos offres, on-premises, SaaS ou hybrides s'adaptent parfaitement à des clients finaux ou des fournisseurs de services de sécurité.

Fortify

Application Security

Leader sur le marché de la sécurité applicative, notre gamme Fortify propose des solutions de SAST (scan de code) et de DAST (scans dynamiques) afin de réduire les risques de mauvaise utilisation du code applicatif.

Notre plateforme de sécurité des applications automatise les tests tout au long du CI/CD afin que les développeurs puissent résoudre rapidement les problèmes.

Voltage

Data Privacy & Protection

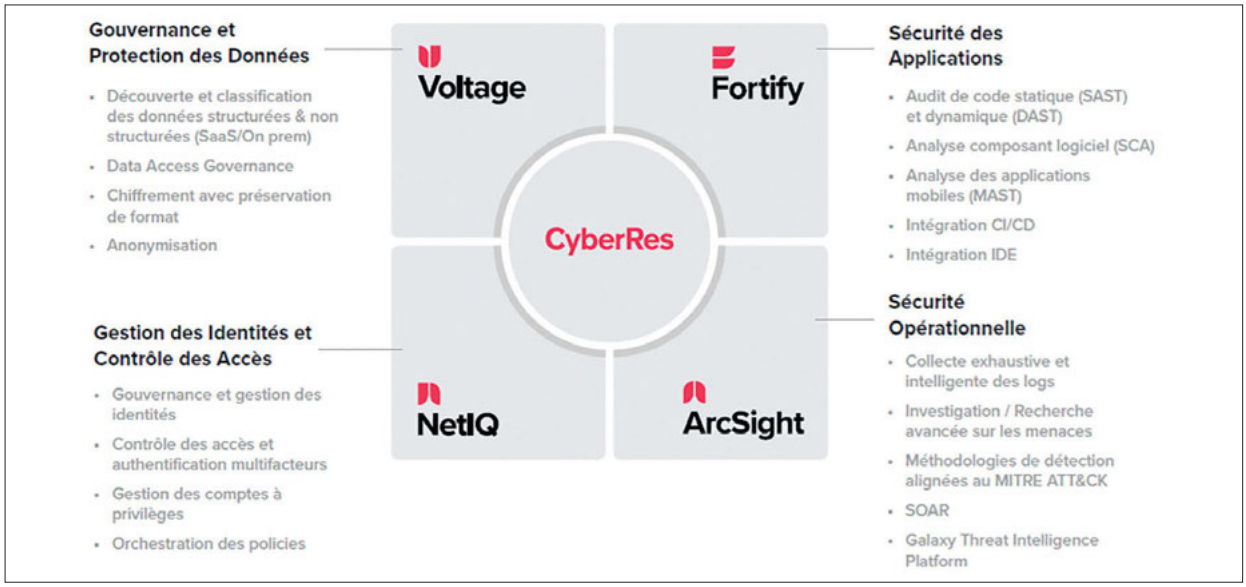
Découvrez, analysez et protégez vos données sensibles, structurées et non structurées dans le respect des exigences réglementaires RGPD notamment.

Présent dans la sécurité de données (dans le monde de la carte de paiement notamment) depuis une quinzaine d'années, la plateforme Voltage propose de sécuriser vos emails, vos documents, mais aussi vos données structurées, pour améliorer votre posture de sécurité.

NetIQ

Identity and Access Management

De la gouvernance des identités à l'authentification forte, en passant par la gestion des accès et la sécurisation des comptes à privilèges, Micro Focus propose la gamme complète et modulaire NetIQ de solutions IAM à déployer chez vous ou dans le cloud.



Société : CS NOVIDY'S
Adresse : 22 avenue Galilée
92350 Le Plessis Robinson
Site Web :
https://www.csnovidys.com/

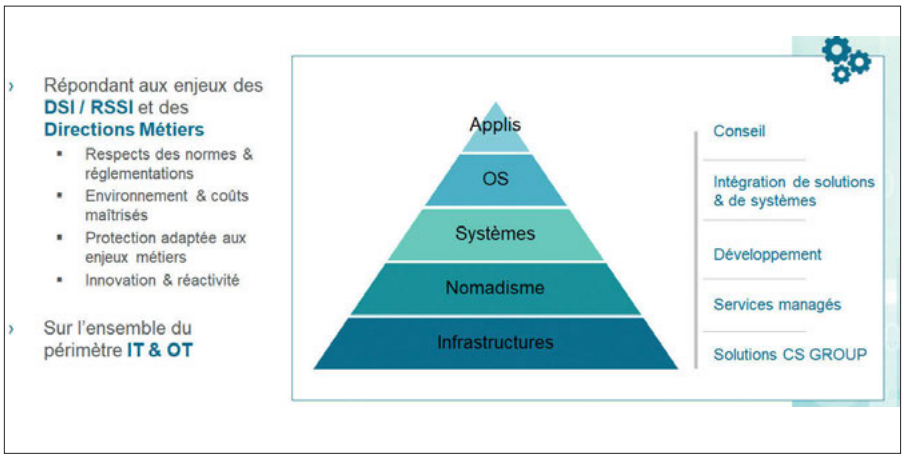
A travers sa filiale CS-NOVIDY'S, CS GROUP se positionne dans le top 5 des sociétés de services françaises sur le marché de la cybersécurité

Notre positionnement nous permet de couvrir l'ensemble des enjeux de la cybersécurité sur les SI d'entreprise (IT), et les SI industriels (OT), du Conseil aux services managés en passant par l'intégration de solutions et de systèmes.

L'enjeu est de déployer une sécurité au juste niveau pour permettre une maîtrise optimale de l'ensemble des infrastructures et systèmes. Nous concilions ainsi l'approche des DSI, RSSI et des directions opérationnelles métiers

UNE EXPERTISE du plus haut niveau :

- **CERT - CS GROUP**
- **Qualification PASSI & PASSI LPM**
- **Produits certifiés EAL3+**
- **NOC/SOC externalisé / hybride**
- **Laboratoire de Lutte Informatique**
- **La R&D au profit d'une sécurisation forte & flexible**

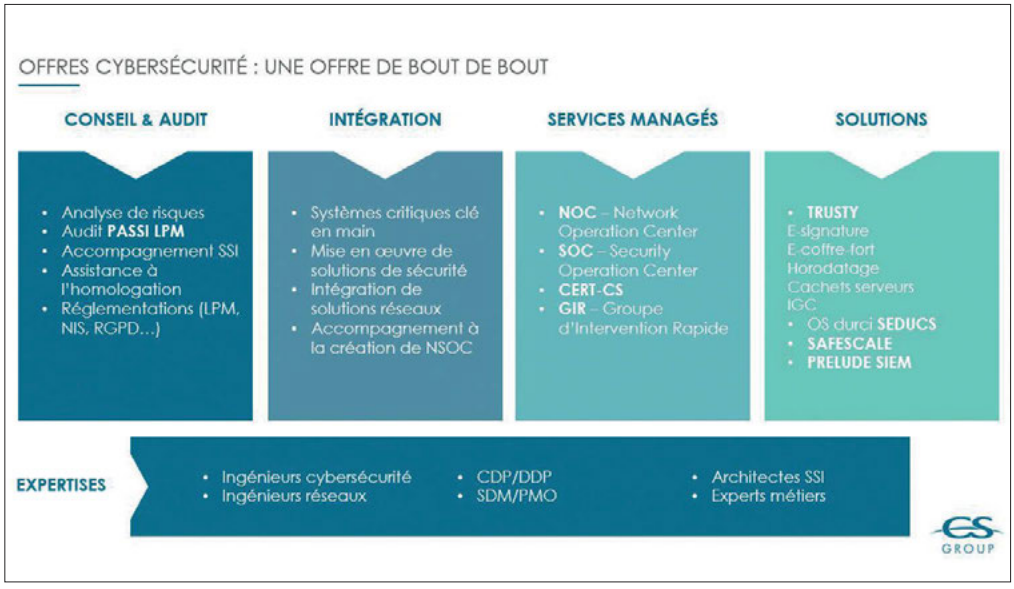


Offre

Une approche holistique de la cybersécurité :

- la sécurité des infrastructures et des communications (Lan, Wan, Cloud,…)
- des systèmes d'exploitation sécurisés,
- l'intégration de systèmes et d'applications sécurisés
- l'homologation de système d'informations sensibles …

Par ailleurs, expert en Data Intelligence, nous maîtrisons totalement les aspects de sécurisation, de confidentialité et d'intégrité de la donnée, enjeu majeur des entreprises en environnement cloud et collaboratif, et proposons une approche « security by design ».
Nous intervenons sur des secteurs stratégiques : la défense, la sécurité publique, le nucléaire, le spatial, l'aéronautique ou encore l'énergie. En tant que ETI française, nous proposons à nos clients qui opèrent dans ces secteurs d'importance vitale des solutions souveraines. Dans le domaine de la valorisation et de la sécurisation des données, nous sommes particulièrement impliqués dans des initiatives nationales et européennes et auprès de nos grands clients pour contribuer à garantir la souveraineté numérique européenne.
En nous apportant sa capacité à intégrer des solutions de sécurité, elle complète notre positionnement historique d'intégrateur de systèmes sécurisés. Nous sommes aujourd'hui dans le top 5 des sociétés de ce secteur, avec près de 300 experts.





NOVIDY'S

WWW.CSNOVIDYS.COM

CS-NOVIDY'S, filiale de CS GROUP

ACTEUR LEADER

POUR LA SÉCURISATION DE VOS SYSTÈMES D'INFORMATION D'ENTREPRISE & INDUSTRIELS

CERT IS A MARK OWNED BY CARNEGIE MELLON UNIVERSITY
CERT
AUTHORIZED TO USE CERT
Software Engineering Institute
Carnegie Mellon

VISA DE SÉCURITÉ

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

FRANCE CYBER SECURITY

SYSTÈMES CRITIQUES INTELLIGENTS CYBERPROTÉGÉS

CS GROUP

EGE Ecole de Guerre Economique

L'Ecole de Guerre Economique propose des formations de référence en intelligence économique, renseignement, risques, sûreté et cybersécurité depuis 25 ans, à la fois en formation initiale et formation continue.

Elle s'appuie sur un réseau d'experts de plus de 3000 membres à travers le monde. Elle est la seule structure française habilitée à délivrer le Titre d'Expert(e) en Intelligence Economique (RNCP, niveau 7).

Chiffres clés :

- **3000 anciens.**
- **400 diplômés par an.**
- **1er réseau d'experts en intelligence économique en France.**
- **1er au classement Eduniversal des Meilleurs Masters depuis 2002.**
- **1ère formation à destination des professionnels depuis 2005.**
- **2 campus Paris et Rabat.**

Accréditations

Titre d'Expert(e) en Intelligence Economique (RNCP, niveau 7)

Nos formations

MBA Executive Management Stratégique et Intelligence Economique MSIE

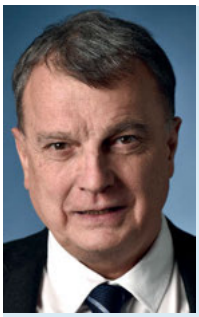
Première formation continue à destination des professionnels, le MBA executive Management Stratégique et Intelligence Economique MSIE donne également accès au titre "Expert(e) en Intelligence Économique", de niveau 7, enregistré au Répertoire National des Certifications Professionnelles (RNCP).

MBA Risques, Sûreté Internationale et CyberSécurité RSIC

La formation en alternance de l'EGE, traitant de l'approche globale de la cybersûreté et des risques, le MBA Spécialisé «Risques, Sûreté Internationale et Cybersécurité» (RSIC) est accessible avec un Bac+3 et peut se préparer en deux ans (M1+M2) ou 1 an (M2).

MBA Executive Management de la Cybersécurité et Gouvernance des Systèmes d'Information MaCYB

répond à un besoin de spécialisation de l'Ecole de Guerre Economique sur la dimension « cyber » du management de l'information. Le recours croissant aux technologies de l'information oblige les entreprises et les administrations à adapter leur mode de fonctionnement aux enjeux numériques.



Ecole de Guerre Economique

L'Ecole de Guerre Economique a été créée en 1997 afin de répondre aux nouvelles exigences stratégiques générées par la mondialisation. L'EGE est organisée autour d'un pôle d'enseignement, d'un pôle de recherche CR451, d'un pôle conseil (seule junior entreprise en intelligence économique). Cette structure pionnière en Europe sur la question de la guerre économique a conçu un enseignement fondé sur une approche interactive de l'économie, du management et de la géopolitique. La révolution numérique en cours nous a amené à développer un nouveau programme sur la maîtrise du risque, de la sûreté internationale et de la cybersécurité.

Aider les entreprises à conquérir des marchés, gagner les appels d'offres, favoriser l'implantation internationale des entreprises, trouver des solutions pour exporter : telles sont les missions fondamentales que l'Ecole de Guerre Economique s'est assignée pour construire son projet pédagogique, ainsi que sa politique de recherche.

Notre équipe pédagogique est constituée de professionnels reconnus, du monde de l'entreprise et du conseil, dont la finalité est de transmettre des méthodologies, des savoir-faire et des expériences concrètes et opérationnelles. Les professeurs d'université qui interviennent dans nos programmes ont intégré notre grille de lecture sur les pratiques de guerre économique.

L'EGE s'appuie sur son réseau des anciens, l'AEGE. elle entreprend toutes les actions susceptibles de favoriser l'insertion et la progression professionnelle des diplômés. Sur le principe de la formation permanente, l'AEGE organise gratuitement des cours de perfectionnement et gère le plus grand fonds documentaire français sur l'IE, en particulier le Portail de l'IE, le site vitrine de la discipline.

En partenariat avec de grands groupes, l'EGE propose depuis 17 ans un programme de professionnalisation en intelligence économique intitulé Mercurle. D'une durée de 8 mois, ce dispositif unique en France assure un taux de placement de plus de 85% de nos étudiants directement dans les métiers de l'IE.

Faire l'EGE, c'est apprendre à penser autrement pour faire face aux enjeux d'un monde complexe et conflictuel tout en relevant le défi des métiers de demain.

MBA Executive Management des Risques et Gestion de la Sûreté Globale MARS

Le lancement de la formation continue MARS répond à un besoin de spécialisation de l'EGE dans le domaine de la sûreté et de la protection des entreprises. Les directions de grands groupes, mais aussi les entreprises de taille moyenne, sont confrontées à des problématiques croissantes en termes de menaces. La fonction sûreté prend de l'ampleur sous l'effet de ces contraintes, qui deviennent des opportunités.

Liens réseaux sociaux de l'EGE

https://www.facebook.com/EcoleGuerreEconomique.EGE
https://twitter.com/ege_fr
https://www.linkedin.com/company/ege/

Ecole de Guerre Economique
196, rue de Grenelle
75007 Paris
01 45 51 00 02
mail : **contact@ege.fr**
www.ege.fr

FORMATIONS
POUR PROFESSIONNELS

EGE Ecole de Guerre Economique

MBA
Management des Risques Sûreté Internationale & Cybersécurité

Leader français de la formation continue en management stratégique et intelligence économique, forte de vingt quatre ans d'**innovation pédagogique** et d'un réseau international de 2300 experts, l'**Ecole de Guerre Economique** ouvre la 7ème session de sa formation **MBA Management des Risques, Sûreté Internationale et Cybersécurité (MRSIC)**.

“Se préparer aux risques de demain”

Aujourd'hui, la **question de la sûreté matérielle** des entreprises ne peut plus être dissociée de la problématique des **menaces immatérielles** qui affectent la vie économique via les **réseaux informatiques** et **Internet**.

La **protection de l'entreprise** est désormais un **enjeu stratégique** qui ne peut plus être traité par une série de **mesures techniques**.

Pour répondre à ce besoin d'approche globale de la cyber-sûreté et des risques, l'EGE a décidé de lancer le **programme exécutive MBA Spécialisé Management des Risques, Sûreté Internationale et Cybersécurité (MRSIC)**. La formation se déroule au centre de Paris, dans les locaux de l'EGE.

L'admission à cette formation est réservée à tous les **professionnels de tous secteurs d'activités en charge de fonction sûreté et Cyber sécurité**, **Risk Managers**, **cadres** secteurs publics (police, défense…) en reconversion, réserviste ou en activité.

Ecole de Guerre Economique / 196, rue de Grenelle / 75007 Paris
contact@ege.fr / +33 1 45 01 00 02 / **www.ege.fr**

ÉTABLISSEMENT D'ENSEIGNEMENT SUPÉRIEUR PRIVÉ

INFORMER
pour transformer l'entreprise

La dématérialisation, le Cloud,
les communications unifiées,
les nécessités de la cybersécurité
transforment le travail et toute l'entreprise,
les services publics.
Le magazine, le site, ses newsletters
vous informent sur cette actualité mouvante
et vous aident à décoder les tendances

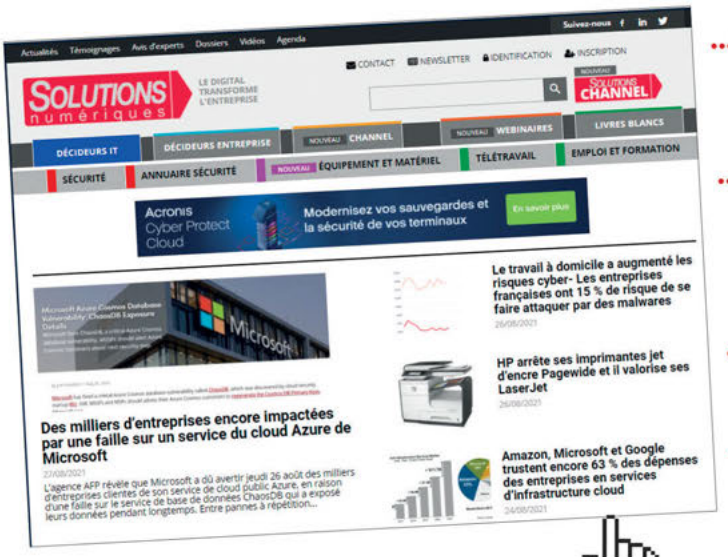


Abonnez-vous

www.solutions-numeriques.com/abonnement/

Toutes les ressources et newsletters en ligne

Pour répondre à vos besoins d'information



- La cybersécurité vous concerne ? Cliquez sur l'onglet. Vous trouverez les infos, l'annuaire, le lexique, etc
- L'emploi, les salaires, les formations, les offres vous intéressent ? Le site sur l'Emploi dans le numérique est à votre disposition
- Votre site Télétravail. Infos et bonnes pratiques pour le travail à distance et le travail hybride
- Solutions Channel. L'info des partenaires, intégrateurs, distributeurs

www.solutions-numeriques.com

EIFFAGE ÉNERGIE SYSTÈMES

Adresse : 3-7 place de l'Europe
78140 Vélizy-Villacoublay

E-mail :
contact.clemessy@eiffage.com

Site web :
www.eiffageenergiesystemes.com

Spécialisations :

Expertise en systèmes industriels et techniques permettant d'intégrer la cybersécurité sur tout le cycle de vie des installations.

SÉCURITÉ ACCRUE À TOUS LES NIVEAUX
Connaissance des enjeux et des failles de cybersécurité propres aux systèmes industriels et techniques pour une sécurité efficace.

OPTIMISATION DES COÛTS
Intégration et adaptation des solutions de sécurisation pour des coûts optimisés et des systèmes plus performants.

SÉCURITÉ TOUT AU LONG DU CYCLE DE VIE
Intégration des règles et mesures de cybersécurité dès la conception des systèmes et jusqu'à la maintenance-exploitation.

Chiffres clés :

Présents dans la cybersécurité depuis 20 ans

Dirigeant
Pierre Guilleminot
Directeur Général

Contact
Jocelyn ZINDY
Directeur commercial cybersécurité
03 89 32 37 08 - 06 24 90 18 94
Jocelyn.zindy@eiffage.com

Eiffage Énergie Systèmes conçoit, réalise, exploite et maintient des systèmes et équipements en génies électrique, industriel, climatique et énergétique dans le respect des Hommes et de l'environnement. Eiffage Énergie Systèmes propose une offre sur mesure pour les marchés de l'industrie, des infrastructures et réseaux, des villes et collectivités et du tertiaire.

Eiffage Énergie Systèmes vous accompagne dans la protection de votre patrimoine en renforçant la sécurité de vos systèmes industriels ou techniques.

Nos équipes intègrent la cybersécurité sur tout le cycle de vie de vos installations, vous garantissant la conformité aux normes en vigueur et l'optimisation de vos investissements en limitant les risques.

Une offre de services 360°, sur mesure et clé en main.

Audit, diagnostic, et conseils	Sécurisation des systèmes	Maintien en conditions de sécurité
• Inventaire et cartographie physique, logique, technique et fonctionnelle • Évaluation du niveau de sécurité/référentiels • Analyse de risques EBIOS • Analyse des mesures cybersécurité en réduction de risques • Rapport et restitution • Proposition d'un plan d'action	• Etude, intégration de solutions matérielles et logicielles (détection et protection) • Remédiations et durcissement • Sécurisation des architectures industrielles, réseaux, données, logiciels, postes et équipements • Evaluation des risques résiduels	• Maintenance • Veilles de vulnérabilité • Mises à jour • Formation de sensibilisation • Simulation d'attaques et réponse sur incident



« Eiffage Énergie Systèmes travaille sur la sécurité dans le domaine industriel depuis plus de 20 ans. Nous sécurisons les systèmes existants en débutant par une phase de diagnostic.
Nous évaluons les vulnérabilités, identifions les systèmes obsolètes et analysons les risques. Cette phase permet ensuite de planifier et prioriser les interventions nécessaires. Nous procédons enfin à la remise en état en réduisant les indisponibilités du système. Notre expertise nous permet également d'intervenir sur des sites industriels neufs. La cybersécurité est ainsi intégrée dès la conception.»

Jocelyn Zindy,
Directeur commercial cybersécurité

Certifications

Eiffage Énergie Systèmes respecte de nombreux référentiels spécifiques ou normatifs (Loi de Programmation Militaire–LPM, PIMSEC ANSSI, IEC62443, APSAD D32) dans des contextes exigeants ou chez les opérateurs d'importance vitale.

Références Clients

Automobile / Environnement / Défense / Agro-alimentaire / Chimie / Pharmacie/ Nucléaire / Spatial / Aéronautique

1er éditeur Européen de solutions de sécurité*

Société : ESET
Adresse : 20 allée Louis Calmanovic
93320 Les Pavillons-sous-Bois
Tel : 01 55 89 08 85
Site web : **www.eset.com/fr**

Indépendance, intégrité, connaissance et expertise sont les fondements qui guident nos collaborateurs depuis plus de 30 ans. Située au cœur de l'Europe et présente dans plus de 200 pays, la société ESET est leader en matière de détection proactive des menaces et protège plus d'un milliard d'internautes dans le monde.

Spécialisations :

- **Protection Endpoint (postes, serveurs, mobiles, données)**
- **Protection des serveurs de messagerie et des outils collaboratifs**
- **Endpoint Detection and Response (EDR)**
- **Sandbox Cloud**
- **Managed Detection & Response**
- **XDR**
- **Health Check**
- **Déploiement & Upgrade**

Chiffres clés :

Effectif mondial : plus de 2000 collaborateurs et chercheurs
R&D : 13 laboratoires

Twitter : **@ESET_France**
LinkedIn : **esetfrance**
Blog : **welivesecurity.com/fr**

Contact
Nicolas CHAUBARD
Directeur clients finaux
nicolas.c@eset-nod32.fr

Références *

*Liste non exhaustive

spie batignolles
Gendarmerie nationale
HONDA
Musée de l'Armée Invalides
Allianz Suisse
Canon

Partenaires

MEMBRE DU DISPOSITIF
CYBERMALVEILLANCE.GOUV.FR
RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité
CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

Offres

Légères, efficaces et actuelles : les diverses solutions ESET protègent le patrimoine numérique des entreprises, en prenant en compte les contraintes liées au télétravail et nomadisme grandissant.
S'appuyant sur le moteur maintes fois primé NOD32, nos clients nous recommandent pour notre simplicité de déploiement, d'administration et notre capacité à assurer une protection contre les menaces courantes autant que les menaces ciblées (APT) et ransomwares.

Protégez vos postes de travail, serveurs et terminaux mobiles
Les solutions de sécurité ESET endpoint allient technologie multicouche, machine learning et expertise humaine pour offrir un juste équilibre entre performance, détection et faux positifs.

Pilotez la sécurité de vos terminaux depuis un point central
Offrant une visibilité complète et des fonctionnalités d'administration puissantes, ESET PROTECT (sur site ou dans le Cloud) simplifie le déploiement, l'administration et la gestion au quotidien.

Contrez les attaques ciblées (APT) et prévenez les menaces zero-day
Détectez en temps réel les comportements anormaux et réagissez immédiatement grâce à ESET Inspect. Identifiez les menaces inconnues avec ESET LiveGuard Advancede grâce à une Sandbox Cloud qui simule le comportement d'un utilisateur pour contrer les techniques d'évasion.

Protégez vos données et sécurisez vos moyens d'accès
Protégez vos données en les chiffrant avec ESET Endpoint Encryption et renforcez leurs accès avec une double authentification assurée par ESET Secure Authentication.

Services

Professional Services
Des techniciens experts sont d'astreinte pour répondre aux besoins en cybersécurité des entreprises avec une assistance 24h/24, 7J/7, proposant également Déploiement, Upgrade et Health Check.

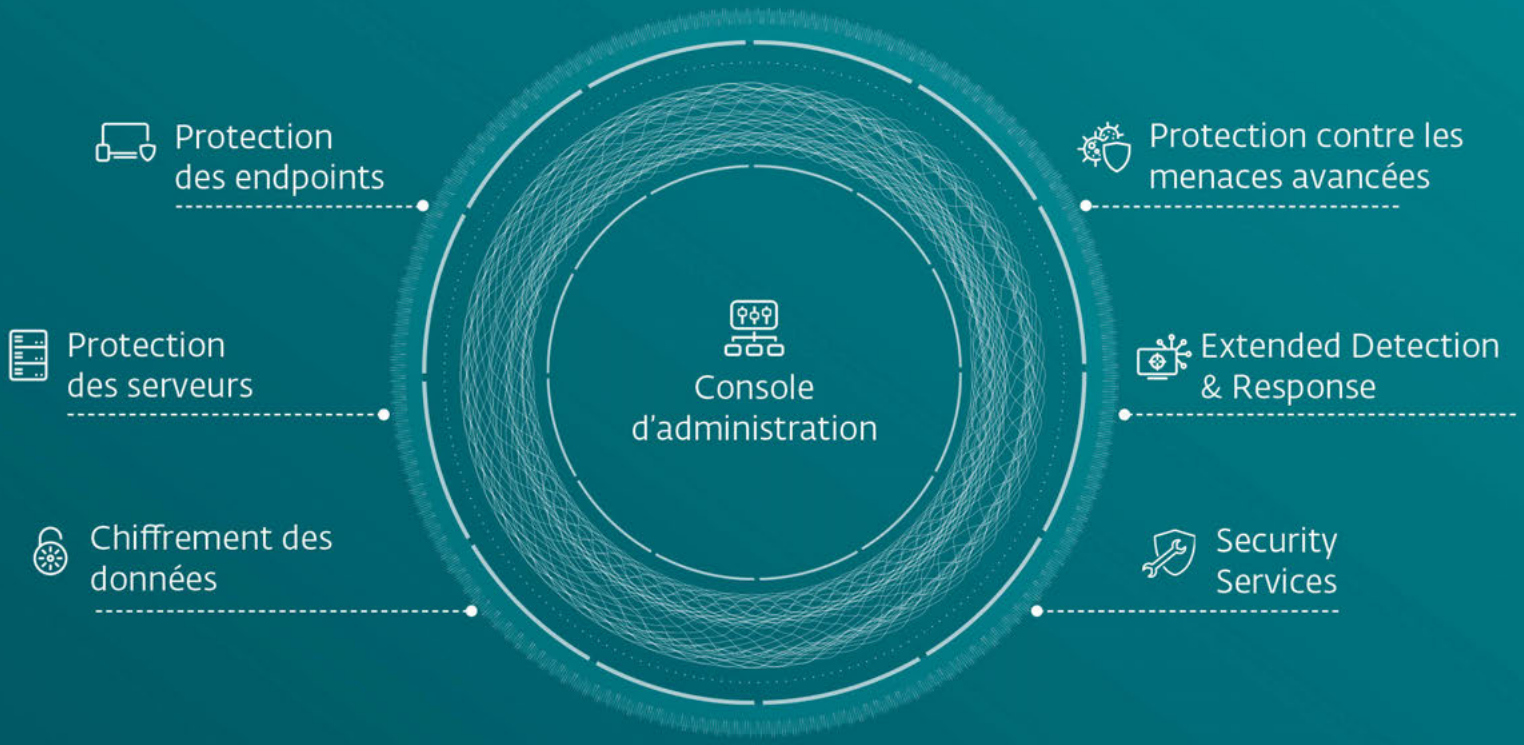
Security Services pour Endpoints & EDR
ESET Security Services pour Endpoints fonctionnent avec vos produits de sécurité ESET afin de fournir une solution de sécurité complète qui agit de manière préventive, réactive et proactive. Accélérez également la détection et la remédiation des incidents liés à l'EDR grâce à la recherche proactive et la surveillance des menaces avec ESET Threat Monitoring et ESET Threat Hunting.

**Source : Gartner Inc, Magic Quadrant for Endpoint Protection Platforms, Peter Firstbrook, Lawrence Pingree, Dionisio Zumerle, Prateek Bhajanka, Paul Webber, August 20, 2019.*

PROTECT MDR

PROTÉGEZ L'AVENIR DE VOTRE ENTREPRISE

Protection maximale de votre environnement informatique, avec une gestion complète des cyber-risques et une expertise de nos experts



Premium Support

www.eset.com/fr

FORTINET

Société : Fortinet France SARL
Adresse : Tour Alto 2-8 Boulevard de Neuilly / 4 Place des Saisons / 92400 Courbevoie / France
Tel : +33 (0) 1 80 42 05 40
Mail : **france_marketing@fortinet.com**
Site Web : **www.fortinet.com/fr**

Nom des marques
Les marques de Fortinet incluent, sans s'y limiter : Fortinet, FortiGate, FortiGuard Labs, FortiCare, FortiDeceptor, FortiManager, FortiAnalyzer, FortiOS, FortiASIC, FortiMail, FortiClient, FortiEDR, FortiNDR, FortiSIEM, FortiSandbox, FortiWiFi, FortiAP, FortiSwitch, FortiWeb, FortiADC, FortiCloud, FortiCNP, FortiNAC, FortiAI, FortiSASE…

Spécialisations :

Next Generation Firewall, Data Center&IPS, Endpoint Security, Virtualized Next-Generation Firewall, Secure Wi-Fi, Application Delivery Controllers, Security Subscriptions, Sandbox, Web Application Firewall, AWS/Azure/GCP Security, DDoS, Management, Email Security, SIEM, Cloud Access Security Broker, Identity and Access Management, Network Access Control, SD-WAN, Endpoint protection, SASE, Zero Trust

Chiffres clés :

CA : 2021 : $3.34 milliards
Effectifs : 11508 employés



Dirigeant
Entrepreneur expérimenté, Ken Xie a débuté sa carrière en créant sa première entreprise de sécurité réseau, Stanford InfoSystem, Inc. en 1993. Quelques années plus tard, il créera NetScreen (NASDAQ: NSCN), avant de fonder Fortinet en 2000, dont il est l'actuel PDG.



Contact
Le bureau de représentation français est dirigé par Mme Claire Souhaut, Country Manager, qui possède plus de 30 années d'expérience sur le marché IT français.

Fortinet (NASDAQ : FTNT) rend possible un monde numérique auquel nous pouvons toujours faire confiance grâce à sa mission de protection des personnes, des appareils, des applications et des données partout dans le monde. C'est pourquoi les plus grandes entreprises, les fournisseurs de services et les organisations gouvernementales du monde entier choisissent Fortinet pour accélérer en toute sécurité leurs échanges numériques. La plateforme Fortinet Security Fabric offre des protections étendues, intégrées et automatisées sur toute la surface d'attaque numérique, sécurisant les appareils, les données, les applications et les connexions critiques du Datacenter au cloud en passant par le travail à domicile. Classé au premier rang pour le nombre d'appliances sécurisées délivrées dans le monde, Fortinet compte plus de 595 000 clients qui lui font confiance pour protéger leurs organisations. Et le Fortinet NSE Training Institute, une initiative du Training Advancement Agenda (TAA) de Fortinet, propose l'un des programmes de formation les plus vastes et les plus larges du secteur afin de rendre la formation à la cybersécurité et les nouvelles opportunités de carrière accessibles à tous. Pour en savoir plus, consultez le site https://www.fortinet.com/fr, *le blog Fortinet ou FortiGuard Labs.*

Offres

Des réseaux filaires/sans fil aux plateformes de messagerie, applications Web, bases de données et davantage, les solutions Fortinet sécurisent les infrastructures réseau et les données d'entreprise, dans leur intégralité, permettant ainsi aux organisations utilisatrices de garder la main sur leurs réseaux, leurs utilisateurs et leurs données. En parallèle, les solutions de reporting et de gestion centralisées de Fortinet permettent de gérer et de surveiller tous les environnements, de quelques équipements à plusieurs milliers d'appliances et d'agents sur les postes clients. Les utilisateurs bénéficient ainsi d'une administration simplifiée et d'une visibilité précise sur leur statut de sécurité en temps réel.

Services

FortiGuard Labs est l'organisme de renseignement et de recherche sur les menaces de Fortinet. Sa mission est de fournir aux clients de Fortinet les meilleurs renseignements sur les menaces de l'industrie afin de les protéger contre les activités malveillantes et les cyberattaques sophistiquées. Il est composé de chasseurs de menaces, chercheurs, analystes, ingénieurs et spécialistes des données parmi les plus compétents de l'industrie, travaillant dans des laboratoires de recherche spécialisés dans le domaine de la menace dans le monde entier. FortiGuard Labs surveille en permanence la surface d'attaque mondiale en utilisant des millions de capteurs réseau et des centaines de partenaires de partage de renseignements. Il analyse et traite ces informations en utilisant l'intelligence artificielle (IA) et d'autres technologies innovantes afin d'exploiter ces données pour détecter de nouvelles menaces. Ces efforts se traduisent par des renseignements sur les menaces qui peuvent être exploités en temps utile, sous la forme de mises à jour des produits de sécurité Fortinet, de recherches proactives sur les menaces pour aider les entreprises à mieux comprendre les menaces et les acteurs auxquels ils sont confrontés, et en fournissant des services de conseil spécialisés pour aider nos clients à identifier et à renforcer leur exposition à la sécurité.

Solutions

• Certifications, labels ou points forts

Fortinet possède plus de certifications produit que n'importe quel autre constructeur d'appliances de sécurité. Ces certifications délivrées par des tiers démontrent la capacité de l'entreprise à consolider de nombreuses technologies de sécurité dans un seul système tout en respectant les plus hauts standards de performances et de précisions.

La qualité des fonctions de sécurité est également certifiée par des organisations indépendantes telles qu'ICSA Labs, MITRE et Virus Bulletin 100. Plusieurs certifications gouvernementales ont également été obtenues telles que FIPS 140-2 et 140-3, Common Criteria eAL2 et eAL4+ et d'autres certifications majeures liées à IPv6 et à ISo9001. Fortinet a également reçu plus de 1269 brevets et a plus de 260 brevets en cours de validation.

• Références Clients

Fortinet possède de nombreuses références clients dans tous les secteurs d'activité et dans toutes les catégories d'entreprises parmi lesquelles en France, Lagardère Group, Novarès, la Cnaf, le CG 92, Pierre&Vacances, Lyreco, HR Path, VGRF…



FortiEDR

Permet une détection et une réponse plus rapides aux menaces

La sécurité numérique
partout où vous en avez besoin

Copyright © 2022 Fortinet, Inc. All Rights Reserved.

FORTINET®

GATEWATCHER



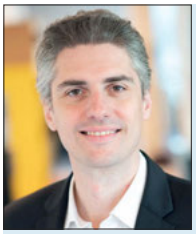
Société : GATEWATCHER
Adresse : Campus Cyber, Tour Eria, 5 rue Bellini 92800 Puteaux
Tel : 01 44 51 03 93
Mail : **contact@gatewatcher.com**
Site Web : **www.gatewatcher.com**

Spécialisations :

- **Network Detection & Response (NDR)**
- **Cyber Threat Intelligence (CTI)**
- **Network Intrusion Detection System**
- **Détection des APTs**
- **Sécurité IOT et OT**

Chiffres clés :

Création : 2015
Effectifs : Plus de 90 collaborateurs



« Grâce à un traitement machine learning et à une analyse contextuelle approfondie des comportements des utilisateurs, nos solutions permettent la détection des cybermenaces directement sur le réseau et simplifient le travail d'investigation de vos analystes »

Jacques de La Rivière,
CEO

Historique

2015 : Création de Gatewatcher
2016 : Label France Cybersécurité
2017 : Lauréat du prix spécial du jury FIC
2018 : Lauréat du Silicon Cybersecurity Awards (Meilleure solution de détection)
2019 : Qualification élémentaire de l'ANSSI pour la plateforme Trackwatch
2020 : Lauréat du prix Com Cyber et rachat du spécialiste CTI LastInfoSec
2021: Lancement de l'offre NDR AIONIQ
2022 : Première levée de fond de 25 M€ et emménagement au Campus Cyber

Révéler les menaces cyber avant qu'elles n'assombrissent votre organisation

Leader Européen de la détection d'intrusions et de menaces avancées, GATEWATCHER protège depuis 2015 les réseaux critiques des plus grandes entreprises comme des institutions publiques.

Notre vision est d'offrir une approche flexible (cloud, sur site, hybride), innovante et ouverte à l'IA, sans perturber l'architecture en place pour permettre aux équipes cybersécurité une meilleure efficacité dans la priorisation de leurs actions de remédiation.

Nos solutions apportent une amélioration immédiate grâce à une vision à 360° des cybermenaces. Elles combinent l'apprentissage automatique avec différentes méthodes d'analyse poussées du trafic réseau et sont conçues pour être évolutives et immédiatement opérationnelles pour une intégration facilitée dans les SOCs de nos clients et partenaires.



Solutions

• **Aioniq®** est une plateforme de détection et de réponse réseau (NDR) qui permet d'identifier avec certitude les actions malveillantes et les comportements suspects par une cartographie de l'intégralité des assets présents sur le SI. L'association de cette capacité avec des performances inédites d'analyse des flux réseau chiffrés, permet d'offrir une modélisation à 360° du niveau de risque cyber associé à chaque connexion entre assets et utilisateurs, pour un niveau de détection et de visibilité inégalé.

• **Trackwatch®** garantit une détection à 360° en temps réel de tous les types d'attaque et intrusions grâce à la combinaison d'algorithmes d'apprentissage automatique et de différentes méthodes d'analyse du trafic et de détection contextuelle des anomalies. Qualifiée par l'ANSSI depuis 2019, la plateforme est déployée au sein des organisations les plus critiques et les plus exposées (banque, industrie, énergie, transport..).

• **LastInfoSec®** est une plateforme de Threat Intelligence visant à fournir une amélioration immédiate de votre niveau de protection. Sa technologie exclusive associe machine learning et traitement Big Data pour générer en un temps très court un flux d'information de haute qualité sur les cybermenaces.

• **Aionbytes®** est une offre de type sandboxing permettant d'évaluer la dangerosité de fichiers et d'URL potentiellement malveillants dans un environnement contrôlé et de donner aux équipes SOC et CERT une première estimation des capacités de nuisance d'un malware, sa communication avec l'extérieur et les éventuelles modifications effectuées sur le système.

Certifications

VISA DE SÉCURITÉ
HEXATRUST CLOUD CONFIDENCE & CYBERSECURITY
CYBER TASK FORCE
FRANCE CYBER SECURITY
PRODUITS CERTIFIÉS UTILISÉS PAR LES ARMÉES FRANÇAISES

GATEWATCHER

HIGHLIGHT CYBER THREATS BEFORE THEY DARKEN YOUR BUSINESS

AIONIQ®

AUGMENTED DETECTION

NDR avec analyse comportementale et cartographique alimentée par l'IA

AIONBYTES®

DYNAMIC ANALYSIS

Analyse sandboxing dans un environnement dédié et contrôlé

TRACKWATCH®

ENHANCED DETECTION

Plateforme intelligente pour détecter et analyser les menaces et les intrusions

LASTINFOSEC®

SMARTER DETECTION

Flux CTI enrichis avec analyse et investigation contextuelle

+ 600
INFRASTRUCTURES PROTÉGÉES

100M
DE FICHIERS ANALYSÉS PAR JOUR

+ 20 Bn
D'ÉVÈNEMENTS TRAITÉS PAR JOUR

www.gatewatcher.com

Boostez l'intelligence de vos lignes de défense !

La multiplicité des attaques et la persévérance des attaquants compliquent la reconnaissance et la détection des malwares. Il faut donc trouver de nouveaux moyens de détection des attaques avancées.

Société : GLIMPS
Adresse : Digital Square – 1137A Avenue des Champs Blancs 35510 Cesson-Sévigné
Tél : 02 44 84 78 44
Mail : contact@glimps.re
Site Web : www.glimps.fr

Spécialisations :

Malware Analysis
Une solution d'investigation sur les fichiers permettant la détection, l'analyse et la caractérisation des menaces.

Chiffres clés :

Effectifs : Plus de 30 collaborateurs



Dirigeants
Cyrille VIGNON
Co-fondateur et CEO



Frédéric GRELOT
Co-fondateur & Scientist Lead



Jérémy BOUETARD
Co-fondateur et CTO



Valérian COMITI
Co-fondateur et COO

De nouvelles solutions de détection existent pour répondre à ces nouvelles attentes, notamment basées sur le DeepLearning. Elles détectent des menaces plus avancées que les solutions classiques. Seulement, elles ne parviennent pas à détecter un malware lorsqu'il a subi une forte évolution et ne fournissent pas d'explication sur celui-ci. Grâce à sa nouvelle technologie, GLIMPS peut relever ces défis ! La conceptualisation de code mise au point chez GLIMPS permet en effet de détecter les menaces et leurs divers variants.

Cette technologie parvient à combler le manque de protection des entreprises face aux groupes d'attaquants de plus en plus armés pour contourner les solutions existantes. Mais elle offre également une solution opérationnelle aux SOC et CERT pour faire face aux manques de talents en matière de sécurité. Et surtout elle parvient à détecter des menaces avancées qui se cachent sur les réseaux et les systèmes des entreprises.

Solutions

GLIMPS Malware :
GLIMPS Malware permet d'offrir une véritable Malware Analysis Platform clé en main répondant au besoin grandissant de détection et de blocages automatiques des menaces et variants de menaces. Avec l'apport d'un niveau de détails élevés sur les éléments malveillants identifiés. Connectée aux solutions de sécurité existantes chez le client (EDR, SIEM, SOAR email…), la plateforme permet de ne manquer aucune menace grâce à la combinaison des meilleurs modules d'analyses et d'extractions statiques et dynamiques. La Malware Analysis Platform apporte un contexte riche et précis sur les menaces et prend en charge la visualisation des fichiers, les règles Yara, l'export des données et les intégrations avec outils tiers. Avec une réponse moyenne inférieure à 5 secondes, le temps de détection et de qualification des incidents est réduit.

GLIMPS Audit :
Le produit GLIMPS Audit permet d'accélérer l'ensemble des analyses logicielles en boîte noire (type audit de binaire). Cet outil complet possède de nombreux avantages :

- Reverse-engineering simplifié : facilite les opérations des analystes de binaires et diminue le temps de remédiation en cas d'incident
- Analyse instantanée : comparaison avec des millions de bibliothèques en quelques secondes
- Un outil collaboratif : il permet aux équipes d'analystes d'utiliser leur propre Datasets et de partager leurs analyses avec leurs collègues
- Une solution cross-architecture
- Une intégration facilitée

Points Forts

Les avantages de notre Malware Analysis Platform :

Détecter :
- Détection des variants
- Détection des APTs et des attaques « zeroday »
- Détection et identification des menaces sur la même plateforme
- Détection des évasions de sandbox
- Détection de codes malveillants dans les attaques file-less
- Réduction de votre MTTD : analyse < 3 secondes
- Compatibilité avec les flux importants (messagerie, etc.)

Répondre :
- Réduction de votre MTTR
- Automatisation de la réponse
- Informations détaillées et contextualisées sur les menaces
- Plus de 20 moteurs d'analyses centralisés sur une seule et même plateforme
- Recherche de binaires malveillants par décomposition multicouches (orchestrateur)
- Informations de rétro-ingénierie dans des rapports simples et faciles à comprendre en moins de 3 secondes.

Historique :

2019 : Création de GLIMPS
2019 : Le prix du Public de l'European Cyber Week
2020 : Le Prix du Jury de l'European Cyber Week
2021 : Le Prix du Public des Assises de la sécurité
Avril 2021 : Levée de fonds par ACE Capital et soutenu par Breizh Up
2022 : Présence sur le radar Wavestone des start-ups de cybersécurité françaises

HeadMind Partners

Membre-Fondateur du Campus Cyber, HeadMind Partners est un acteur majeur et expert en Cybersécurité

Société : HEADMIND PARTNERS CYBER RISK & SECURITY
Adresse : 11-13 av. du Recteur Poincaré, 75016 Paris
Tél : +33 1 44 30 90 00
Mail : communication@headmind.com
Site Web : headmind.com

Le cabinet HeadMind Partners, acteur de référence du Conseil en Cybersécurité en France et à l'international, est positionné à mi-chemin entre les directions métiers et les technophiles au sein des entreprises. Pour œuvrer au dialogue entre les différents acteurs de la transformation numérique, le cabinet se positionne comme un partenaire de confiance avec :

- ***Une approche orientée clients grâce à des femmes et hommes issus des meilleures formations, continuellement formés/certifiés et dotés d'un excellent savoir-être ;***
- ***Une expertise de pointe et une capacité d'innovations (Machine Learning, Blockchain, Cybersécurité…), qui leur garantissent un bénéfice fort de différenciation ;***
- ***Des méthodes et une éthique professionnelle qui assurent leur autonomie stratégique ;***
- ***Un modèle d'entreprise, qui fait de HeadMind Partners, une ETI robuste et agile, dotée d'une forte capacité d'investissement.***

Spécialisations :

HeadMind Partners apporte une expertise sur l'ensemble de la chaîne de confiance : identification des risques, prévention, détection des attaques, gestion de crise et de ses conséquences… et accompagne une centaine d'entreprises (CAC40 & SBF120 de divers secteurs) dans :

- **La maîtrise de leur destin,** par la sécurisation des données qu'elles stockent tout en facilitant leur exploitation et leur valorisation ;
- **La résilience opérationnelle,** par une démarche proactive pour assurer les capacités de reprise et de reconstruction des services essentiels ;
- **La confiance dans les services IT :** dans un contexte géopolitique tendu, il est primordial de maîtriser le niveau de confiance de toutes les parties prenantes des entreprises et de leur supply chain.

Chiffres clés :

CA : 120 M€ CA en 2021
Effectifs : 1500 collaborateurs Monde

Offres



LABS :

Chaque LAB est composé d'un pool de consultants et piloté par un « Technical Champion » sur un sujet à enjeu (⚗ voir ci-dessus). En capitalisant sur le partage de bonnes pratiques, HeadMind Partners favorise l'appropriation d'une expertise de pointe, l'intelligence collective, une intégration en mission client plus rapide et des consultants plus agiles.

Certifications

- Certifié **ISO 9001** pour ses missions managées grâce au Système de Management de la Qualité (depuis 2013)
- Certifié **ISO 27001** (depuis 2015)
- Qualifié **PASSI & PASSI LPM**
- Labellisé **« Numérique Responsable »** en 2022



Dirigeant
Guy-Hubert BOURGEOIS
Président Directeur Général

Maxime de Jabrun,
Vice-Président Executif Monde Cyber Risk & Security et AI & Blockchain
mdejabrun410@headmind.com
+33 6 64 65 28 39

« L'explosion de la cybercriminalité (extorsion et vol), renforcée par l'usage de l'arme cyber dans les conflits géopolitiques, place la cybermenace comme l'un des principaux risques auxquels faire face. Acteur de référence dans le Conseil en Cybersécurité, HeadMind Partners a un rôle clé à jouer pour aider les entreprises, les administrations et plus largement les hommes et femmes à prendre des risques numériques. L'IA, la Blockchain, les objets connectés, l'industrie connectée, la voiture autonome… transforment progressivement et profondément nos habitudes. Plus que jamais, le rôle des experts de la cyber sera essentiel pour favoriser l'adoption et l'exploitation de ces technologies, mais aussi le développement des usages qui vont en découler de la manière la plus sûre et durable possible. »

Cybersécurité : RESTEZ INFORMÉ



L'actualité quotidienne
News, avis d'experts, témoignages, livres blancs, etc.
https://www.solutions-numeriques.com/securite/

La newsletter
Chaque lundi, comme 40 000 professionnels et décideurs, recevez la synthèse des informations.
C'est gratuit, inscrivez vous :
https://www.solutions-numeriques.com/securite/inscription/

L'annuaire : Guide papier et en ligne
Trouvez l'éditeur de solution, le prestataire de services qu'il vous faut.
https://www.solutions-numeriques.com/securite/annuaire-cybersecurite/

037CRI

Vous aider à construire une organisation plus sûre et autonome

HelpSystems est un leader des logiciels de cybersécurité fournissant des solutions à plus de 30 000 clients dans le monde. Nos suites de produits aident les entreprises à sécuriser les données critiques, à gérer la conformité et à garder une longueur d'avance sur des menaces en constante évolution.
Notre suite de sécurité des données aide les entreprises à détecter, gouverner et sécuriser leurs données sensibles tout au long de leur cycle de vie, quel que soit l'endroit où elles résident ou la manière dont elles sont partagées, tandis que notre suite de protection de l'infrastructure vous aide à réduire le bruit et à hiérarchiser les risques qui comptent réellement pour votre organisation.
Digital Guardian,Titus, Boldon James, GoAnywhere, Core Security, Cobalt Strike, Terranova Security, Digital Defense, Agari et Clearswift sont quelques-unes des marques de cybersécurité de HelpSystems



Société : HELPSYSTEMS
Adresse : 11095 Viking Dr. Suite 100, Eden Prairie, MN 55344
United States
Tél : +1 800-328-1000
Mail : **info@helpsystems.com**
Site Web : **www.helpsystems.com/fr**

Spécialisations :

Data Security & Infrastructure Protection

Chiffres clés :

CA : $800M+ (US Dollars)
Effectifs : 3000+



Dirigeants
Kate BOLSETH
Chief Executive Officer



Jim CASSENS
President



John GRANCARICH
EVP, Product & Growth Strategy



Paolo CAPPELLO
Managing Director, International

Offres

Du contrôle et de la sécurité de vos données (détection, accès, partage) à la protection de votre environnement, nous vous aidons à minimiser les menaces et à gérer la conformité. Découvrez l'ensemble de nos solutions:

- Data Protection : Titus, Boldon James, Digital Guardian & Vera
- Encryption & Managed File Transfer: GoAnywhere & Globalscape
- Email Security & Anti-Phishing : Agari, Clearswift, Phishlabs & Terranova Security
- Vulnerability Management & File Integrity : Beyond Security, Digital Defense & Tripwire
- Pen Testing & Red Teaming : Core Security & Cobalt Strike

Certifications

HelpSystems est lauréat 2021 de Cybersecurity Excellence Awards dans les catégories Data Classification, Data Leakage Prevention, Data Security et Data-Centric Security.
Digital Guardian a remporté le prix de la meilleure solution DLP aux SC Media Awards 4 années de suite.

Références Clients

Quelques clients français : ST Microelectronics, Airbus, CEA, Ministère des Armées, Pôle Emploi, ARCOM, Thales, Bouygues Telecom, Abeille Assurance, BNP Paribas, Société Générale, Crédit Agricole, ENGIE, Essilor et RATP

HelpSystems Stand LES ASSISES DE LA CYBERSECURITE 2022 : #173



Contacts
Julian GOUEZ
Partner Manager HelpSystems - **julian.gouez@helpsystems.com**

« En quelques années, HelpSystems s'est hissé comme un acteur important de la Cybersécurité. Notre suite de Protection des données (Digital Guardian, TITUS, Boldon James et VERA) en est probablement l'élément le plus emblématique, mais il ne représente qu'une partie de nos activités. HelpSystems est également présent sur la lutte contre le phishing (Phishlabs, Agari, Terranova), les échanges sécurisés de données (Globalscape, GoAnywhere) ou encore la sécurité offensive avec Core Impact ou Cobalt Strike.

HelpSystems est donc une entreprise de logiciels par excellence. Nous proposons des solutions basées sur les principes fondamentaux d'une bonne conception technologique : une qualité optimum, une expérience utilisateur et des performances toujours améliorées. »

Antoine CID
Regional Sales Manager
antoine.cid@helpsystems.com

Dalila BEN ATTIA
Regional Director for Terranova Security
dalila.benattia@terranovasecurity.com

Sebastien LE GOFF
Regional Sales Manager Southern Europe
slegoff@digitalguardian.com

HOLISEUM

Spécialiste de la Cybersécurité des Infrastructures Critiques et Industrielles

Société : HOLISEUM
Adresse : 5 place de la Pyramide
92088 Paris La Défense
Mail : **contact@holiseum.com**
Site Web : **https://www.holiseum.com**

Notre approche globale, dite holistique, de la sécurité nous confère un point de vue privilégié pour adresser efficacement les risques multifactoriels de nos clients :

- *Couverture de l'ensemble de la chaîne de valeurs des services en cybersécurité,*
- *Adresser de manière transverse les processus d'une organisation et ses environnements (IT/OT/SI Sûreté/IoT),*
- *Pluridisciplinarité faisant converger les disciplines Cybersécurité, Sûreté et Intelligence Économique.*

Nos secteurs d'interventions de référence :


Maritime

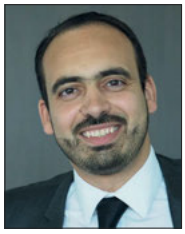

Industrie


Énergie


Banque/Finance

Spécialisations :

Cybersécurité industrielle, infrastructures critiques, Maritime, SCADA, SI de sûreté, IT, IoT, LPM, NIS, etc.



Dirigeants
Faïz DJELLOULI
Co-fondateur et Président



An NGUYEN
Co-fondateur et Directeur Général

Conseil et Services :

Nos consultants interviennent sur des missions à forte valeur ajoutée et sur des problématiques et contextes complexes au travers de nos cinq rôles :

- **CONSEILLER**
Aider votre organisation à établir ou développer une stratégie globale de sécurité.
- **AUDITER**
Une gamme complète d'audits, du plus élémentaire au plus complexe (Audit 360 de sites industriels, pentests…)
- **SÉCURISER**
Mise en œuvre de projets de sécurisation et intégration de solutions cybersécurité.
- **FORMER**
Sensibiliser les utilisateurs de votre entreprise aux problématiques de la cybersécurité.
- **INVESTIGUER**
Faire la lumière sur les compromissions avérées ou supposées.

VISA DE SÉCURITÉ — ANSSI

« La qualification PASSI de Holiseum sur les cinq portées d'audit du référentiel de l'Anssi témoigne de la diversité de nos expertises et de notre approche holistique de la cybersécurité, consistant à aborder les problématiques de cybersécurité dans toute leur complexité et leur dimension multifactorielle. »

Faïz DJELLOULI

Éducation :



SENSIBILISATION ET FORMATION

Nous organisons des sessions de **Sensibilisations** et/ou **Formations** dans divers domaines (Cybersécurité industrielle, Blockchain, IoT, Radio, etc.) adaptables à tout niveau d'expérience.
Nous développons également nos propres démonstrateurs industriels dans les domaines de la cybersécurité, la sûreté, le maritime etc.



WEB-SERIE ÉDUCATIVE

CYBER VOX est une chaîne dédiée à la vulgarisation des menaces cyber et de la cybersécurité.
Le but : faire de l'éducation populaire centrée sur la cybersécurité, mais aussi fédérer les professionnels autour d'une vision partagée.
https://bit.ly/31RPWOV



SERIOUS GAME

CYBER WARGAME est un serious game qui plonge vos collaborateurs dans un contexte d'attaque – défense cyber portant sur les actifs d'une organisation.
Le jeu Cyber Wargame est disponible en version **physique** et **numérique.**
www.cyber-wargame.com

HOLISEUM

Holiseum lance le premier Tir à Blanc de Ransomware du marché !

Problématique :

« Comment connaître le niveau de résilience de mon SI face au risque particulier du Ransomware? »

Le Tir à Blanc de Ransomware est une solution qui s'appuie sur un Ransomware de notre conception - **inoculé volontairement dans le SI client** - qui permet de tester en conditions réelles l'étendue des actions pouvant y être réalisées.

Bien qu'il soit **démuni de sa charge malfaisante**, ce ransomware déploie les techniques les plus sophistiquées utilisées par les attaquants.

LES RSSI EN PARLENT !



Replay disponible :

Découvrez les témoignages de trois de nos clients RSSI sur le Tir à Blanc de Ransomware, tel qu'ils l'ont vécu dans leurs organisations.

https://youtu.be/ljdzeoNrFPc

BÉNÉFICES ATTENDUS :

1 **Tester les défenses en place** (antivirus, EDR, sonde IDS/ IPS, réactivité du SOC etc.)

2 **Cartographier les actifs compromis, les chemins de propagation et les vulnérabilités exploitées**

3 **Identifier un plan d'actions permettant de cibler la menace des ransomwares**

Réservez dès maintenant votre créneau de présentation avec nos experts : contact@holiseum.com

HS2
Hervé Schauer Sécurité

Société : HS2
Adresse : Campus Cyber pour HS2
5 Rue Bellini – 92800 Puteaux
Tél : 09 74 77 43 90
Mail : **formation@hs2.fr**
Site Web : **https://www.hs2.fr**

Spécialisations :

Formations continues en cybersécurité techniques, organisationnelles, continuité d'activité et vie privée

Chiffres clés :

CA : 2 400 000 €
Effectifs : 2



Dirigeants

SCHAUER Hervé
Président

BENCHIKH Lynda
Directrice générale
Tél : 09 74 77 43 90
formation@hs2.fr

*« **Hervé Schauer** est un expert renommé internationalement en cybersécurité, également formateur en cybersécurité depuis 1989 et pionnier de la formation continue francophone en cybersécurité et vie privée. En 2018, il créé HS2, société de formations inter-entreprises dédiée à la cybersécurité (technique, organisationnelle, continuité d'activité, vie privée et droit de la cybersécurité) respectant les critères de qualité chers à Hervé Schauer et reposant sur :*

- *Des contenus de haut niveau (reconnus par nos participants)*
- *Des instructeurs experts qui partagent leurs retours opérationnels*
- *Des formations dispensées par deux intervenants (formateurs)*
- *Des formations certifiantes ou préparant à des certifications (ISC², Certi-Trust, AFNOR Certification, CISA...) »*

Vos formations en cybersécurité par des experts passionnés



Créée en 2018, HS2 est une société de formation inter-entreprises dédiée à la cybersécurité. Elle propose des formations certifiantes ou préparant à des certifications.

Nos principales formations :

1. **RSSI** – « Formation RSSI »
   Pour appréhender le poste de RSSI en toute sérénité

2. **ISO27RM** – « ISO27005 Risk Manager »
   Pour apprendre à faire sa gestion des risques en sécurité conformément à la méthode ISO27005

3. **SECUCYBER** – « Fondamentaux techniques de la cybersécurité »
   Acquérir les bases techniques de la cybersécurité, comprendre le fonctionnement des attaques et des mesures grâce à des exercices

4. **SECUINDUS** – « Cybersécurité des systèmes industriels »
   Comprendre la cybersécurité des systèmes industriels et les sécuriser dans leur contexte

5. **SECUBLUE** – « Surveillance, détection et réponse aux incidents de sécurité »
   Apprendre à utiliser au mieux l'existant pour détecter et répondre aux incidents de sécurité.

6. **FORENSIC1** – « Analyse inforensique Windows »
   Apprendre à investiguer sans aide extérieure des postes de travail et produire des preuves opposables en justice.

Certifications

Qualiopi processus certifié
RÉPUBLIQUE FRANÇAISE

La certification qualité a été délivrée au titre de la catégorie d'action suivante : ACTIONS DE FORMATIONS



HS2
Hervé Schauer Sécurité

Formation cybersécurité technique

DÉTECTION ET RÉPONSE • INFORENSIQUE
• SÉCURITÉ OFFENSIVE

PROGRAMME

Détection et réponse aux incidents

OSINT
Formation OSINT/CTI
SECUSOC
Surveillance, analyse et corrélation
SECUBLUE1
Surveillance, détection et réponse aux incidents de sécurité
SECUBLUE2
Surveillance, détection et réponse avancée aux incidents de sécurité
SPLUNK
Formation SPLUNK
ELASTICSEARCH
Formation ELASTICSEARCH

Inforensique

FORENSIC1
Analyse inforensique Windows
FORENSIC2
Analyse Inforensique avancée
REVERSE1
Rétroingénierie de logiciels malfaisants
REVERSE2
Rétroingénierie avancée de logiciels malfaisants

Sécurité Offensive

PENTEST1
Tests d'intrusion
PENTEST2
Tests d'intrusion et développement d'exploits
PENTESTWEB
Tests d'intrusion sur applications Web
PENTESTINDUS
Tests d'intrusion des systèmes industriels

+ 33 974 774 390

www.hs2.fr

formation@hs2.fr

Illumio empêche les failles de se transformer en « cyber-catastrophes » grâce à la Microsegmentation Zero Trust

Société : ILLUMIO
Site Web : **https://www.illumio.com/**

Le leader de la Microsegmentation Zero Trust Illumio fournit la seule suite de produits de Microsegmentation éprouvée spécialement conçue pour la sécurité Zero Trust.
Les co-fondateurs Andrew Rubin et PJ Kirner ont lancé Illumio en 2013 pour créer une technologie de sécurité remarquablement facile à utiliser qui empêche les pirates et les logiciels malveillants de se déplacer latéralement sur les réseaux.

Spécialisations :

Zero Trust, Microsegmentation, Cybersecurity

Effectifs : 500+ employées

Historique : *Fondée en 2013*



Dirigeants
ANDREW RUBIN
Chief executive officer and co-founder



PJ KIRNER
Chief technology officer and co-founder



Contact
Sebastien BERNARD
Regional Sales Director SEMEA
sebastien.bernard@illumio.com
+ 33(0)6 07 11 45 68

La Microsegmentation Illumio Zero Trust révèle les risques, isole les attaques et sécurise les données dans les applications natives du cloud, les clouds hybrides et multi-cloud, les centres de données On Premise et les terminaux physiques ou virtuels.

Illumio aide les principales organisations mondiales à renforcer leur cyber-résilience et à réduire les risques pour éviter que les violations ne se transforment en cyber-catastrophes.

Certifications

Common Criteria

SOC 2 TYPE 2 AICPA SOC

Chiffres clés :

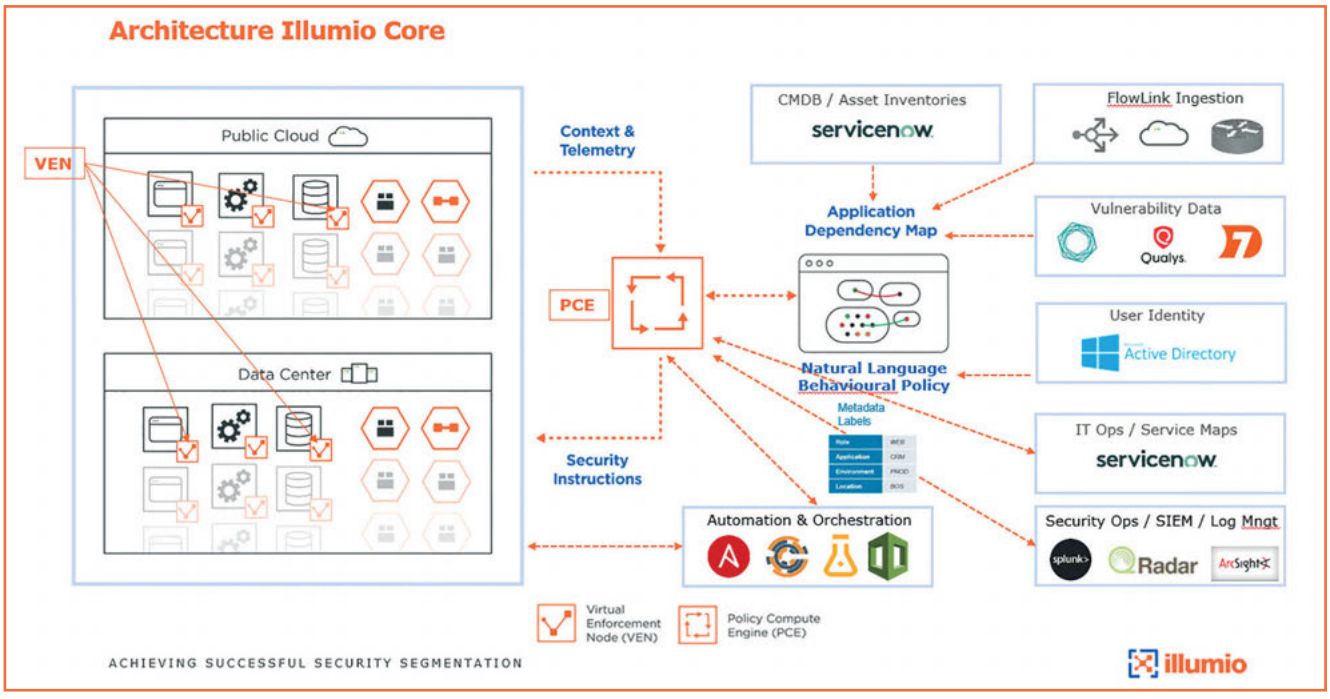
- *15% du Fortune 100*
- *6 Top Banques mondiales*
- *5 Top Compagnies d'Assurances mondiales*
- *3 Top Entreprises SaaS mondiales*

FORRESTER® NEW WAVE LEADER 2022 Microsegmentation

Illumio désigné Leader dans 2 rapports Forrester Wave™ : Microsegmentation et Zero Trust

"Illumio est le choix des organisations qui veulent une microsegmentation prédictible"

The Forrester New Wave™: Microsegmentation, Q1 2022



infoclip

Société : INFOCLIP
Adresse : 20 rue de la Michodière, 75002 PARIS
Tel : 01 43 18 19 20
Mail : **contact@infoclip.fr**
Site web : **www.groupe-infoclip.com**

Spécialisations :

- **CyberSécurité**
- **Cloud souverain**
- **Infogérance**

Historique :

Fondé en 1989, le Groupe INFOCLIP se classe aujourd'hui comme un prestataire global et incontournable de solutions cloud et sécurité pour les PME et ETI



Dirigeant
Éric MELKI
Co-Fondateur & Dirigeant
Email : **emelki@infoclip.fr**

« La Cyber Sécurité est l'enjeu majeur des PME et ETI pour les 5 prochaines années.

En effet, selon l'ANSSI, le nombre d'attaques sur les PME et ETI a été multiplié par quatre ces douze derniers mois.

En Europe, la moyenne hebdomadaire sur 2021, des attaques par organisation est de 777, en augmentation de 36 %. (CheckPoint Research). En France, en cas d'attaque par ransomware, 25 % des entreprises optent pour le paiement d'une rançon qui s'élève en moyenne à 130 000 €.

Notre objectif est d'accompagner les PME et ETI à relever ce défi pour assurer la continuité de leur business. Nous avons souhaité créer une offre simple, lisible et accessible : CyberExcellence qui s'accompagne d'un indicateur de mesure et suivi de l'exposition, CyberRésistance©.»

Certifications

ISO 27001 · ISO 9001:2015 · ITIL

Evaluez votre Score CyberRésistance© et renforcez votre cyber résilience

La sécurité est généralement considérée comme une charge et non comme un investissement. On peut considérer que c'est vrai… tant que l'entreprise n'est pas victime d'une attaque. Mais alors le prix à payer est considérable et l'on comprend pourquoi la cybersécurité est une composante incontournable au service du business de l'entreprise.

Le Score CyberRésistance© permet à l'entreprise de connaître son niveau d'exposition face aux attaques ; c'est un outil stratégique pour mesurer l'efficacité des mesures de sécurité mises en place.

Cyber excellence

Cyber résistance

- Installation de nos solutions d'analyse des vulnérabilités multi facteurs
- Identités, accès, endpoints, infrastructure et domaine internet
- Évaluation de votre score CyberRésistance
- Élaboration des recommandations déclinées en quick Win et actions de moyen terme

Sécurisation globale

- Durcissement de votre écosystème
- Déploiement des solutions antivirales / firewall / DLP / Authentification renforcée / Durcissement solutions cloud
- Sensibilisation des collaborateurs
- Mise en place de la charte informatique / conformité RGPD

SOC mutualisé

- Mise en place d'un SOC conçu pour les PME et ETI
- Détection en temps réel des menaces pesant sur vos actifs via moteur de règles comportementales et de data cyber analystes
- Identification de la menace et de sa gravité potentielle en fonction du métier et des actifs
- Classification sur la menace, blocage de l'attaque et nettoyage, correctifs et mises à jour et remis en ordre de marche
- Disponibilité du service en 24h/24 pour vos services critiques, alertes automatiques. Traitement proactif

Cellule de crise

- Préparation de vos réponses à un incident de sécurité (interne/ partenaire / fournisseur/ autorités, banques, etc)
- Gestion de votre incident de sécurité y compris la levée de doute.
- Déclenchement et gestion de la cellule de crise.
- Prise en charge de la communication interne et externe
- Gestion 24h/24 de l'évènement
- Résolution de l'incident,
- Vérification de la remise à l'état initial
- Reprise du service et capitalisation

Continuité business

- Hébergement sur notre CyberCloud souverain de vos processus métier les plus critiques
- Déclenchement de votre PRA et PCA en cas d'incident de sécurité
- Reprise des activités sur notre système de secours
- Remédiation sur votre site principal
- Restauration des données et systèmes le cas échéant sur votre site de production
- Reprise des activités au nominal
- Capitalisation

Cyber assurance

- Identification de votre risque résiduel
- Vérification de votre éligibilité en fonction de votre risque résiduel
- Analyse et mesure des écarts entre les exigences des assureurs et votre existant
- Si besoin, alignement de vos systèmes avec les attendus des assureurs
- Assistance à la sélection des contrats et compagnies d'assurance et à la réponse au questionnaire Cyber de l'assureur
- Suivi contractuel, vérification de la conformité semestrielle
- Assistance en cas de sinistre ex. plainte auprès des autorités, banques et accompagnement auprès de l'assureur

Société : IN Groupe
Nom des marques : Nexus SmartID
Adresse : 38 Avenue de New-York, 75016 Paris, France
Mail : **contact.fr@nexusgroup.com**
Site Web : **www.ingroupe.com**

Spécialisations :

Identités électroniques, PKI, Authentification forte, Credential Management, Sécurité IoT, Convergence logique et physique.

Chiffres clés :

CA : 453 M€
Effectifs : 1800 personnes

Historique

Date de création 1538



Philippe FONTON
Partner Manager
France-Belux
01 40 07 06 06



Olivier DUSSUTOUR
CEO Nexus Group
01 40 07 06 06

IN Groupe, entreprise de souveraineté numérique, procure des solutions d'identité et des services de confiance pour accompagner les États dans l'exercice de leur souveraineté, préserver l'intégrité des entreprises et protéger l'identité des citoyens.

S'appuyant sur les technologies de Nexus, IN Groupe contribue à sécuriser la société et l'économie numérique par la production et la gestion d'identités de confiance pour les personnes et les objets. La plateforme Nexus Smart ID intègre une gamme de produits permettant la mise en œuvre d'un environnement complet, centralisé et automatisé pour des identités de confiance sécurisées. Cette solution contribue à l'émission et la gestion du cycle de vie d'identités électroniques de confiance pour les employés et devices ainsi que pour l'Internet des objets (IoT). IN Groupe compte 1800 employés à travers le monde, répartis sur 8 centres de recherche et d'expertise en Europe et plus de 10 bureaux dans le reste du monde.

IN Groupe est membre du Campus Cyber



Nexus SmartID



Notre solution **Nexus Smart ID** intègre l'essentiel de notre technologie, et offre des modules standardisés, simples d'utilisation, permettant aux organisations :

- De produire et gérer les identités logiques et physiques centralement.
- De dériver les identités vers des usages mobiles.
- D'utiliser les identités électroniques en environnements multiples
- Sécuriser l'ensemble des accès et communications workforce, workplace et IoT.

Offres :

Smart ID Identity Manager
Portail de production et gestion de cartes & credential, RFID, workflows, Self-Services.

Smart ID Certificate Manager
Solutions PKI pour les utilisateurs, les devices, l'IoT.

Smart ID Digital Access
Authentification multi facteurs, Gestion des identités et des accès, ID fédération.

Smart ID Mobile APP
Mobile Virtual SmartCard pour authentification, signature et chiffrement mobile.

Smart ID Desktop APP
Virtual Smartcards pour authentification, signature et chiffrement.

Certifications

ISO 27001, Critères Communs EAL4+, TISAX

Références Clients

Orange, Electrolux, Airbus, Vinci, Ministère des Finances, Banque de France, BMW, Vodafone, Volkswagen, Siemens.



SPÉCIALISTE MONDIAL DE L'IDENTITÉ ET DES SERVICES DE CONFIANCE

IN Groupe, entreprise de **souveraineté numérique,** contribue à faire valoir pour chacun un droit fondamental : le Droit d'être soi.
Nous procurons des solutions d'identité et des services numériques sécurisés pour accompagner les **États** dans l'exercice de leur souveraineté, protéger l'identité des **citoyens** et préserver l'intégrité des **entreprises**.

IN GROUPE

LE DROIT D'ÊTRE SOI

CAMPUS CYBER
MEMBRE

I-TRACING
CYBERSECURITY EXPERT

I-TRACING, pure player des services de Cybersécurité

Société : I-TRACING
Adresse : 25 Quai du Président Paul Doumer - 92400 Courbevoie, France
Tél : +33 1 70 94 69 70
Mail : contact@i-tracing.com
Site Web : www.i-tracing.com

Créé en 2005, I-TRACING est un spécialiste français et indépendant des services de cybersécurité qui accompagne plus de 400 clients, dont 35 acteurs du CAC 40, dans la maîtrise de leurs risques cyber depuis l'anticipation des menaces pour maintenir le meilleur niveau de sécurité de leurs systèmes et actifs, à la capacité de réaction en cas d'attaques pour limiter les conséquences. I-TRACING réalise un CA de 75 millions d'euros en 2021 et compte aujourd'hui près de 400 collaborateurs principalement en France et également à Londres, Hong-Kong et Montréal.

Le développement à l'international d'I-TRACING a été porté par l'ouverture de filiales détenues à 100% par I-TRACING. Cette organisation en mode "follow the sun" permet de suivre et sécuriser l'activité des clients internationaux. Les ingénieurs, experts et analystes I-TRACING, principalement basés en France mais aussi présents à Hong-Kong et au Canada, sont ainsi disponibles à n'importe quelle heure du jour et de la nuit, quel que soit le fuseau horaire.

Spécialisations :

Services de cybersécurité

Chiffres clés :

17 ans d'expérience

75 millions d'euros de CA en 2021, soit +45% vs 2020

400 clients, dont 35 acteurs du CAC 40

420 collaborateurs dont 90% d'ingénieurs en cybersécurité en France et à l'international



Dirigeants
Laurent CHARVÉRIAT
Cofondateur et Directeur Général



Théodore-Michel VRANGOS
Cofondateur et Président



Michel VUJICIC
Directeur Technique



Lydie BERTHOME
Directrice des Ventes

Services

Au travers d'une gamme complète de services de cybersécurité allant du conseil à l'intégration aux services managés, I-TRACING réunit toutes les expertises techniques et l'expérience d'ingénierie pour répondre aux demandes des clients les plus exigeants.

- Un devoir permanent de conseil.
- Une innovation pragmatique sur les dernières technologies.
- Des SOCs et CERT avec une densité d'expertise unique sur le marché.
- Une base de connaissance partagée qui bénéficie à tous les clients.

Depuis son ancrage français, I-TRACING propose un service de surveillance, d'analyse et de réponse aux incidents **« SOC, CERT et MDR - follow the sun »** pour protéger l'activité de ses clients à travers le monde :

- 1,3M d'utilisateurs protégés dans +120 pays,
- +800 000 endpoints surveillés,
- +3 000 points de contrôle,
- + 12 milliards d'événements analysés/jour.

Offres

Fort de ses retours d'expériences, I-TRACING développe des offres de services de cybersécurité dans différents domaines d'expertises :

- **Gestion des identités & des accès (IAM)**
- **Gestion des menaces & des vulnérabilités**
- **Sécurité du Cloud**
- **Sécurité des infrastructures réseaux**
- **Sécurité des applications (AppSec)**
- **Protection des données**
- **Gestion des risques & Conformité**
- **Sécurité du workplace**
- **Sécurité industrielle & OT**

Doté d'un écosystème de plus de **50 partenaires éditeurs** leaders dans leur domaine, I-TRACING a développé une connaissance fine du marché, tout en restant agnostique. Cette expertise permet à I-TRACING de sélectionner les solutions les plus adaptées aux environnements techniques et usages de ses clients.

Certifications

Qualifications ANSSI

Label France Cyber Security

- Services Managés Sécurité
- Audit & Forensic

Référencé Cybermalveillance : assistance et prévention en sécurité numérique

Cette année I-TRACING est classée 6ème au classement Happy at Work dans la catégorie entreprise de 200 à 500 salariés. I-TRACING a obtenu la médaille d'or dans le cadre de sa certification EcoVadis et fait ainsi partie des 4% des sociétés les plus vertueuses en matière de RSE.

I-TRACING
CYBERSECURITY EXPERT

Vous accompagner dans la gestion opérationnelle de vos risques cyber

CONSEIL & AUDIT

ARCHITECTURE & INTÉGRATION

DÉTECTION & RÉPONSE

SOC & CERT

SUPPORT & SERVICES MANAGÉS

SENSIBILISATION

NOS EXPERTISES EN CYBERSECURITE

- Gestion des identités & des accès (IAM)
- Gestion des menaces & des vulnérabilités
- Sécurité du Cloud
- Sécurité des applications (AppSec)
- Sécurité des infrastructures réseaux
- Protections des données
- Gestion des risques & Conformité
- Sécurité du workplace
- Sécurité industrielle & OT

Une entreprise française, un service de surveillance et de réponse aux incidents « follow the sun » 24/7 pour suivre l'activité de nos clients à l'échelle mondiale.

FRANCE CYBER SECURITY

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

contact@i-tracing.com
01 70 94 69 70
www.i-tracing.com

ITrust éditeur de solutions souveraines et innovantes en cybersécurité

Société : ITRUST
Toulouse : 118 Route d'Espagne - 31100 Toulouse
Paris : 6 Rue du 4 Septembre, 92130 Issy-les-Moulineaux
Tél. : 0567 34 67 80
Mail : sales@itrust.fr
Site Web : www.itrust.fr

Depuis 15 ans, ITrust réunit une équipe d'experts en architecture sécurité et tests d'intrusion. Nous vous accompagnons dans votre démarche de sécurisation informatique, en vous proposant nos conseils, audits de sécurité, tests d'intrusion, MSSP, ainsi qu'une suite d'outils innovants et souverains, développés par nos équipes à Toulouse et à Paris. Notre Reveelium XDR grâce à ses trois moteurs, corrélation, Threat Intelligence et UEBA, détecte les signaux faibles et les anomalies et permet de remédier rapidement aux cyberattaques.

Spécialisations :

Audit de sécurité (dont PASSI), tests d'intrusion, scanner de vulnérabilité, XDR, supervision, détection et remédiation cybersécurité

Chiffres clés :

Effectifs : 60

Solutions

Notre activité s'articule en trois pôles :

- Expertise et conseil : tests d'intrusion, audit d'architecture, audit de configuration, audit de code, audit organisationnel, accompagnement PSSI/PRA et PCA, accompagement ISO 2700x / LPM / RGPD
- Solutions de cybersécurité : scanner de vulnérabilité IKare, Reveelium XDR
- Services managés
  - Centre de contrôle de sécurité (SOC) : nous assurons totalement ou partiellement la supervision de la sécurité de votre système d'information
  - EDR managé : nous assurons la détection, la réponse et la remédiation rapide sur vos terminaux et postes de travail



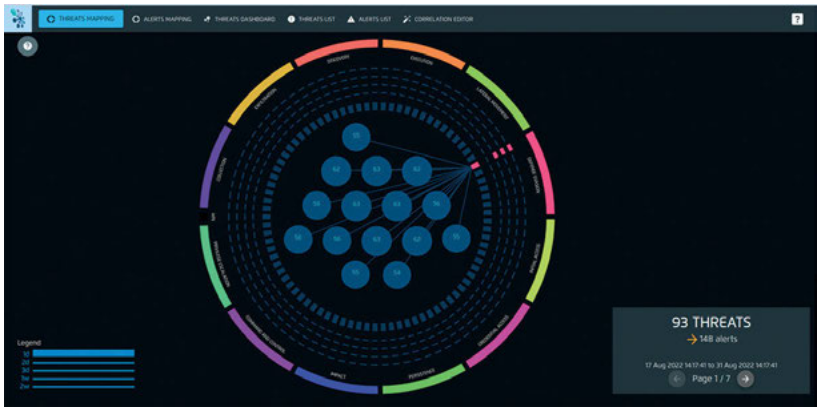
Dirigeant
Jean Nicolas PIOTROWSKI
Président Fondateur
jnpiotrowski@itrust.fr



Interface du scanner de vulnérabilités IKare
Scoring des vulnérabilités par B.U.

Labels & Prix

- Label France Cybersécurité
- TOP 25 Machine Learning Providers par CIO Applications (Reveelium)
- TOP 10 Most Valuable Cyber Security Solution Provider 2019 par CEO VIEWS
- Champions de la Croissance 2021 par les Echos & Statista
- Certifié ISO 9001 sur l'ensemble des activités de l'entreprise
- Certifié PASSI par l'ANSSI



Interface de Reveelium XDR Classification des alertes selon la Matrice Mitre

ITrust

CYBERSECURITY AS A SERVICE

LE PLUS HAUT NIVEAU DE PROTECTION EN CYBERSÉCURITÉ



PREVENIR

Scanner de vulnérabilité
Audit et expertise
cybersécurité



DETECTER

SIEM XDR UEBA
REVEELIUM



SECURISER

Centre de supervision de
la cybersécurité SOC et
EDR managés

1ER ÉDITEUR FRANÇAIS DE SOLUTIONS INNOVANTES ET EXPERT EN CYBERSÉCURITÉ

International Organization for Standardization ISO 9001

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION ANSSI

FRANCE CYBER SECURITY

FÉDÉRATION FRANÇAISE DE LA CYBERSÉCURITÉ FFCYBER

SOLUTIONS FRANÇAISES UTILISÉ PAR LES ARMÉES

www.itrust.fr

kaspersky

A vos côtés contre les cyber-menaces depuis 25 ans.



25 ans après sa création, Kaspersky, c'est aujourd'hui une équipe internationale de 4 000 personnes réparties dans 35 bureaux locaux à travers le monde. Nous travaillons avec plus de 11 000 partenaires pour apporter le meilleur de la sécurité aux 270 000 entreprises et aux 400 millions d'utilisateurs qui nous font confiance.
Notre offre de sécurité figure parmi les plus recommandées du marché. Les experts indépendants et les meilleurs analystes attribuent régulièrement les meilleures notes aux technologies Kaspersky. (kaspersky.fr/top3).
Aujourd'hui plus que jamais, Kaspersky reste engagé dans la création de technologies pour un futur cyber-immune et un monde plus sûr.

Société : KASPERSKY
Adresse : Tour Trinity
1 bis place de La Défense
92035 La Défense Cedex
Mail : **info@kaspersky.fr**
Site Web : **www.kaspersky.fr**

Spécialisations :

Protection contre les attaques ciblées, EDR, MDR, Threat Intelligence, sécurité des environnements industriels

Chiffres clés :

Effectif : + de 4000 professionnels dont 1/3 au département recherche et développement



Dirigeant
Bertrand TRASTOUR
Directeur Général

Contacts

Stéphane FICHERA
Head of enterprise sales, France
Stephane.fichera@kaspersky.com

Catherine OUDOT
Head of Channel, France
catherine.oudot@kaspersky.fr

Pascal NAUDIN
Head of B2B Sales North, West & Central Africa
pascal.naudin@kaspersky.fr

Offres

Kaspersky EDR

Logiciels malveillants, ransomwares, et nombre de menaces échappent de plus en plus à la détection. Le risque d'une attaque sérieuse est plus conséquent que jamais, tout comme les niveaux de dommages et de perturbations. Kaspersky EDR offre une visibilité approfondie sur les menaces, des outils d'analyse et d'investigation simples et une réponse automatisée avec de l'apprentissage automatique et de l'analyse comportementale. Vous êtes en mesure de détecter la menace, de la comprendre et de réagir instantanément, évitant ainsi toute interruption de votre activité. Le déploiement centralisé et la gestion unifiée de Kaspersky EDR sont disponibles depuis le cloud ou sur site.

Kaspersky Threat Intelligence Services

Les services de Threat Intelligence de Kaspersky vous donnent accès aux informations nécessaires pour détecter les cybermenaces les plus complexes. Notre équipe de chercheurs et d'analystes internationaux suit près de 900 groupes APT et vous apporte une connaissance réellement internationale des menaces. Nos services vous permettent ainsi la détection rapide des cybermenaces, la hiérarchisation des alertes de sécurité et une réponse efficace aux incidents.

7 centres de transparence

Depuis 2018, Kaspersky s'engage pour une transparence totale de ses technologies de protection, de son infrastructure et de ses pratiques de traitement des données. Nous avons ainsi ouvert, à ce jour, 7 centres de transparence (Suisse, Espagne, Etats-Unis, Malaisie, Brésil, Singapour, Japon) dans lesquels nous invitons les experts des gouvernements ou des entreprises à vérifier notre code source, nos mises à jour, nos règles de détection des menaces ainsi que nos processus techniques ou organisationnels.

Certifications

Kaspersky a obtenu plus de premières places que tous les autres fournisseurs de sécurité lors de tests indépendants. Et c'est une performance que nous répétons année après année.
www.kaspersky.com/top3

Reconnu.
Transparent.
Indépendant.

MEMBRE DU DISPOSITIF
CYBERMALVEILLANCE.GOUV.FR
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité
CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique


kaspersky
25 ans
Plus de visibilité.
Plus de puissance.
Plus de contrôle.
Vous ne pensiez pas être prêt pour l'EDR ? Maintenant, vous l'êtes.
More Visibility
More Power
More Control
Kaspersky Optimum Security
2022 AO KASPERSKY LAB.

KEYSIGHT TECHNOLOGIES

Société : KEYSIGHT TECHNOLOGIES
Adresse : France Parc Technopolis – bâtiment Olympe – ZA Courtaboeuf 3 avenue du Canada CS 50035 91941 Les Ulis Cedex
Tél. : (toll free) 0805 980333
Mail : contactcenter_france@keysight.com
Site web : https://www.keysight.com/

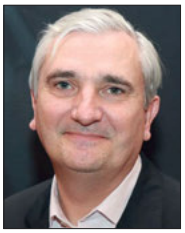
Spécialisations :

- **Tests et sécurité (IT/OT, CLOUD)**
- **Breach and Attack Simulation pour vérifier la sécurité opérationnelle**
- **Réseaux sans fil (4/5G)**
- **Solutions pour l'Automotive**
- **Solutions pour l'IOT**
- **Solutions pour l'Aerospace/defense**

Chiffres clés :

CA : $ 5 Mds en 2021
Effectifs : +15 000
Historique : création de HP en 1939, création de Keysight en 2014 suite au spin off d'Agilent

Contacts



Vincent ROUAULT
Regional Sales Manager
vincent.rouault@keysight.com



Lionel HAYERE
Channel Manager
lionel.hayere@keysight.com

Références Clients

Keysight compte parmi ses 30 000 clients des sociétés technologiques les plus innovantes ainsi que des opérateurs de services essentiels les plus importants au monde, notamment Apple, Amazon, Google, Microsoft, Facebook, NVIDIA, Qualcomm, la NASA, Thales, EDF, Airbus, RITP, TOTAL, ENEDIS, RENAULT, LA POSTE pour n'en citer que quelques-uns.

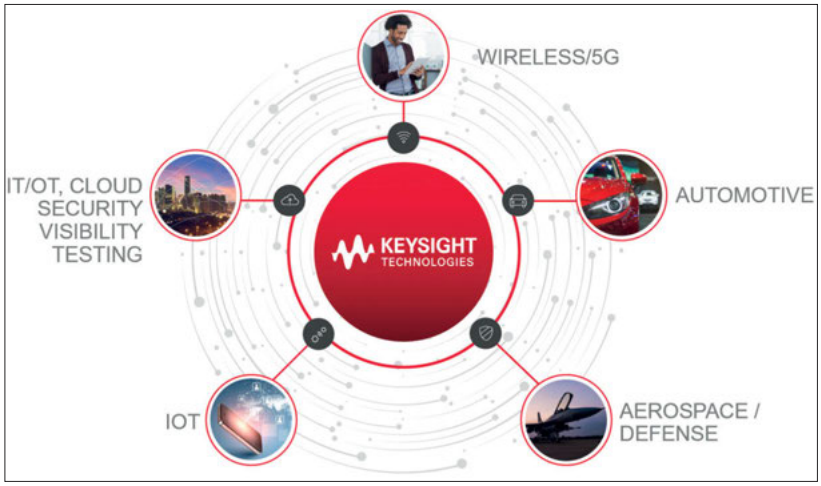
Keysight est à la pointe de l'innovation technologique, dans les domaines de la sécurité des réseaux, de la conception électronique, du test, de la fabrication électronique et de l'optimisation des processus de réponse aux incidents IT.

Nos 15 000 employés créent des solutions de classe mondiale sur les marchés de la sécurité, des communications sans fil, de la 5G, de l'automobile, du quantique, de l'aérospatiale, de la défense et des semi-conducteurs dans plus de cent pays.

Notre activité de mesure électronique a vu le jour en 1939, qui était à l'origine de la création de Hewlett Packard. Notre histoire s'appuie sur plus de 80 ans d'innovation, d'expertise en science de la mesure et le développement de relations étroites avec nos clients. Nous travaillons chaque année avec environ 30 000 clients dans le monde entier, dont la plupart appartiennent au Fortune 1000.

Offres

En 2016, Keysight a transformé la structure de l'entreprise, passant de divisions axées sur les produits à des organisations de solutions axées sur l'industrie, permettant un alignement plus étroit avec les clients.



Solutions pour les industries



SECURITE INDUSTRIELLLE OT/IT

FULL VISIBILITY

La solution de visibilité de Keysight est conçue pour les environnements IT et OT, du Datacenter au Cloud, et couvre, avec des produits dédiés, les sites OT soumis à des conditions de température et d'humidité extrêmes, ce qui fait de nous la seule société capable d'offrir une VISIBILITÉ TOTALE sur les réseaux industriels 4.0.



THREAT SIMULATOR

BREACH AND ATTACK

La sécurité n'est jamais statique. De nouvelles cyberattaques apparaissent constamment et les erreurs de configuration sont monnaie courante. Comment se préparer à des menaces en constante évolution ?

Le seul moyen est de vous attaquer avant que les pirates ne le fassent.

Plate-forme SaaS de simulation de brèches et d'attaques (BAS), Threat Simulator teste en permanence vos défenses en simulant des attaques sur votre réseau de production et vos postes de travail.



SCADA AND IT NETWORK TESTING

TEST YOUR DESIGN

BreakingPoint de Keysight peut créer une simulation de réseaux SCADA complexes et distribués comprenant des dizaines ou des milliers de points d'extrémité, des applications telles que Modbus, IEC et Bacnet, ainsi que des exploits et des logiciels malveillants. Ces simulations aident les organisations à mesurer la résilience des systèmes, à prendre des décisions d'achat, à former les équipes d'exploitation sur les incidents de sécurité SCADA et à prendre des décisions sur le déploiement de nouvelles technologies.

KEYSIGHT TECHNOLOGIES



Eliminate the blind spots!

ACCELERATE INNOVATION TO CONNECT AND SECURE THE WORLD

Keysight enhances your security with total visibility solutions, from IT Cloud down to extreme conditions OT/ICS environments.

KEYSIGHT TECHNOLOGIES

www.keysight.com

Distributeurs : ARROW abbakan

KUDELSKI SECURITY



Kudelski Security est une entreprise leader dans le domaine de la cybersécurité, dont l'objectif principal est de remettre en cause le statu quo. Nous collaborons avec nos clients afin de renforcer leur confiance en matière de cybersécurité, leur résilience aux menaces et la protection de leurs données grâce à un ensemble unique de solutions comprenant conseils, technologies, services de sécurité managés et innovation personnalisée. Avec des bureaux en Europe (Suisse, France – Paris, Allemagne, Royaume-Uni, Espagne) et à travers les États-Unis, nous sommes forts d'une longue tradition d'ingénierie et d'innovation, qui nous permet de développer des solutions à même de résoudre les défis de cybersécurité les plus complexes auxquels sont confrontés nos clients.

Société : KUDELSKI SECURITY
Adresse : Route de Genève 22
CH-1033 Cheseaux-sur-Lausanne
Suisse

86, Rue Henri Farman
92130 Issy-les-Moulineaux
France

Tel : +41 21 732 01 01
Mail : info@kudelskisecurity.com
Site Web : www.kudelskisecurity.com

Spécialisations :

- **Services de sécurité managés pour environnements IT, Cloud, Endpoints et OT 24 h/24, 7 j/7**
- **Services managés de détection et de réponse aux menaces (MDR)**
- **EDR managé**

Chiffres clés :

Revenus bruts 2021 (Kudelski Security) : 167 millions de dollars

Revenus 2021 (Groupe Kudelski) : 779 millions de dollars

Effectifs Kudelski Security : 400+



Dirigeants
Andrew HOWARD
CEO



David CHETRIT
VP Sales EMEA

Services

Services de sécurité managés

- Services de sécurité managés pour infrastructures IT, Cloud, Endpoints et OT. 24 h/24 et 7 j/7
- Services managés de détection et de réponse aux menaces (MDR)
- Surveillance et chasse proactives des menaces
- EDR managé
- Services de réponse aux incidents
- Services de sécurité du Cloud

Conseil

- Audits et conformité
- Tests d'intrusion avancés
- Évaluation stratégique de programmes de cybersécurité
- Conception et développement de programmes de cybersécurité
- Programme d'accompagnement des CISO/RSSI

Technologies

- Évaluations de technologies
- Conception et architecture de cybersécurité
- Implémentation et migration de technologies

Innovation

- Sécurité des produits connectés
- Services de sécurité IoT
- Évaluation et validation de la sécurité logicielle et matérielle et analyse forensique
- Sécurité des blockchains

Certifications

- Certifié ISO 27001:2013
- Certifications CERT *(Computer emergency Response Team)*
- Membre actif du FIRST *(Forum of Incident Response and Security Teams)*
- Nos laboratoires avancés sont accrédités par l'ANSSI pour délivrer la certification de sécurité CSPN

Distinctions

Nous recevons régulièrement des distinctions pour nos services MDR de la part de :

Gartner
FORRESTER®
FROST & SULLIVAN

Références Clients

Pernod Ricard
Créateurs de convivialité

mgen
GROUPE VYV

CANAL+

suez

L'ORÉAL

GROUPE APICIL

En France, un nombre croissant d'entreprises nous font confiance

« Kudelski Security connaît un solide développement en France depuis 2018. Un nombre croissant d'entreprises fait appel à nos services de sécurité managés innovants, et notamment à nos services managés de détection et de réponse aux menaces pour les environnements IT, Cloud, Endpoints et OT/ICS, fournis à travers notre Cyber Fusion Center basé en Suisse. Nos services de sécurité managés et de réponse aux incidents ont d'ailleurs été distingués par de nombreux analystes tels que Gartner, Forrester et IDC.»

David CHETRIT,
VP Sales EMEA

LuxTrust : créez un parcours digital sécurisé grâce à nos solutions de confiance numérique

Société : LUXTRUST
Adresse : 121, avenue des Champs-Elysées, 75008 Paris, France
Tél : 01 72 71 85 71
Mail : **sales@luxtrust.com**
Site Web : **www.luxtrust.com**

Leader des services de confiance en Europe, LuxTrust est une Autorité de Certification et un Prestataire de Services de Confiance Qualifié (PSCQ). La société développe depuis 2005 une large gamme de solutions qui facilite la transformation numérique des organisations. Certifiée selon le règlement européen eIDAS, LuxTrust opère des services comme la création et validation de signatures électroniques, l'archivage électronique ou l'horodatage.

Spécialisations :

- **Services de confiance : signatures et cachets électroniques, validation de la signature électronique, archivage, horodatage qualifié**
- **Dématérialisation et transformation numérique**
- **Gestion de consentement et protection de données personnelles**
- **Certificats électroniques et identités numériques**
- **Authentification forte**

Dirigeants



Fabrice ARESU
Directeur général
fabrice.aresu@luxtrust.lu



Pierre GRASSET
Directeur commercial
pierre.grasset@luxtrust.lu

LuxTrust est un des prestataires offrant la plus large gamme de solutions de confiance numérique de niveau qualifié eIDAS dans l'UE. Avec une présence internationale dans plus de 170 pays, LuxTrust accompagne les entreprises en France et à l'étranger afin de les aider à intégrer ces solutions dans leurs workflows.

Des services de confiance variés et complémentaires

De par son statut d'Autorité de Certification, toutes les solutions LuxTrust sont certifiées avec des niveaux de confiance, de responsabilité et de confidentialité optimaux, qualifiés selon le règlement eIDAS afin de simplifier et sécuriser les activités, les échanges et les transactions numériques des citoyens et des entreprises. Parmi la large palette de services offerts, LuxTrust propose l'identité numérique, l'intégration et la validation de la signature électronique, le cachet électronique, l'horodatage des actifs numériques, ou bien même la gestion du consentement conformément au RGPD. La plateforme COSI, par exemple, permet aux clients de facilement signer et cacheter leurs documents numériques, mais aussi de dématérialiser les flux métiers en faisant appel à l'ensemble des services de confiance.

Accompagner pour mieux numériser

En plus de ces solutions offertes, LuxTrust accompagne les entreprises dans leurs parcours de transformation digitale afin qu'elles puissent facilement numériser leurs processus métiers. Dans le domaine des banques par exemple, LuxTrust les aide à intégrer la signature électronique dans leurs processus internes afin de dématérialiser l'entrée en relation, la signature de contrats et les transactions financières. De même, LuxTrust met à disposition des entreprises et sociétés d'énergie des services de cachet électronique qualifié afin de garantir l'authenticité des factures des fournisseurs d'énergie.

Une flexibilité pour accommoder les clients

Afin de mieux s'adapter aux besoins des clients et aux différentes plateformes existant sur le marché, les services de confiance LuxTrust sont basés sur une approche "confidentiality by design". Ce qui permet aux utilisateurs d'accéder à toutes sortes de services avec leur identité numérique qu'elle soit fournie par LuxTrust ou par un autre prestataire de services de confiance. En facilitant l'intégration de ces différentes identités et signatures numériques dans la plateforme LuxTrust, les clients bénéficient de plus de flexibilité pour effectuer leurs transactions avec des identités numériques qu'ils ont déjà.

Historique

2005 : Création de LuxTrust au Luxembourg

2009 : Lancement d'horodatage qualifié

2012 : Intégration de la technologie LuxTrust dans les passeports luxembourgeois

2014 : Intégration de la technologie LuxTrust dans les cartes d'identité luxembourgeoises, ces dernières pouvant être utilisées pour signer électroniquement

2017 : LuxTrust facilite la 1ère signature électronique apposée sur un acte législatif de l'Union européenne

2020 : Inauguration des bureaux LuxTrust à Paris et à Bruxelles

2022 : Inauguration des bureaux LuxTrust à Monaco

LastPass pour l'entreprise

Permettez à vos employés d'effectuer leurs tâches en toute sécurité

De l'authentification à l'accès aux mots de passe, LastPass gère tous les points d'accès de votre entreprise afin que vous puissiez minimiser les risques tout en améliorant la productivité de vos employés.

Société : LastPass
Adresse : The Reflector,
10 Hanover- Quay, Dublin,
D02 R573, Irlande
Tel : +353 1 254 1490
Mail : https://www.lastpass.com/fr/contact-sales
Site Web : https://www.lastpass.com/fr/products/business

Spécialisations :

Gestion d'identité et d'accès (IAM)

Chiffres clés :

CA : $29,4 millions
33 millions d'utilisateurs
100 000 entreprises clientes
Effectifs : 350
Historique : créé en 2003



Contacts
Patrick BRENNAN
Channel Manager France
Patrick.Brennan@goto.com
+33 6 10 24 51 96



Gwendoline DENISSE
Responsable Grands Comptes
Gwendoline.Denisse@goto.com

Solutions

Accès sécurisé, centralisé

Avec sa solution intégrée d'authentification unique et de gestion des mots de passe, LastPass Enterprise offre un contrôle de chaque point d'accès.

- **Authentification unique (SSO)**

Un catalogue de 1200+ apps pré-intégrées et des intégrations personnalisées offrent un accès transparent sans mot de passe.

- **Gestion des mots de passe**

Simplifiez l'accès à toutes les apps en créant, capturant, et remplissant automatiquement les identifiants pour n'importe quel site.

- **Accès simple et intégré**

Apps dans le nuage, mobiles, anciennes ou internes : centralisez les accès des employés à l'aide d'une solution intégrée.

Points forts

Déploiement simple à l'échelle de tous les utilisateurs

LastPass Enterprise automatise des processus informatiques clés et simplifie l'accès des employés pour favoriser la productivité du personnel.

Console d'administration performante

Quel que soit le point d'entrée, la visibilité des accès par le SI à l'échelle de l'entreprise est fondamentale pour assurer la sécurité.

Diminution de la friction pour les utilisateurs

LastPass Enterprise fournit aux employés un accès simple et rapide à leur travail ainsi qu'une solution unique pour se connecter à tout.

Poste de sécurité renforcé

Du modèle zéro connaissance aux fonctionnalités de sécurité en option, LastPass Enterprise assure la sécurité de votre actvivité.



Fonctionnalités de sécurité performantes :

- Conformité SOC 2 Type 2
- Authentification multifacteur
- Gestion des points d'accès
- Solution d'identité tout en un
- Contrôle informatique centralisé

Offres

https://www.lastpass.com/fr/business-solutions

« 80 % des failles de sécurité en entreprise sont liées aux mots de passe. LastPass est une solution tout-en-un pour la gestion des identités et des accès. Concrètement, cela signifie qu'il n'est nécessaire de se souvenir que d'un seul mot de passe maître, et LastPass s'occupe du reste. Une fois les individus débarrassés de la nécessité de se souvenir de leurs mots de passe, le risque pour l'entreprise est réduit et les collaborateurs peuvent ainsi augmenter leur productivité. LastPass s'adresse à tout le monde et chacun peut télécharger une version personnelle. Nous proposons aussi une offre professionnelle pour les entreprises de toutes tailles et issues de tous les secteurs d'activités. »

Patrick Brennan
Country Channel Manager France

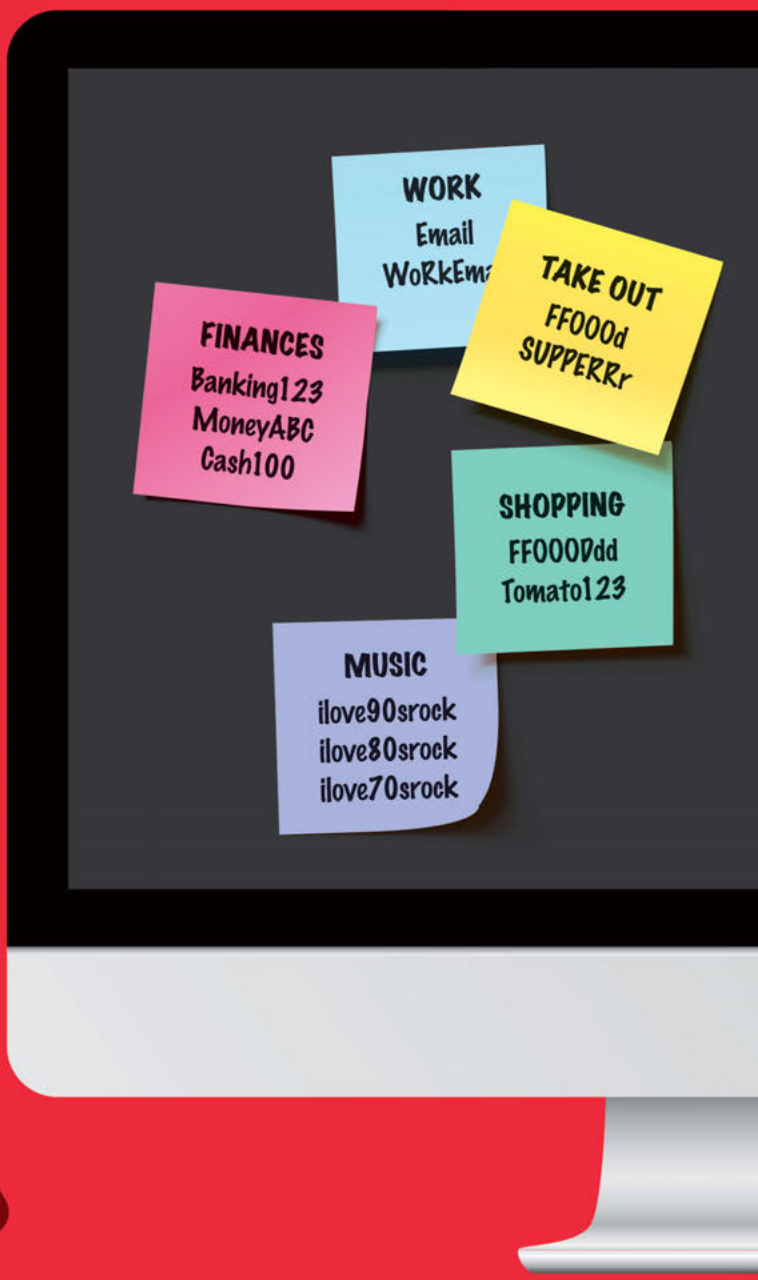
LastPass •••|

Il existe une meilleure façon de gérer les mots de passe de votre organisation.

#BeCyberSmart

Plus de vigilance. Plus de

#CyberIntelligence.



Lastpass.com

Notre prochain rendez-vous

LES ASSISES

12 - 15 Oct >> Monaco >> Stand 117

MAKE IT SAFE

Réduire les risques d'un écosystème et maintenir la conformité

Société : MAKE IT SAFE
Nom de marque : MAKE IT SAFE
Tél : 07 48 84 50 09
Mail : **contact@makeitsafe.fr**
Site Web : **https://www.makeitsafe.fr**

Make IT Safe est le logiciel métier des RSSI et des DPO : simple d'utilisation, complet et collaboratif, il accompagne le pilotage de la conformité et la maîtrise des risques cyber de l'ensemble d'un écosystème (entités, filiales, sous-traitants, tiers…). Les nombreuses fonctionnalités de Make IT Safe en font un outil adaptable à chaque organisation et modulable.

Spécialisations :

Solution logicielle innovante et 100% française, Make IT Safe outille le maintien de la conformité (selon des référentiels intégrés : RGPD, PSSI, LPM, ISO 27001, Sapin 2…), l'évaluation et le pilotage des risques en temps réel grâce à ses multiples fonctionnalités :

- **analyse de tiers**
- **audit management**
- **conformité RGPD**
- **gestion des risques cyber**
- **intégration de la sécurité dans les projets (ISP)**
- **pilotage groupe**
- **plan d'action**
- **plan assurance sécurité (PAS)**
- **projets cyber collaboratifs**

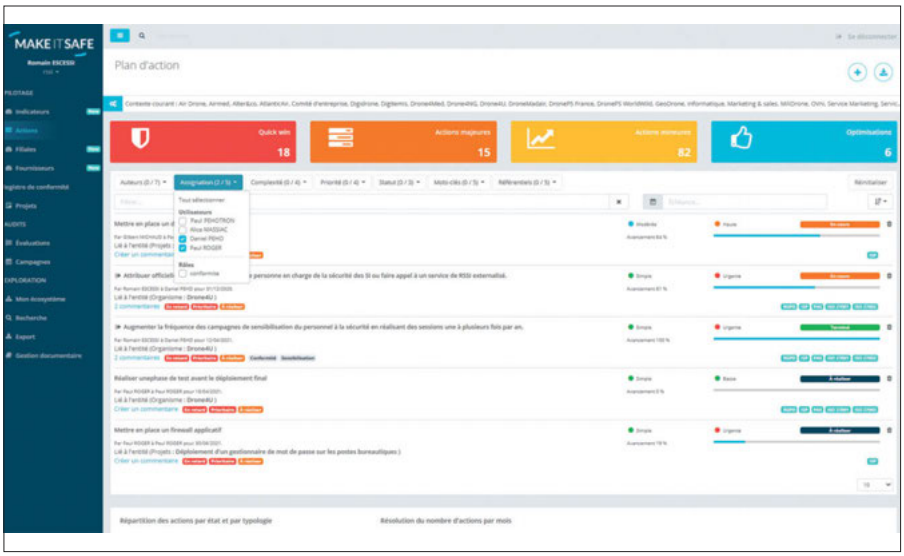


Contact
Clément LONGÉPÉ
(Responsable Partenariats)
clement.longepe@makeitsafe.fr

Yves PARIS
(Sales Manager)
yves.paris@makeitsafe.fr

Historique :

Né en 2018 de la fusion des outils Peridiag et Book My Data, le logiciel Make IT Safe a été co-construit au sein de l'entreprise Digitemis par des experts cyber, des RSSI et des juristes. En 2022, l'entité Make IT Safe est devenue une entreprise indépendante, éditrice du logiciel du même nom et possédant sa propre stratégie de développement. Notre leitmotiv : l'amélioration continue de notre logiciel et la satisfaction de nos clients.



Offres

Connaître précisément les vulnérabilités d'un écosystème et réduire durablement l'exposition aux risques cyber, voilà les 2 problématiques majeures susceptibles de remettre en cause la viabilité et la croissance des organisations.

Make IT Safe augmente leur efficacité et leur productivité grâce à des processus collaboratifs standardisés tels que notamment le plan d'assurance sécurité (PAS), l'intégration de la sécurité dans les projets (ISP), l'automatisation et le suivi des plans d'action selon l'importance des risques et en impliquant les parties prenantes. Make IT Safe accélère la transformation des organisations en améliorant leur cyber maturité par la digitalisation des processus collaboratifs.

Certifications

- Qualification PASSI par l'Anssi
- Référencement UGAP
- Bpifrance Excellence
- France Cybersecurity
- Pass French Tech

Références Clients

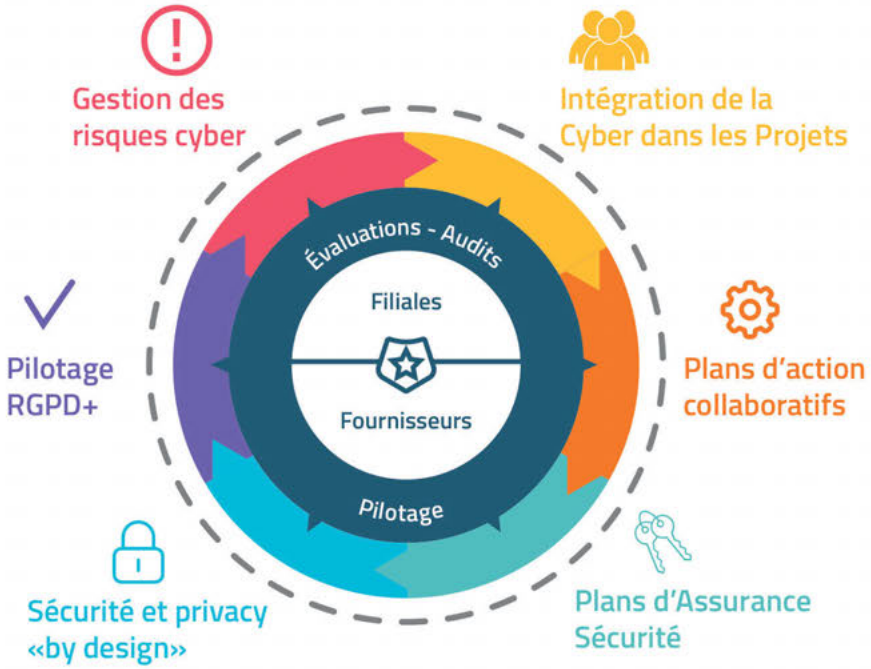
Cour des comptes · Sodebo · EDF · MAIF assureur militant · VINCI ENERGIES · SUEZ environnement

MAKE IT SAFE, LA SOLUTION POUR RÉDUIRE VOS RISQUES CYBER ET POUR GARANTIR VOTRE CONFORMITÉ

MODULABLE, COLLABORATIVE ET 100% FRANÇAISE

MAÎTRISEZ VOTRE EXPOSITION AUX RISQUES CYBER ET ANALYSEZ EN TEMPS RÉEL LA CONFORMITÉ DE VOTRE ÉCOSYSTÈME

LES FONCTIONNALITÉS DE MAKE IT SAFE



PLANS D'ACTION COLLABORATIFS

DÉPLOYEZ DES CAMPAGNES D'AUDIT AUPRÈS DE STRUCTURES INTERNES COMME TIERCES, SELON DES RÉFÉRENTIELS STANDARDS OU PERSONNALISABLES, ET COMPILEZ LES RÉSULTATS SOUS FORME DE PLANS D'ACTION.

ÉVALUATION & AUDIT MANAGEMENT

AUTOMATISEZ LA CRÉATION DE PLANS D'ACTION SPÉCIALEMENT CONÇUS POUR RÉDUIRE LES RISQUES DÉTECTÉS DANS CHAQUE ENTITÉ ÉVALUÉE.

SECURITY & PRIVACY « BY DESIGN »

STRUCTUREZ UNE APPROCHE « SECURITY BY DESIGN » EN ÉVALUANT TOUTES LES DIMENSIONS D'UN PROJET IT LORS DE CHACUNE DE SES PHASES.

PLAN D'ASSURANCE SÉCURITE

STANDARDISEZ ET INDUSTRIALISEZ LA CONTRACTUALISATION DE PLANS D'ASSURANCE SÉCURITÉ PERFORMANTS AVEC L'ENSEMBLE DES FOURNISSEURS D'UNE ORGANISATION.

PILOTAGE RGPD+

MISE EN CONFORMITÉ ET MAINTIEN DANS LE TEMPS.

PASS FRENCH TECH

Éditeur référencé UGAP-SCC

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

FRANCE CYBER SECURITY

PROGRAMEZ!

Le magazine des dévs

SÉCURITÉ & QUANTIQUE

HACKER UN DRONE

SECURE BY DESIGN

INJECTION SQL

BUG BOUNTY

DEVSECOPS

PENTEST

OWASP



SPÉCIAL ÉTÉ 2022

100% SÉCURITÉ

M 01642 - 8 - F: 6,99 € - RD

© istock

Numéro compilé en partenariat avec yogosha

Printed in EU - Imprimé en UE - BELGIQUE 7,50 € - Canada 10,55 $ CAN - SUISSE 14,10 FS - DOM Surf 8,10 € - TOM 1100 XPF - MAROC 59 DH

Anticipez vos risques cyber et protégez votre entreprise

Menaya propose une solution clé en main de cyberdéfense pour permettre aux dirigeants d'entreprises et aux équipes techniques de mieux appréhender les failles de sécurité et de les corriger, dans le but de se protéger des cyberattaques. Issue du savoir-faire israélien, Menaya bénéficie de plus de 20 ans d'expérience ayant permis l'élaboration de solutions de protection des entreprises pour une défense efficace de leurs infrastructures majeures.

Société : MENAYA
Adresse : 22 Avenue de Versailles,75016 Paris
Tél : 0 805 98 79 65
Mail : **leconrard@menaya.com**
Site Web : **www.menaya.com**

Spécialisations :

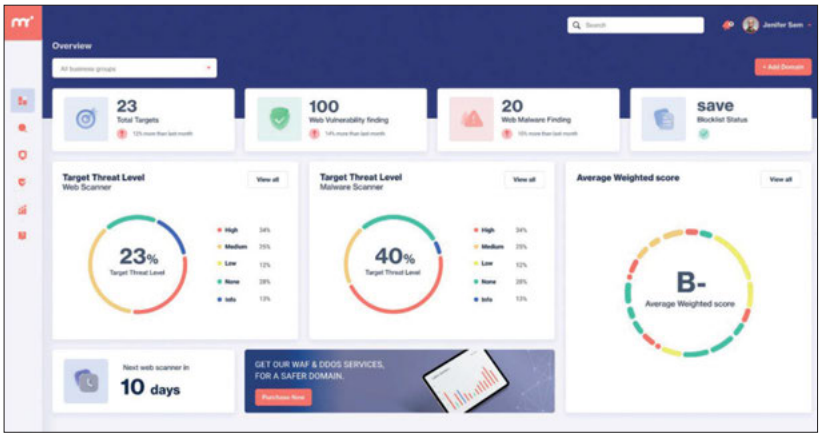
- **Audit de sécurité**
- **Scanner de vulnérabilités**
- **Rating**
- **Web Detection**



Dirigeant
Avi BARTOV
CEO
abartov@menaya.com
+972 54454 1718

Références Clients





Offre

L'offre de Menaya combine l'intégration de plusieurs outils automatisés pour identifier et détecter les attaques cyber avant qu'elles ne surviennent. L'équipe de Security Experts de Menaya a créé une réponse inédite aux incidents. Elle réunit l'ensemble des services nécessaires pour assurer la gestion de vos risques cyber et renforcer la protection et la sécurité de vos données.

Grâce à l'offre de Menaya, les PME peuvent bénéficier de la même protection que les grandes entreprises afin d'éviter les incidents de sécurité.

A l'aide de son réseau de partenaires, Menaya propose un accompagnement à la remédiation. Tout cela dans un but de prévention et de protection de vos données d'entreprise.

On estime qu'environ 80 % des cyberattaques peuvent être évitées ou atténuées grâce à une gestion préventive des risques cyber. Avec Menaya, protégez vos données et sécurisez votre entreprise.

Solutions

Grâce à nos deux solutions parfaitement complémentaires, nous examinons sur le Net et le Darknet l'ensemble de vos risques cyber, ainsi que les vulnérabilités de vos applications web. Suite aux analyses, fiches techniques et rapports vous seront remis. Ils permettront de remédier aux failles détectées.

- **Cyber Web Détection**
  Scanner de vulnérabilité et détection de malwares

La solution de Cyber détection Menaya est une combinaison de technologies automatisées visant à identifier les vulnérabilités des applications Web de votre entreprise.

Cette solution vous permet de prendre connaissance de vos faiblesses applicatives. Conçue comme outil de « hacker Ethique Virtuel », elle permet d'identifier, d'analyser et de couvrir les failles de vos applications web, les erreurs de configuration ainsi que les logiciels malveillants susceptibles de servir de porte d'entrée aux hackers.

Grâce aux rapports de vulnérabilités web, vous serez en mesure de mettre en place des correctifs pour protéger vos données. Vous renforcez ainsi la sécurité de votre entreprise avant qu'un hacker ne puisse utiliser ces failles.

- **Cyber Security Rating**
  Evaluation et classification du risque Cyber

En se fondant sur des informations publiques issues du nom de domaine et du nom d'entreprise, cette solution permet de déterminer une cartographie des risques cyber et votre niveau d'exposition aux cyberattaques. Cyber Security Rating surveille en permanence plus de 400 indicateurs de risques clés.

S'adressant à la fois aux dirigeants d'entreprises et aux équipes techniques, elle fournit des rapports détaillés permettant de mieux mesurer leur exposition face aux risques de cyberattaques. Ceci permettra de mettre en place la stratégie adéquate pour remédier aux risques et se protéger des cyberattaques.

METSYS

Présent sur l'ensemble du territoire, (Paris, Lille, Rennes, Nantes, Tours, Bordeaux, Toulouse, Aix-en-Provence, Lyon et Strasbourg), Metsys intervient sur les phases de Conseil & Gouvernance, Analyse, Intégration, Services Managés SOC/Micro SOC/GRC/CERT et Formation.

Société : METSYS
Adresse : 121 rue d'Aguesseau,
92100 Boulogne-Billancourt
Tél : +33 181 891 970
Mail : **contact@metsys.fr**
Site Web : **www.metsys.fr**

Spécialisations :

Metsys, acteur incontournable dans le conseil en cybersécurité vous apporte toute son expertise afin de garantir l'efficience de votre chaine de défense de bout en bout et contribuer à l'accélération de votre stratégie de cyber-résilience. Metsys vous propose des services et solutions afin d'anticiper ces risques et de mettre en place une gouvernance solide sur les différents points d'entrées des cyberattaques : Identité, Endpoint, Data, Réseau, Outils collaboratifs, Applications.

En complément de ses offres de conseil, d'analyse et l'implémentation de solutions, Metsys vous propose des Services Managés dédiés à la Cybersécurité, via son Centre Opérationnel de Cybersécurité (SOC).

Un dispositif organisationnel et technique permet d'assurer la supervision de la sécurité informatique d'une société et intervenir rapidement en cas d'incident ou d'attaque.

Chiffres clés :

CA prévisionnel 2022 :
70 millions d'euros

Effectif 2022 :
450 collaborateurs

Clients actifs : 500

En s'engageant vers une transition digitale, les organisations font face à des failles de sécurité de plus en plus nombreuses. Afin d'apporter une réponse efficace à leurs besoins, elles doivent considérer la sécurité selon une approche globale. Sécuriser les infrastructures ne suffit plus, il s'agit d'anticiper les cybermenaces tout en assurant la gouvernance et la conformité des données. De plus, et malgré toute la prévention, les cybercriminels sont encore capables de contourner les systèmes de protection. Les entreprises doivent être en mesure de réagir efficacement en cas d'attaque.

Metsys s'appuie sur la mise en œuvre de moyens informatiques et humains pour anticiper les menaces et sur son SOC/Micro SOC pour anticiper, surveiller et réagir aux attaques.

Notre équipe d'experts Cyber, vous aide à :
- Prévenir & détecter
- Sécuriser votre SI
- Réagir, intervenir & remédier
- Superviser & gouverner

Offres

• Centre Opérationnel de Cybersécurité :
Notre Centre Opérationnel de Cybersécurité Metsys (S.O.C.), délivre des services de sécurité 24/7 adaptés aux enjeux de nos clients. Spécialement conçu pour répondre à l'évolution constante des menaces, il fournit les éléments liés à la compromission. Nos experts cybersécurité apportent une réponse optimisée et personnalisée pour une meilleure maîtrise de la sécurité des Systèmes d'Information. Prévention des menaces - Supervision optimisée - Réponse adaptée aux exigences métiers - Gestion des vulnérabilités.

• Micro SOC :
A la différence d'un SOC qui se concentre sur la surveillance des menaces et la prise en compte des incidents à l'échelle de l'ensemble du Système d'Information, le Micro SOC se focalise sur un périmètre précis de détection. Cette approche permet de garantir un haut niveau de protection sur les éléments les plus exposés et sensibles.

• GRC as a Service :
Premier service managé pour outiller et accélérer votre démarche de conformité ! Que vous soyez dans une démarche de certification ou de maintien de cette dernière, notre offre de GRC as a Service va vous permettre d'accélérer la mise en place d'un référentiel et de faciliter le suivi de votre conformité.

« Notre ambition est de proposer à nos clients une offre de sécurité, dite, de bout en bout capable d'anticiper les cybermenaces en assurant une gouvernance renforcée et une meilleure maîtrise des données au travers d'une approche sécuritaire globale. Depuis la détection et l'anticipation des menaces jusqu'à la remédiation, la mise en conformité et la gouvernance des données, Metsys accompagne ses clients dans une démarche globale de maîtrise de la sécurité des SI, avec l'aide de ses spécialistes formés et certifiés.

Nicolas Verdier, *RSSI et Directeur de l'agence Metsys Centre Val-de-Loire.*



Dirigeant
Laurent CAYATTE
Président
et Fondateur de
Metsys



Contact
Nicolas VERDIER
Directeur des centres de services Cybersécurité.
Tel : +33 762 793 608
nicolas.verdier@metsys.fr

METSYS

Libérez-vous de la gestion de votre cybersécurité avec nos offres de services managés !

SOC

Optez pour un dispositif organisationnel et technique afin d'assurer la supervision de la sécurité informatique de votre entreprise et de garantir une intervention rapide en cas d'incident ou d'attaque.

Micro-SOC

Focalisez-vous sur un périmètre précis de détection grâce au Micro-SOC et garantissez un haut niveau de protection sur vos éléments les plus exposés et sensibles au sein de votre entreprise.



Services CERT

Supprimez vos doutes, optimisez votre gestion de crise et améliorez votre temps de réponse face aux incidents de sécurité grâce à un centre d'alerte et de réaction aux attaques informatiques.

GRC as a Service

Accélérez la mise en place d'un référentiel et facilitez le suivi de la mise en place ou du maintien de votre conformité avec les services GRC (Gouvernance, Risques & Conformité).

Faites appel à nos experts

contact@metsys.fr



Société : MIEL
Adresse : Parc Burospace 5,
91570 Bièvres
Tel : +33 1 60 19 34 52
Mail : **reseausecu@miel.fr**
Site Web : **www.miel.fr**

Spécialisations :

- **Cybersécurité Zero Trust**
- **Digital Workplace**
- **Data centers multi-clouds**
- **Réseaux du Cloud computing**

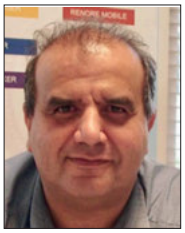
Chiffres clés :

55 collaborateurs, 400+ personnes formées chaque années, 1000+ partenaires revendeurs nous font confiance.

- 1985 : Création par Roger Bonini
- 1992 : Partenariat Citrix
- 2008 : Partenariat Palo Ato Networks
- 2021 : 12 éditeurs partenaires dans le domaine de la cybersécurité



Dirigeant
Jean-Baptiste POMMÉ
Directeur général
jean-baptiste.pomme@miel.fr



Contact
Kamel MOUHOUBI
Directeur pôle produits Cybersécurité
kamel@miel.fr

Tél. : 01 73 23 66 20

Créée en 1985, MIEL introduit sur le marché français, via un réseau de revendeurs qualifiés, les nouvelles technologies à l'attention des DSI et des Cloud providers. MIEL a connu les débuts de l'ère du PC et accompagné son développement dans les entreprises en lançant en précurseur en France les technologies mémoire Flash, Wi-Fi, client léger, optimisation WAN, virtualisation, NAC, switching 10GbE, hyper-convergence, cybersécurité Zero Trust…

MIEL propose un éventail complet et complémentaire de technologies pour sécuriser l'informatique d'entreprise à l'ère du Cloud : de la protection du endpoint à la sécurité du Cloud et des accès SaaS, en passant par le réseau, la messagerie, les identités, les données. Visibilité, Machine-learning, menaces connues et inconnues, la sécurité dernier cri pour la transformation numérique.



Distributeur des nouvelles technologies pour la cybersécurité des entreprises.

Cybersécurité opérationnelle (SOC) : Zero Trust, next-gen firewall piloté par machine-learning, SASE, SOAR, EDR, Micro-segmentation

Solutions SIEM et UEBA unifiées, collecte et corrélation de logs temps réel.

Contrôle de tous les accès au LAN. **NAC moderne**. Convergence de sécurité IT et OT.

Prise de main à distance ultra-sécurisée (PMAD). Gestion des **comptes à privilèges**.

Protection prédictive de la messagerie. Anti-spear-phishing, sécurité intégrée O365.

Détection des vulnérabilités, évaluation des risques, automatisation SecOps

Analyse réseau temps réel, Nord-Sud et Est-Ouest. NDR.

Passerelle de sécurité. VPN SSL, filtrage d'accès, SSO.

Simulation de cyberattaques as-a-Service, sur tous les vecteurs d'attaque.

Authentification forte sans mot de passe. Biométrique.

Gestion des accès et identités dans le Cloud. IAM.

Back-up des données O365.

Adoptez et maîtrisez la CYBERSÉCURITÉ dernière génération

avec

MIEL

Votre **DISTRIBUTEUR**, centre de compétence, de **SUPPORT** et de **FORMATION** pour :

BEYOND IDENTITY
BeyondTrust
citrix
FORESCOUT
illumio
illusive
logpoint
opentext Security Solutions
paloalto NETWORKS
RAPID7
vade
yuno

MIEL vous présente les réponses innovantes aux projets actuels

Nos ingénieurs rencontrent au quotidien les équipes informatiques, DSI et RSSI, partenaires revendeurs et cloud providers partout en France pour expliquer, démontrer, répondre aux questions, organiser des PoC.

Contactez-nous dès aujourd'hui pour organiser la prochaine démo !



Appelez le 01 60 19 02 30

www.miel.fr

Haute disponibilité des services critiques en ligne

Société : Nameshield
Adresse : 39 bld des Capucines
75002 Paris
Tel : +33 2 41 18 28 28
Mail : commercial@nameshield.net
Site Web : https://www.nameshield.com/

Chiffres clés :

Date de création : 1994
Effectifs : 100
Actionnariat : détenue à 100 % par ses salariés et par le fonds de dotation Esperancia.

Dirigeants
Gérard GOURJON
DG

Aymeric DE VACHON
DG

Florent BLONDEAU
DG / Dir. Etudes et développements

Contact



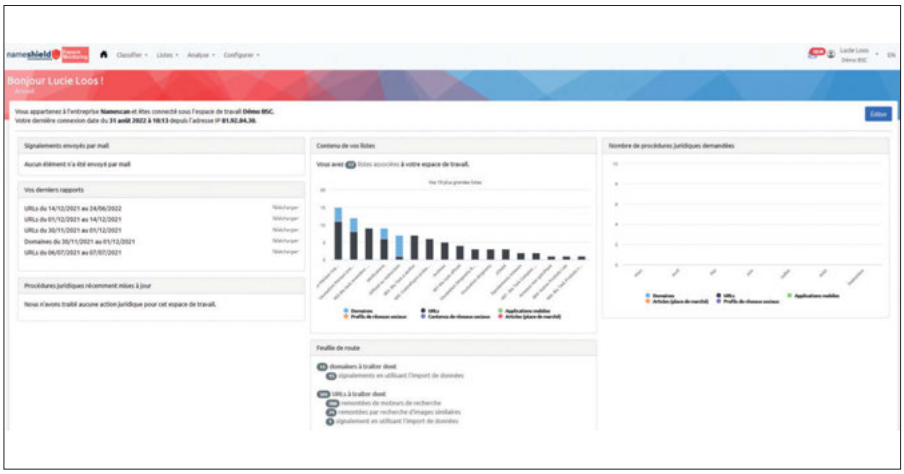
Murielle BOCHATON
Directrice commerciale
murielle.bochaton@nameshield.net

Points Forts

- **Gestion des risques** ciblant les noms de domaine et services associés
- Adaptation **aux environnements complexes**
- Politique de **développements internes / solutions propriétaires**
- Certifié **ISO 27001**
- **Conformité ANSSI**
- **Support dédié et équipes expertes**
- **Service juridique internalisé**
- Solution **DNS Premium labellisée France Cybersecurity**
- **Hébergement des données sur le sol français**
- **Engagement sociétal** avec le fonds de dotation Esperancia

Avec 28 ans d'expérience au service de ses clients et partenaires, **Nameshield** ***garantit la haute disponibilité des services stratégiques en ligne d'une entreprise/administration et assure la surveillance et la défense de leurs noms de domaine.***

Nameshield est le registrar français de référence en gestion et sécurisation de portefeuille de noms de domaine et services associés. Nameshield propose une solution globale de management, de surveillance et de défense des noms de domaine. Ses services de détection des menaces et remédiation garantissent la cyber-sécurité des marques en ligne de ses clients. Son authentificateur d'URL (breveté) permet d'agir en anticipation des fraudes.



Offres

Nameshield met à votre disposition une équipe d'experts pour vous accompagner **sur tous les aspects de la gestion des noms de domaine et des menaces associées :**

- Gestion/sécurisation de parc de noms de domaine contre le vol de données, le détournement, la non-conformité de zones DNS (SSO, Filtrage IP, MFA, gestion scope et droits...)
- Solution haute disponibilité DNS : filtrage anti-DDoS – réseau anycast – Failover – GeoIP – DNSSEC
- Sécurisation de la messagerie : Accompagnement déploiement politique SPF, DKIM, DMARC, BIMI
- CTI pour détection des menaces en ligne : phishing, usurpation d'identité, contrefaçon, sites contrefaits, faux comptes réseaux sociaux, etc.
- Solutions de remédiation et service juridique internalisé
- Mise en place de politique de sécurité et gouvernance noms de domaine
- Cartographie des risques sur les actifs numériques / audit
- Sécurité technique : certificats TLS/SSL, etc.

Certifications

Registrar français certifié **ISO 27001**, intégrant un **CERT** et disposant du Label **France Cybersecurity sur sa solution DNS Premium.**

Nameshield évolue au cœur de l'écosystème cybersécurité et participe à son évolution au travers d'associations et d'organismes tels que **Hexatrust, First, Clusif, DNS Oarc, ACN.** Nameshield est également présent au sein du groupe **ICANN Stakeholder.**

Références Clients

Administrations / Pure player du web / Banque / Energie / Industrie / Pharmaceutique / Retail / etc.

nameshield
Online Assets Security

GARANTIT LA HAUTE DISPONIBILITÉ DE VOS SERVICES STRATÉGIQUES EN LIGNE, ASSURE LA SURVEILLANCE & LA DÉFENSE DE VOS NOMS DE DOMAINE.

Le BASTION DNS : Tout le savoir-faire de Nameshield pour protéger vos noms de domaine stratégiques

Votre trafic web, vos emails et de nombreuses applications clés de l'entreprise dépendent de certains de vos noms de domaine. Ce sont vos **noms de domaine stratégiques**. La moindre indisponibilité prive d'accès vos clients et utilisateurs avec des conséquences irrémédiables sur les données, le chiffre d'affaires, l'image de marque et la fidélité.
Malheureusement ces noms de domaine attisent les convoitises et leur **surface d'attaque** est importante, entre l'exposition à des **risques administratifs**, tels que les tentatives d'usurpation du nom, et à des **risques techniques**, tels que les attaques DDoS sur l'hébergement DNS.
Garantir leur **intégrité** et leur **disponibilité**, les **surveiller**, les **analyser** et **être alerté** en cas d'attaque est primordial. Pour répondre à ces impératifs, Nameshield, fort de son savoir-faire reconnu par ses pairs et d'une expérience de près de 30 ans dans la gestion de noms de domaine critiques, a créé le Bastion DNS : service unique de protection, surveillance et d'alerte.

Les 5 piliers du Bastion DNS Nameshield :



Intégrité

Protection totale contre les tentatives d'accès, d'usurpation, de transfert, de modification ou de suppression de vos noms de domaine.



Disponibilité

Vos noms de domaine toujours disponibles, rapides et résilients face aux tentatives de cyber-attaques DDoS, DNS spoofing ou DNS cache poisoning.



Surveillance

Surveillance dédiée et continue de la disponibilité de vos noms de domaine et équipe d'astreinte 24/365.



Analyse

Analyse mensuelle du trafic de la zone et sous-zone(s), rapport d'optimisation technique et de conformité aux préconisations de l'ANSSI.



Alerte

Système d'alerte en cas de détection d'anomalie de trafic basé sur le monitoring permanent du trafic du nom de domaine.

Sécurisation de la messagerie : Accompagnement au déploiement d'une politique SPF, DKIM, DMARC, BIMI

L'email est le premier vecteur de communication en entreprise. C'est aussi le premier vecteur de cyberattaque, il est primordial de sécuriser votre messagerie, notamment contre le phishing.

Plusieurs protocoles, comme SPF, DKIM, BIMI et DMARC peuvent être déployés de façon efficace.

Nos experts DMARC Nameshield vous accompagnent dans le déploiement de cette politique, pour une sécurisation optimale.



www.nameshield.com
blog.nameshield.com

Téléchargez nos plaquettes

Opérateur français

Certifié ISO 27001 depuis 2017

Labellisé France Cybersecurity

Membre Hexatrust

Membre First

Membre de l'ACN

Membre du groupe ICANN Stakeholder

Crédit images : Nameshield | Storyset.com

NEOWAVE

Société : NEOWAVE
Nom des marques :
Weneo, Winkeo, Badgeo, Linkeo, Holdeo

Adresse : Pôle d'Activités Y. Morandat
1480, avenue d'Arménie
13120 Gardanne (France)
Tél : +33 (0)4 42 50 70 05
Mail : contact@neowave.fr
Site Web : www.neowave.fr

Le spécialiste de l'authentification forte et des transactions sécurisées

NEOWAVE est une entreprise spécialisée dans l'authentification forte et les transactions sécurisées. Notre mission principale est de protéger le patrimoine numérique des entreprises et des usagers grâce à des technologies d'authentification forte à base de composants sécurisés et de certificats numériques. Nos solutions adressent les marchés de la cybersécurité, de la confiance numérique et de la gestion des identités. Notre expertise et notre agilité permettent d'accompagner et conseiller nos clients sur des projets spécifiques.

Spécialisations :

- **Authentification forte Windows**
- **Authentification forte Web / SSO**
- **Chiffrement de données**
- **Signature électronique**
- **Sécurité des cryptoactifs**
- **Contrôle d'accès physique et gestion des temps**
- **VPN**

Chiffres clés :

CA : 710 K€
Effectifs : 7

Historique

- **NEOWAVE a été fondée en 2007 à Gardanne avec les Smart Objects comme cœur de métier.**
- **A partir de 2012, l'entreprise a recentré son activité sur le marché de la sécurité numérique.**
- **En 2022, NEOWAVE propose 3 grandes familles de produits : les solutions ID 2.0, les produits FIDO et les lecteurs de carte à puce.**

Offres :

Les produits de NEOWAVE combinent le haut niveau de sécurité offert par la carte à puce avec les avantages des technologies de stockage et de connectivités : USB, RFID / NFC et Bluetooth Low Energy (BLE). Conçus et fabriqués en France, ils répondent aux exigences de sécurité des agences européennes.

Solutions ID 2.0



Les solutions ID 2.0 de NEOWAVE sont des cartes à puce et des tokens USB avec leur Middleware (sécurisation des accès logiques et physiques). Elles constituent des solutions évolutives permettant d'héberger des certificats pour le chiffrement, la signature électronique et l'ensemble des services liés à la dématérialisation. Elles sont compatibles avec la majorité des logiciels et des équipements déployés dans les entreprises, organisations professionnelles et collectivités.

Afin de concilier confort et sécurité, nos solutions ID 2.0 permettent de gérer de manière centralisée tous les droits d'accès logiques ou physiques.

Gamme FIDO



Les standards FIDO U2F (Universal Second Factor) et FIDO2 sont adoptés par des leaders mondiaux de l'Internet. De nombreux services en ligne sont compatibles avec ces standards.

Ces produits sont parfaitement adaptés aux acteurs de la confiance numérique (signature électronique, chiffrement, lettre recommandée, consentement, services financiers, assurances, santé...). Ils s'adressent particulièrement à ceux qui souhaitent se mettre en conformité avec la règlementation eIDAS (electronic IDentification, Authentication and trust Services – Identification, Authentification et Services de Confiance Electroniques) et le RGPD.

Lecteurs de carte à puce



La gamme de lecteurs carte à puce de NEOWAVE, à contact et/ou sans contact (RFID/NFC), facilite la mise en œuvre de multiples applications sécurisées. Les produits de la gamme sont facilement installés, mis en œuvre et intégrés dans un environnement bureautique, grâce à leur compatibilité PS/SC CCID.



Dirigeant
Bruno BERNARD
Président : bruno.bernard@neowave.fr
Tel : 04 42 50 70 05

Contacts :
Corinne JOACHIN
Responsable Marketing & Communication
corinne.joachin@neowave.fr
Tel : 04 42 50 70 05

Références Clients

Certinomis, Crédit Agricole, Ministère de l'Intérieur, CertEurope, Allianz, Pierre Fabre, ChamberSign

Distributeurs européens

UGAP, Atlantis Software, Probitas, SMLB Next, Openseas, Hermitage Solutions

Certifications

CYBERSECURITY MADE IN EUROPE
Solutions 100% Made in France, en conformité avec les règlements et standards européens de sécurité numérique

Composants sécurisés certifiés EAL5+ par l'ANSSI / Produits FIDO2 certifiés par l'ANSSI

Labélisation France Cyber Security 2016, 2017 et 2019

Leader en matière de visibilité et de sécurité des réseaux informatiques industriels et de l'IoT

Société : NOZOMI NETWORKS
Adresse : Via Maria Ghioldi-Schweize 2, 6850 Mendrisio, Switzerland
Tél : +41 91 647 04 06
Mail : **info@nozominetworks.com**
Site Web : **www.nozominetworks.com**

Nozomi Networks est le leader en matière de visibilité et de sécurité des réseaux informatiques industriels et de l'IoT. L'entreprise accélère la transformation numérique en unifiant la visibilité de la cybersécurité pour les plus grandes infrastructures critiques des secteurs, de l'énergie, du manufacturing, de l'extraction minière, du transport, des bâtiments intelligents dans le monde entier.

Spécialisations :

Sécurité et visibilité OT et IoT

Chiffres clés :

Effectifs : 5 employés en France

Historique :

Fondée en 2013 par Andrea Carcano et Moreno Carullo, Nozomi Networks est devenue le leader des solutions de Visibilité et de Sécurité en environnements Industriels. Établie en Suisse, à Mendrisio, Nozomi Networks a ensuite déménagé son siège légal aux États Unis en Octobre 2016 lié à différentes levées de fonds.

Néanmoins, la conception et le développement technique de la solution restent entièrement gérés et exécutés depuis le siège historique à Mendrisio en Suisse. Ce pôle est le centre d'excellence technique de la société.



Dirigeants
Andrea CARCANO
Co-Fondateur & CPO
https://www.linkedin.com/in/andreacarcano/



Moreno CARULLO
Co-Fondateur & CTO
https://www.linkedin.com/in/morenocarullo/



Edgard CAPDEVIELLE
PDG
https://www.linkedin.com/in/edgardcapdevielle/

Offres

Nozomi Networks offre une gamme étendue de sondes de détection d'intrusion physiques et virtuelles, appelées Guardian. Ces sondes existent sous forme d'appliances physiques (durcis ou non), d'appliances virtuels compatibles avec les différentes plateformes de virtualisation ainsi que sous forme container pour l'intégration dans des solutions tiers comme Siemens RuggedCom, Gatewatcher ou autre. La gamme permet d'adresser aussi bien les sites comptant quelques centaines d'équipements que plusieurs dizaines de milliers voire millions dans le cas extrême des réseaux de compteurs d'énergie connectés ou d'équipements IoT. Dans le cas de sites complexes, étendus ou multiples, une console centrale de management est également disponible au format virtuel ou physique.

Nozomi Networks lance la solution SaaS Vantage hébergée dans le cloud qui permet une évolutivité illimitée en termes de nombre de sonde, de sites et d'équipements supervisés.

Afin d'enrichir les capacités natives des sondes Nozomi Networks propose des abonnements complémentaires :

Threat Intelligence, qui assure la mise à jour continue des bases de vulnérabilité et des bases de signatures pour les moteurs de détection par paquets YARA et indicateurs STIX. Cet abonnement permet de maintenir dans le temps les capacités de détection des risques connus.

Asset Intelligence, qui permet à la sonde d'accéder à une base de connaissance détaillée des équipements industriels, IoT ou IT susceptible d'être détecté sur le réseau des clients. Cette base contient un inventaire des caractéristiques et des fonctionnalités des équipements. Cela permet à la sonde d'être plus précise dans l'identification des anomalies et de limiter au maximum le taux de faux-positifs. Un taux de faux-positifs faible assurant une meilleure capacité de traitement des incidents et des alertes.

Services

La technologie innovante de Nozomi Networks permet d'identifier et résoudre les problèmes de configuration et de sécurité dans les réseaux de contrôles industriels. Cette analyse s'effectue de manière passive et non intrusive grâce à la sonde Nozomi Networks Guardian qui analyse le trafic de production copié via un port miroir, un TAP ou une capture au format PCAP. Cette sonde détecte automatiquement et en temps réel, les équipements présents dans le réseau de contrôle qu'il s'agisse de protocole OT, IoT ou IT. Il est alors possible de produire une cartographie détaillée des relations qui existent entre les différents équipements.

Solutions

Nozomi Networks accélère la transformation numérique en protégeant les infrastructures critiques mondiales, ainsi que les organisations industrielles et gouvernementales contre les cybermenaces.

Notre solution offre une visibilité exceptionnelle sur le réseau et les équipements, la détection des menaces et des informations pour les environnements OT et IoT.

Certifications

- Visa de sécurité pour la certification CSPN de notre produit Guardian NSG-M (version 21.3 rapport de certification ANSSI-CSPN-2021/28)
- ISO9001:2015
- ISO27001:2013
- SOC 2 TYPE 2

oodrive

Une sécurité sans faille, pour collaborer en totale confiance

Oodrive est la première suite collaborative européenne de confiance. Depuis plus de 21 ans, elle développe des solutions de gestion des contenus sensibles et propose aux entreprises une suite collaborative hautement sécurisée de solutions de partage de documents, signature électronique intégrée, gestion de ressources numériques, réunions de gouvernance, et de sauvegarde.



La sécurité ne devrait pas être un frein

La façon dont nous travaillons évolue. Les outils de collaboration du cloud sont en train de révolutionner la notion de productivité : le partage des calendriers et des documents ou le stockage des fichiers en ligne permettent aux équipes une meilleure collaboration et une meilleure coordination. Mais cette nouvelle agilité a un coût caché : **la réelle sécurité des données.**

Protégez vos contenus sensibles

L'**espionnage industriel** est une réalité et les acteurs étatiques sont en conflit actif sur la scène économique. D'autre part, le cryptage, les pares-feux et les datacenters locaux n'offrent qu'une protection incomplète contre les menaces étrangères à motivation politique : la plupart des entreprises utilisent des logiciels de productivité de fournisseurs américains. La législation, notamment le **CLOUD Act,** donne ainsi aux autorités américaines la possibilité d'accéder aux données détenues par n'importe quel fournisseur de cloud d'origine américaine, quel que soit le serveur (et sa localisation) sur lequel elles se trouvent dans le monde.

Une collaboration agile basée sur la confiance

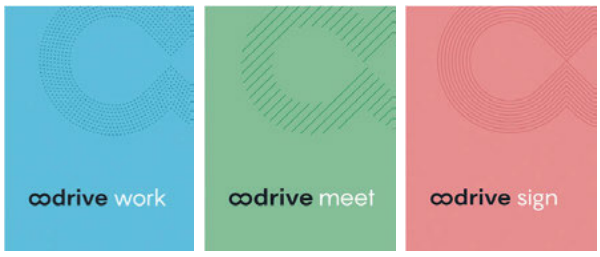
Détenue et exploitée en Europe, **Oodrive** garantit à plus d'un million d'utilisateurs les plus hauts niveaux de sécurité des données grâce aux meilleurs outils de collaboration. Les équipes peuvent enfin sécuriser tous les contenus sensibles sans ralentir leur travail.

Dotées des plus hauts niveaux de certifications de sécurité, et de plus de 20 ans d'expérience dans le domaine, les solutions souveraines ont gagné la confiance de plus de 3 500 clients qui sécurisent leurs données contre les menaces privées ou politiques.

Oodrive propose une offre de services de cloud privés qualifiée **SecNumCloud** par l'ANSSI et répond aux critères les plus stricts mis en place pour le traitement des données sensibles et l'exploitation des infrastructures critiques.
Totalement indépendante du point de vue financier, technologique et opérationnel, Oodrive permet d'être en conformité avec la législation locale et de protéger votre organisation des ingérences extraterritoriales.

Collaborez, communiquez et fluidifiez votre activité

Avec sa plateforme unifiée et sécurisée, **Oodrive** protège ainsi les processus sensibles de bout en bout. Son interface intuitive est le fruit d'une recherche approfondie sur les utilisateurs.



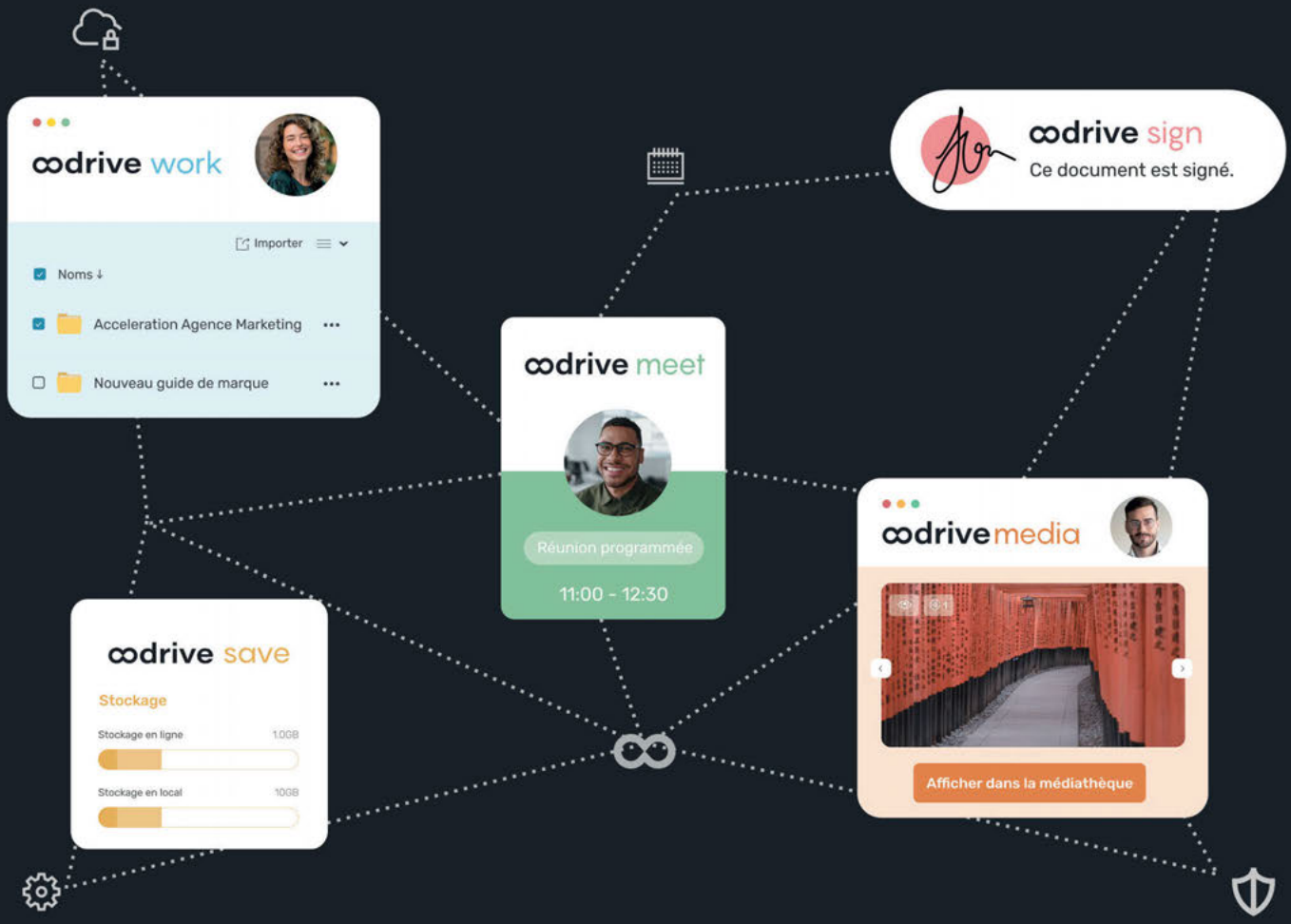
Son premier module, **Oodrive Work**, permet de créer, collaborer et partager des documents dans un environnement de confiance. Le second, qui permet d'organiser des comités et réunions de gouvernance dans un environnement confidentiel est **Oodrive Meet**. Enfin, **Oodrive Sign** combine l'efficacité de la signature électronique avec la conformité nécessaire à la construction de relations professionnelles de confiance.

Contact
Oodrive, 26 rue du Faubourg Poissonnière
75010 Paris - France - Tel : +33 (0)1 46 22 07 00
m.geffray@oodrive.com - www.oodrive.com

En savoir plus sur la signature électronique Oodrive :
https://www.oodrive.com/fr/produits/oodrive-sign/
Découvrir la suite Oodrive :
https://www.oodrive.com/fr/demander-une-demo/

oodrive

La première suite collaborative de confiance française !



Qualification SecNumCloud - ANSSI

Logiciels et infrastructure 100% français

Oodrive édite et propose des solutions collaboratives sécurisées et hautement qualifiées pour : éditer, partager, signer électroniquement et organiser des comités et réunions de gouvernance.

oodrive.com

opentext™ Security Solutions

Le leader de la cyber résilience

OpenText Security Solutions aide les clients dans leur mission de cyber résilience en intégrant des solutions de sécurité et de gestion des données et les meilleures pratiques au sein des organisations. Les solutions complètes et primées de sécurité et de gestion des données de la société offrent une cyber résilience de bout en bout qui assure la sécurité et la protection des données des organisations. Les solutions de sécurité OpenText arrêtent les mouvements latéraux si les systèmes ou les données ont été compromis afin que les entreprises puissent se remettre rapidement des cyberattaques et de la perte de données accidentelles.

Société : OPENTEXT SECURITY SOLUTIONS
Nom des marques :
Carbonite Webroot

CARBONITE + WEBROOT — opentext Security Solutions

Adresse : Cœur Défense – Tour B, 100 Esplanade du Général de Gaulle, 92931 Paris La Défense
Tél : 01 47 96 55 41
Mail : **france-smbc@opentext.com**
Sites Web : **www.carbonite.fr**
www.webroot.fr

Spécialisations :

Solutions de sauvegarde et de sécurité pour les entreprises et les fournisseurs de services gérés

Chiffres clés :

CA 2022 : 3.4 milliards de dollars
Effectifs : Environ 14 800



Dirigeants Leaders
Mark J. BARRENECHEA, *Vice Chair, Chief Executive Officer and Chief Technology Officer*



Prentiss DONOHUE *Executive Vice President, SMB/C Sales – OpenText Security Solutions*



Alexandra LEMARIGNY *Regional Sales Director – EMEA*

Solutions

Nos Solutions de Sécurité s'appuient sur notre plateforme d'intelligence contre les menaces BrightCloud.

- **Webroot Endpoint Protection :** protège les postes de travail et intercepte les comportements malicieux, les fichiers et les scripts malveillants.
- **Webroot DNS Protection :** déploie le blocage réseau au niveau du DNS et protège les utilisateurs sur réseau interne ou externe grâce au filtrage web embarqué.
- **Webroot Security Awareness Training :** propose une formation et des tests continus, pertinents et mesurables, nécessaires aux entreprises pour minimiser les comportements à risques des utilisateurs et atteindre la cyber résilience

Solutions de Protection des données
Sauvegarde Cloud ou hybride :

- **Cloud to Cloud Backup :** Protège l'intégralité de la suite Microsoft 365, Google Workspace, Salesforce, Dropbox etc.
- **Carbonite Endpoint Backup :** Protège les postes de travail Windows et Mac OS et atténue la perte journalière due aux ransomwares, aux pannes de matériels, au vols et intrusions.
- **Carbonite Server Backup :** Protection de serveur fiable pour les anciens systèmes, les systèmes physiques et les systèmes virtuels. Les données sont sauvegardées sur une cible locale et dans le Cloud sécurisé de Carbonite avec option de restauration complète ou granulaire. Il comprend aussi des sauvegardes incrémentielles perpétuelles avec des options de rétention flexibles et prend en charge à la fois vos besoins de protection et de conformité.

Mobilité des données

- **Carbonite Migrate :** permet de migrer n'importe quelle charge de travail de serveur vers une cible au choix, physique vers physique, physique vers virtuel, virtuel vers virtuel, sur site vers cloud, cloud vers site sans interruption de service.
- **Carbonite Availability :** permet aux entreprises de maintenir la plus haute disponibilité de leurs serveurs Windows et Linux en prévenant les temps d'arrêt ainsi que les pertes de données.

Certifications

OpenText—CRN: Security 100 List 2022 The 20 Coolest Endpoint And Managed Security Companies Of 2022: The Security 100 | CRN

2022 Fortress Cyber Security Awards, OpenText Security Solutions for the Data Protection

Enterprise Security Tech, The Enterprise Security Cyber Top 20 List

2022 bal InfoSec Awards : BrightCloud Threat Intelligence for Best Solution, Threat Intelligence category

« Notre expertise en matière de cyber sécurité et de protection des données permet à nos clients d'atteindre la cyber résilience. Nos solutions permettent à nos clients de se prémunir contre les ransomwares, les pertes accidentelles de données, les actes malveillants mais aussi de les aider à prendre conscience que la première ligne de défense ce sont leurs collaborateurs et que les former et les sensibiliser à la sécurité est l'une des premières étapes pour atteindre la cyber résilience.»

Alexandra Lemarigny

CARBONITE + WEBROOT
OpenText Security Solutions

Renforcez la cyber résilience pour rester opérationnel

Carbonite + Webroot
Une plate-forme puissante



La combinaison de solutions de sécurité et de gestion des données renforce la sécurité de votre entreprise et son bon fonctionnement.

En cas d'attaque ou d'accident, vous serez en mesure de résister et de rétablir rapidement la situation. Notre front uni de défense s'associe à des solutions à plusieurs niveaux pour garantir une disponibilité permanente.

Carbonite

Le bouton « Annuler » par excellence.

Sauvegarde + récupération et conformité.

Webroot

Sécurité proactive et instantanée des données.

Gardez les menaces à l'écart et protégez votre courrier électronique.

PARSEC

La société SCILLE créée en 2014 (startup éditeur de logiciel de cybersécurité) a développé en collaboration avec la DGA (ministère des armées) et le Laboratoire Bordelais de recherche en Informatique (LaBRI), la solution hautement sécurisée PARSEC qui garantit la confidentialité, l'authenticité, et l'intégrité des données sensibles partagées et stockées partout dans le monde quel que soit le cloud de stockage. L'innovation PARSEC réside dans la technologie de synchronisation permettant un partage de données sensibles stockées dans le cloud après chiffrement de bout en bout.



Société : SCILLE
Nom de marque : PARSEC
Adresse : 11 Chemin de Jalès
33160 Saint-Médard-en-Jalles
Mail : **parsec@scille.fr**
Site Web : **www.parsec.cloud**

Spécialisations :

Solution de partage et de stockage sécurisé des données sensibles dans le cloud.

Chiffres clés :

Effectifs : 12 salariés

Historique

Scille est une startup créée en 2014 par Thierry Leblond (CEO) et Emmanuel Leblond (CTO).
En 2016, avec le soutien de la DGA et en collaboration avec le LaBRI, nous avons lancé le développement de la solution de cybersécurité PARSEC, dont la commercialisation a débuté en 2020.



Dirigeants

Thierry Leblond
Co-fondateur et CEO /
Thierry.leblond@scille.fr



Emmanuel Leblond
Co-fondateur et CEO /
emmanuel.leblond@scille.fr

Offres



Parsec est un logiciel open source de distribution décentralisée de la confiance en mode ZeroTrust et Zero-knowledge.
Certifiée CSPN par l'ANSSI, Parsec est une solution collaborative ergonomique permettant le stockage souverain des données. La solution Parsec assure aux entreprises une sécurité « anti-ransomware » grâce à des fonctionnalités innovantes telles que la double authentification, la traçabilité et l'historisation des fichiers, accessibles à tout moment en cas d'attaque du serveur par des personnes malveillantes.

L'axe principal du développement de Parsec repose sur le fait que la confiance du secret donnant accès aux données chiffrées de bout en bout ne doit être confiée qu'à l'utilisateur final. Le modèle de sécurité de Parsec s'appuie donc sur cinq nouveaux paradigmes de sécurité qui sont :

- la confiance nulle ou « Zero Trust »,
- la diffusion de connaissance nulle ou « Zero Knowledge »,
- la sécurité centrée sur l'utilisateur ou « User-centered Security Model ».
- la « micro-segmentation » des données sensibles,
- le fonctionnement en mode « WORM (Write Once, Read Many) ---> fonction **ANTI-RANSOMWARE**

Certifications

- Certification CSPN délivrée par l'ANSSI
- Partenariat 3D Outscale sur la marketplace
- Partenariat Airbus développement
- Autres références et prix : Partenaires - Parsec

Références Clients

Pour notre offre Saas à 5 euros/ user/mois, nous comptons à ce jour plus d'un millier d'utilisateurs parmi lesquels L'Aéroport de Montpellier Méditerranée, des startups/ PME, ainsi que des cabinets dans divers secteurs d'activités.
Avec notre offre On-Premise nous répondons à la demande de grand compte et OIV qui souhaitent renforcer la sécurité de leurs données par des développement très spécifiques. C'est le cas par exemple de l'éditeur suédois de solutions informatique TUTUS, ou encore de la Marine Nationale pour qui nous avons déployé un système d'échange de données sécurisé en partenariat avec l'entreprise Vistory. (voir cas d'usage sur **www.parsec.cloud**)

Rendre chaque jour plus sûr et plus sécurisé que le précédent

Société : PALO ALTO NETWORKS
Adresse : 62, Avenue Emile Zola,
92100 Boulogne Billancourt
Tel : 01 70 83 22 00
Site Web : **www.paloaltonetworks.com**

Palo Alto Networks, leader mondial de la cybersécurité, façonne l'avenir grâce à une technologie qui transforme le mode de fonctionnement des personnes et des organisations. Notre mission est d'être le partenaire de choix en matière de cybersécurité, en protégeant notre mode de vie numérique. Nous aidons à relever les plus grands défis de sécurité du monde grâce à une innovation continue qui s'empare des dernières percées en matière d'intelligence artificielle, d'analytique, d'automatisation et d'orchestration.

Chiffres clés :

Plus de 85 000 clients
CA 2022 : $5,5M
Présents dans +de 150 pays



Dirigeants
Etienne BONHOMME
Vice Président & Directeur Général France

En fournissant une plateforme intégrée et en donnant les moyens à un écosystème croissant de partenaires, nous sommes à l'avant-garde de la sécurité, protégeant des dizaines de milliers d'organisations à travers les clouds, les réseaux et les appareils mobiles. Avec une large présence en Europe, Palo Alto Networks offre une expertise inégalée en matière de menaces, de réglementations et de solutions locales.

Nous proposons le portefeuille de cybersécurité le plus innovant, le plus efficace, une stratégie 'Zero Trust', et nous accompagnons nos clients à chaque étape de leur parcours de sécurité grâce à des conseils d'experts et des services associés.

Nous vous accompagnons sur :

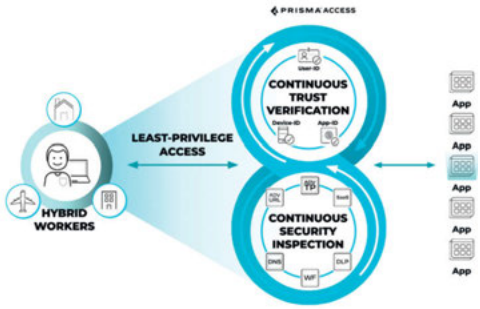
- La sécurisation de votre entreprise : Transformation du réseau
- La sécurisation du cloud : Migration vers le cloud
- La sécurisation de vos besoins à venir : Optimiser les opérations de sécurité

Des solutions nouvelle génération à la hauteur des enjeux actuels

PRISMA SASE

Sécurisez le travail hybride

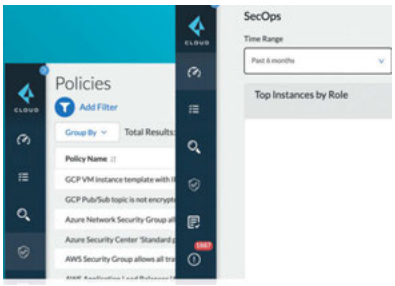
La solution SASE la plus complète du secteur. Prisma SASE offre une fondation sécurisée pour les organisations agiles et adaptées au cloud.



PRISMA CLOUD

Sécurisez tout type de cloud

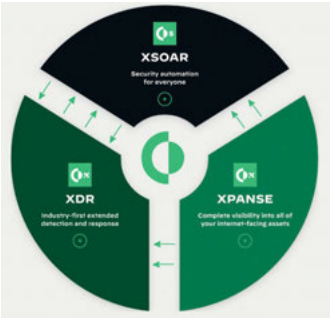
Protégez vos applications cloud-native sur tout le cycle, dans tous les clouds.



CORTEX

Automatisez vos opérations de sécurité

Offrez à vos SecOps toute la puissance de processus de détection, d'investigation et de réponse automatisés.



UNIT 42

Réagissez plus rapidement grâce à nos services de Threat Intelligence et de conseil en sécurité. Les conseils de nos experts vous aident à bloquer les cybermenaces et à y répondre.

Points forts

- Plus de 85 000 clients – dans plus de 150 pays et de multiples industries.
- Plus de la moitié des sociétés du Fortune 100 et du Global 2000 nous font confiance pour améliorer leur approche de la cybersécurité.
- Organisation implantée mondialement Amérique, Europe, Asie et Japon
- Nommé leader "Enterprise Firewall" par Forrester
- Leader du Magic Quadrant Gartner "Networks Firewall"

Certification

Certification de haut niveau de l'ANSSI

La plate-forme Palo Alto Networks a été la première à être certifiée par l'Agence Nationale de la Sécurité des Systèmes d'Information sur les critères de pare-feu de nouvelle génération, notamment les protections basées sur les applications et les utilisateurs. Les tests ont été réalisés par le CESTI et les consultants en sécurité informatique d'AMOSSYS - organismes agréés par l'ANSSI pour réaliser ces évaluations de sécurité.

Tout est visible, tout est protégé

Société : Qualys Technologies
Adresse : Maison de la Défense,
7 place de la Défense,
92400 Courbevoie
Tel : 01 41 93 35 70
Mail : **tam-fr@qualys.com**
Site Web : **www.qualys.com**

Née dans le Cloud et avec une approche novatrice de la sécurité, Qualys Cloud Platform et ses applications intégrées aident les entreprises à simplifier leurs opérations de sécurité et à réduire le coût de la conformité. Notre plateforme fournit en continu de précieux indicateurs de sécurité, et elle automatise le spectre complet des audits, de la conformité et de la protection des systèmes d'information et des applications Web.

Spécialisations :

- **Gestion des actifs IT**
- **Sécurité du SI**
- **Protection du Cloud**
- **Protection des applications web**
- **Conformité**
- **Gestion des certificats**

Chiffres clés :

CA 2021 : $411 millions
CA 2020 : $363 millions

Historique

- Qualys, fondée en 1999, est l'un des premiers fournisseurs de services dans le Cloud, et c'est aujourd'hui le principal fournisseur de solutions de sécurité et de conformité.
- L'entreprise compte aujourd'hui plus de 10 000 clients dans plus de 130 pays et elle est cotée au Nasdaq depuis 2012 sous le symbole QLYS.
- Qualys est également l'un des fondateurs de la Cloud Security Alliance (CSA).
- Quelques chiffres : + de 2000 milliards d'événements de sécurité traités, + de 6 milliards de scans IP/audits par an, 99.9996% de précision d'analyse.



Dirigeant
Sumedh Thakar
Président et CEO Qualys

Offre

Qualys aide les entreprises à rationaliser et fédérer leurs opérations de sécurité et de conformité IT au sein d'une seule et même plateforme, et à intégrer la sécurité à leur transformation numérique pour leur garantir davantage de souplesse, une activité plus dynamique et des économies substantielles.

La Qualys Cloud Platform fournit en permanence aux entreprises un service de renseignement sur la sécurité afin qu'elles puissent automatiser le spectre complet de l'audit, de la conformité et de la protection des systèmes d'information et des applications Web.

Les capteurs offrent une visibilité continue et ce sur sites, sur les points d'extrémité, sur les mobiles, dans les conteneurs ou dans le cloud. Les capteurs de Qualys Cloud Platform sont toujours actifs et offrent une visibilité continue sur tous les actifs informatiques. Déployables à distance, gérés de manière centralisée et auto-actualisés, les capteurs se présentent sous forme d'appliances physiques ou virtuelles, ou d'agents légers.

Services

La Qualys Cloud Platform c'est aujourd'hui 20 applications regroupées en 6 catégories :

- Asset Management
- IT Security
- Cloud and Containers Security
- Web Application Security
- Compliance

Solutions

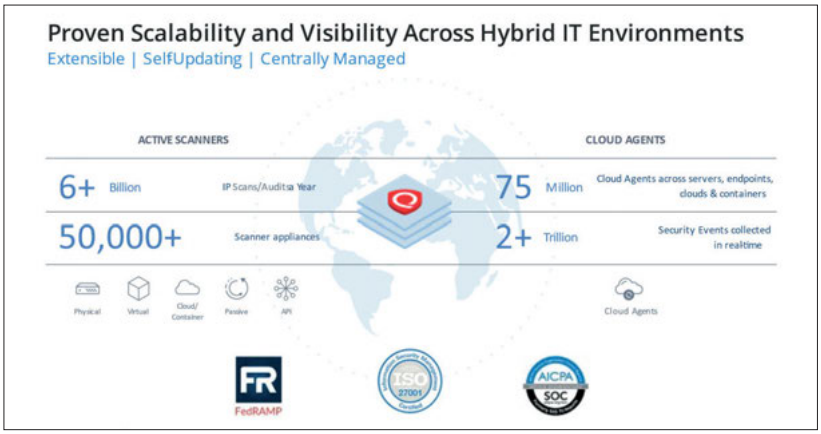
Certifications, labels ou points forts
Points forts de la Qualys Cloud Platform

- Aucun matériel à acheter ou à gérer
- Des coûts d'exploitation réduits
- Des analyses faciles à lancer
- Une plate-forme évolutive
- Des ressources actualisées
- Des données stockées en toute sécurité
- Une solution disponible dans le Cloud public, privé ou sur site

Références Clients

Clients internationaux : Microsoft, Apple, eBay, Amazon, Google, Bank of America, General electrics, PWC…

Clients en France : Accor, Adeo , Air Liquide, Altran, Axa, BPCE, Carrefour, Danone, Groupama, Kering, Orange, RATP, Rexel, Société Générale, Sodexo, St Gobain, Suez, Veolia…



Nos solutions protègent vos ordinateurs et vos données de façon optimale sur les environnements Windows et Mainframe z/OS à travers des solutions logicielles faciles à mettre en œuvre et des supports externes sécurisés, autonomes et multi-plateformes. Toutes ces solutions s'adaptent parfaitement aux besoins des clients, qu'ils soient grands comptes ou PME.

Société : QUERY INFORMATIQUE
Adresse : 1 bd Charles de Gaulle
92700 Colombes
Tél : 01 49 97 33 00
Mail : query@query-informatique.com
Site Web : www.query-informatique.com

Spécialisations :

Protection des postes de travail et des données, prise en main à distance sécurisée, connexion sans mot de passe, anonymisation des données de tests, environnements Windows et Mainframe IBM z/OS

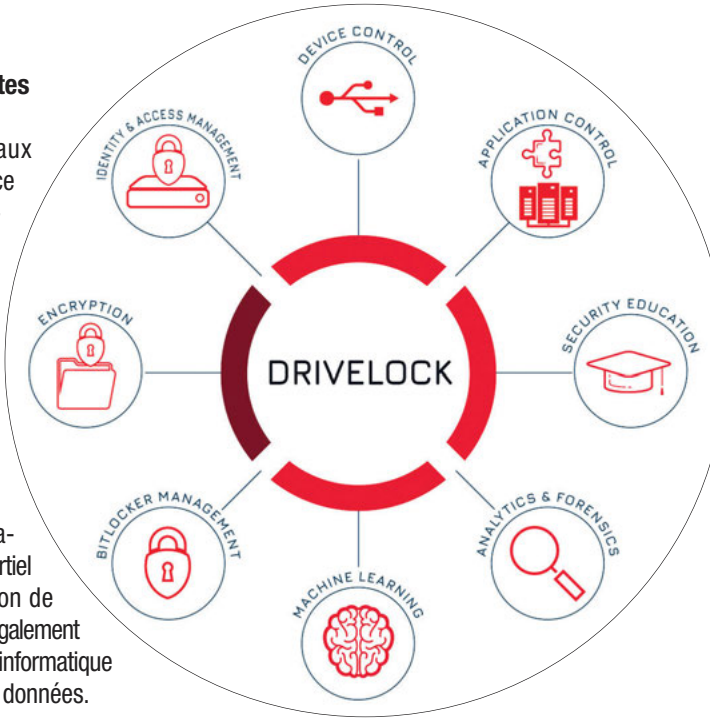
Historique :

Création : 1991

Solutions

Protection des postes de travail

Sécurisez l'accès aux postes de travail grâce à **DriveLock,** une solution facile à mettre en œuvre et très flexible. Depuis une console centralisée, adaptez vos stratégies de sécurité en fonction du type d'utilisateur avec le contrôle des périphériques externes, le filtrage des applications, le chiffrement partiel ou complet, la gestion de BitLocker, etc. Suivez également l'activité de votre parc informatique et le mouvement des données.





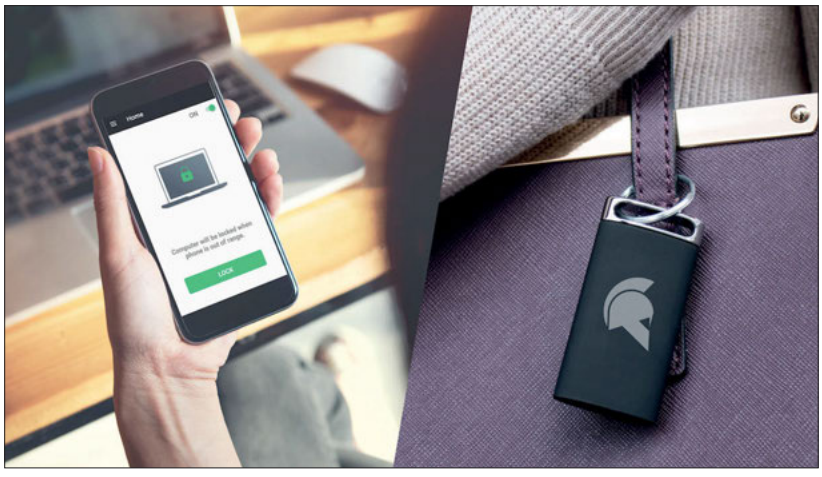
VISA DE SÉCURITÉ — ANSSI

Et plus besoin de mots de passe du fait de leur gestion automatisée et centralisée avec **GateKeeper,** la connexion aux sessions, aux applications et sites web pouvant se faire à l'aide d'un jeton de connexion, avec aussi la possibilité de générer des mots de passe dit "forts" pour l'ensemble des utilisateurs, et plus encore…

Protection des données

Nos clés USB et disques durs externes (dont la Sentry One certifiée ANSSI), chiffrés au niveau matériel, sont multi-plateformes (Windows, Mac et Linux) et très robustes, avec des capacités de stockage allant de 8 Go à 15,3 To. Les utilisateurs disposent ainsi d'un véritable **coffre-fort numérique** leur permettant de transporter des données sensibles en toute sécurité.

Une solution logicielle optionnelle, **Safe-Console,** permet la gestion centralisée de ces périphériques externes sur site ou dans le cloud. Différentes politiques de sécurité y sont paramétrables en fonction de vos besoins : politique de mot de passe, protection en écriture, restriction par types de fichiers, verrouillage d'inactivité, distribution de contenu, géolocalisation, blocage des ports USB…



Points forts :

- Gestion centralisée
- Contrôle des périphériques
- Filtrage des applications
- Chiffrement partiel ou complet
- Périphériques sécurisés
- Connexion sans mot de passe
- Audits et rapports
- Prise en main à distance multiplateformes sécurisée
- Création de jeux de tests sélectifs et anonymisés

Gérez simplement vos accès à privilèges - PAM

Basé à Rennes depuis 2014, RUBYCAT est un éditeur français de logiciels, spécialisé dans la traçabilité et le contrôle des accès sensibles au système d'information.

Fort d'une expertise reconnue dans le domaine de la sécurité des accès au SI, RUBYCAT apporte avec PROVE IT une réponse pragmatique et simple au manque de visibilité sur les actions réalisées par les comptes à privilèges.

Société : RUBYCAT
Adresse :
3 Square du Chêne Germain,
35510 Cesson-Sévigné
Tel : 02 99 30 21 11
Mail : sales@rubycat-labs.com
Site Web : www.rubycat.eu

Nom des marques :
PROVE IT (Standard, Advanced, Cluster)

Retrouvez nos webinaires sur :
www.rubycat.eu/webinaires

Spécialisations :

- **Contrôle et traçabilité des accès sensibles au SI**
- **Gestion des accès à privilèges (PAM/Bastion)**



Dirigeante
Cathy LESAGE
Dirigeante – CEO



Contact
Thomas CRIBIER
Ingénieur Avant-vente / Responsable Partenariats
thomas.cribier@rubycat.eu

Solutions

PROVE IT : La solution de PAM qui sécurise vos accès sensibles en toute facilité

Solution logicielle française certifiée en 2018 par l'ANSSI, PROVE IT s'intègre facilement dans votre environnement pour fédérer les accès sensibles au SI (Sans agent - installation en moins d'une heure).

Elle contrôle et trace les accès tiers et utilisateurs à privilèges aux ressources critiques, avec enregistrement et visualisation des sessions.

PROVE IT intègre un coffre-fort sécurisé d'identifiants secondaires (non-divulgation des identifiants des ressources critiques).

Interfaçage natif avec les solutions de gestion d'évènements (SIEM), d'authentification forte (MFA), ….

PROVE IT évolue constamment pour s'adapter à vos usages et intègre désormais nativement le protocole http/s pour la gestion de ressources web (en plus du RDP/SSH).

PROVET IT ADVANCED/CLUSTER : Pour aller plus loin dans la sécurisation de votre SI

La gamme de PROVE IT propose 3 versions, PROVE IT STANDARD intégrant toutes les fonctionnalités nécessaires à la gestion des accès à privilèges. Pour des besoins plus avancés, la version ADVANCED offre des fonctionnalités supplémentaires :

- La segmentation des droits d'administration par profil – auditeurs / opérateurs / administrateurs – à périmètre variable.
- L'API REST qui facilite les opérations d'administration les plus courantes.

Une version CLUSTER est également disponible proposant une plus forte résilience ainsi qu'une répartition de charge automatique.

Références Clients

- Ministères (DGFIP,…)
- Mairie de Vincennes
- CHU de Nîmes
- Proginov
- Semitan
- SHV Energy SRM
- Limagrain
- Cetih Renov
- Port Boulogne Calais
- Mix Buffet

Témoignages disponibles :
https://www.rubycat.eu/temoignages/

Certifications

PROVE IT certifiée Visa de sécurité – CSPN par l'ANSSI
(Réf 2018/24 - en cours de renouvellement).

PROVE IT éligible dans le cadre du Plan France RELANCE

La Gestion des accès à privilèges (PAM) *est un maillon essentiel dans la gouvernance du SI, elle fait partie des 10 différentes solutions identifiées par l'ANSSI comme pouvant faire l'objet d'un projet d'acquisition dans le cadre du plan* ***France Relance.***

*Pour rappel, l'objectif du volet cybersécurité de France Relance piloté par l'****ANSSI*** *est de renforcer la sécurité de l'Etat, des administrations, des collectivités territoriales, des établissements de santé et des organismes au service des citoyens (social, santé, formation, audiovisuel, sécurité) tout en dynamisant l'écosystème industriel français.*

Notre solution PROVE IT est éligible dans le cadre d'un ***« Appel à projets »*** *de France Relance. Si vous faites partie d'un organisme éligible, n'hésitez pas à nous contacter pour échanger ensemble sur votre projet. Un apport minimum de 30 % est attendu de la part du bénéficiaire. Le montant du cofinancement de l'ANSSI est défini suivant la maturité du projet et les objectifs du plan de relance. Plus d'informations disponibles sur le site de l'ANSSI.*



PROVEIT by rubycat

PROGINOV opte pour le **PAM PROVEIT**

Émilien RICHARD, administrateur système, réseau et sécurité, explique son choix de la solution française PROVE IT pour la **gestion de leurs accès à privilèges.**

*Hébergeur depuis 2001, **Proginov** propose à ses clients d'externaliser leur système d'information. Proginov a opté pour un positionnement à forte valeur ajoutée. La qualité de ses services et de ses infrastructures largement reconnue, couvre des secteurs d'activités aux exigences fortes en termes de sécurité informatique.*

Le **contexte métier**

Les **enjeux** de **PROGINOV** en tant qu'hébergeur :

- Se prémunir des accès non maîtrisés, garantir la sécurité et disponibilité de l'infrastructure mise en place pour ses clients avec une forte exigence de qualité de service.
- Faire évoluer, sans cesse, son modèle d'entreprise en restant constamment à la pointe de l'innovation technologique.
- Respecter les contraintes métiers avec notamment, la double certification ISO 27001 et HDS pour ses clients dans la santé, obligatoire pour la collecte, traitement et conservation des données de santé.

Le **besoin**

Chez Proginov nous hébergeons le système d'information de nos clients. Chaque client a son environnement isolé. Nous avons **besoin de tracer les accès** qui sont réalisés par leurs prestataires pour la maintenance de leurs logiciels.

Depuis que nous sommes agréés hébergeur de données de santé, nous avons besoin de traçabilité. Nous avions réussi à répondre à ce besoin à l'aide d'une **solution maison** qui avait des **limites** et qui devenait **compliquée à maintenir** avec le temps.

Au moment du passage de la norme ISO 27001, nous avons choisi de nous orienter vers un **produit plus robuste et qui nous simplifiait la maintenance**.

> *La transition entre l'ancienne solution et la nouvelle a été **rapide à réaliser** pour nous.*
>
> *Aujourd'hui **on ne reviendrait pas en arrière.***

Solution mise en œuvre

PROVEIT by rubycat

Le bastion d'administration **PROVE IT** de **Rubycat** se positionne directement sur le SI. Il vient fédérer l'ensemble des connexions internes et externes au SI que ce soit sur les réseaux bureautiques, d'administrations ou industriels.

Son approche non invasive permet de le déployer rapidement et simplement dans des environnements hétérogènes.

Nous avons trouvé dans **PROVE IT** une solution qui répond très bien à nos besoins :

- **Attentes techniques :** les fonctionnalités de PROVE IT permettent de tracer l'ensemble des accès des prestataires externes de nos clients, de sécuriser leur connexion, mais également leur permettre d'auditer facilement une intervention en revisionnant l'enregistrement de celle-ci.
- **Simplicité de mise en place, d'utilisation et d'administration :** nous avons testé d'autres solutions souvent trop complexes à mettre en œuvre en termes d'administration, ou qui avaient besoin d'un gros effort de déploiement d'agents. Nous avons trouvé en PROVE IT une solution simple à gérer au quotidien.
- **Relation fournisseur :** ce qui a été déterminant, c'est la facilité de contact avec Rubycat et la simplicité dans les échanges. Ils ont bien compris notre besoin et ont su s'adapter pour nous offrir la meilleure solution.

Émilien RICHARD
Administrateur système/réseau/sécurité chez PROGINOV

Une approche innovante de la sécurité des identités et des accès dans les entreprises

Société : SAILPOINT TECHNOLOGIES
Adresse : Tour Cœur Défense A
110, esplanade du Général de Gaulle
92931 Paris la Défense

Mail : **france_sales@sailpoint.com**
Site Web : **www.sailpoint.com/fr**

La capacité de gérer et de sécuriser les identités aujourd'hui a largement dépassé les capacités humaines. SailPoint, le leader de la gouvernance des identités fournit une approche innovante de la sécurité des identités et des accès dans les entreprises. Grâce à l'intelligence artificielle et au Machine Learning, la plateforme de sécurité des identités de SailPoint fournit toujours le niveau d'accès approprié. Les entreprises actuelles, même orientées cloud, peuvent s'assurer que chacun dispose de l'accès approprié dont il a besoin, au bon moment. Les solutions intelligentes SailPoint, autonomes et intégrées placent la sécurité des identités au cœur des opérations commerciales en ligne. SailPoint permet ainsi aux organisations les plus complexes d'établir des règles de sécurité permettant de se défendre contre les menaces les plus élevées, partout dans le monde.

Chiffres clés :

CA 2020 : 365,3 M$

CA 2021 : 439 M$

16/08/2022 : Acquisition par Thoma Bravo

Effectifs : 1700 employés

Dirigeants



Mark McClain
Chief Executive Officer & Fondateur



Hervé Liotaud
AVP Europe du Sud

Historique

En 2005, Mark McClain et Kevin Cunningham ont entrepris de créer un nouveau type de société, qui promettait de fournir des solutions innovantes aux problématiques de transformation digitale des entreprises et ce, dans un environnement de travail collaboratif passionnant pour des spécialistes de la gestion des identités. SailPoint redéfinit la place de l'identité dans l'écosystème de la sécurité.

Solutions

Les suites SailPoint Identity Security Cloud sont constituées d'un ensemble de composants de sécurité SaaS intégrés aux identités. Elles s'adressent à toutes les entreprises afin d'assurer la sécurité des activités de leurs employés et prestataires. Suivant la maturité des entreprises en terme de gestion des identités, les deux suites proposées comprennent :

- **SailPoint Identity Security Cloud Business :** un ensemble de solutions de sécurité essentielles permettant aux entreprises de structurer leur première démarche de gestion des identités, grâce à l'Intelligence Artificielle et au Machine Learning.
- **SailPoint Identity Security Cloud Business Plus :** une suite complète de sécurité des identités s'appuyant sur l'Intelligence Artificielle et le Machine Learning afin de découvrir, sécuriser et gérer les identités sur l'intégralité d'une infrastructure hybride.

Ces deux suites permettent d'accéder plus facilement et à des prix fortement concurrentiels aux offres de sécurité des identités de SailPoint. Grâce à une implémentation techniquement plus fluide, elles peuvent se prévaloir d'un ROI plus rapide.



Références

Les témoignages publics complets peuvent être consultés sur le site : **https://www.sailpoint.com/customers/**

Parmi eux : Allianz, AXA, ING Direct, Société Générale…

SailPoint

Au coeur de la Sécurité des Identités

Intelligence
inégalée

Automatisation
sans faille

Intégration
complète



LES ASSISES

Venez rencontrer les équipes SailPoint aux Assises et écouter le retour d'expérience d'Hermès le jeudi **13 octobre à 15h.**

SANS | GIAC CERTIFICATIONS

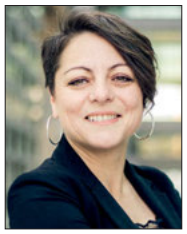
Société : SANS INSTITUTE
Adresse : 11200 Rockville Pike, Suite 200
North Bethesda, MD 20852, USA
Tel : +44 203 384 3470
Mail : **emea@sans.org**
Site Web : **www.sans.org**

Spécialisations : formations dans le domaine de la cybersécurité

Cyberdéfense, Inforensique, réponses aux incidents, management, tests d'intrusion, systèmes de contrôle industriel (SCI), fondamentaux de la sécurité, sécurité du Cloud et audit.

Chiffre clé :

Effectifs : 500



Contact
Axelle SAIM
Business Development Director France & Luxembourg
asaim@sans.org
+ 33 (0)7 67 82 75 52

SANS Institute est la référence mondiale en matière de formation depuis plus de 30 ans dans le domaine de la cybersécurité.

Notre mission fondamentale consiste à partager les connaissances et compétences de pointe en matière de cybersécurité des entreprises, institutions militaires et gouvernementales pour une protection optimale des personnes et des biens.

Une formation de pointe
Les formations SANS préparent les stagiaires à faire face aux menaces d'aujourd'hui et à relever les défis de demain. Pour ce faire, nos cours et nos supports pédagogiques sont constamment mis à jour afin d'enseigner les dernières techniques et outils qui assurent la sécurité des réseaux et des données. Conçues pour être pratiques, nos formations immergent les stagiaires en laboratoire, pour qu'ils appliquent leurs nouvelles connaissances et affinent leurs compétences. Les stagiaires seront en mesure de mettre en œuvre leurs nouvelles compétences dès leur retour au bureau. C'est la promesse SANS.

Une force humaine
Enseignants hors normes de par leur compétences, les formateurs SANS sont actifs auprès de nombreuses organisations influentes; passionnés, ils animent nos formations avec dynamisme et efficacité.

La communauté mondiale
SANS Institute est un membre éminent de la communauté mondiale de la cybersécurité. Nous exploitons l'Internet Storm Centre – un système d'alerte précoce pour Internet. SANS développe, met à jour et publie gratuitement une vaste collection de documents de recherche sur de nombreux aspects de la sécurité de l'information.

Services

Formation ciblée
Nous proposons plus de 70 cours SANS spécifiques, qui s'alignent sur les rôles, responsabilités et disciplines majeurs des équipes de sécurité. Cyberdéfense, inforensique, réponses aux incidents, management, tests d'intrusion, développeur, systèmes de contrôle industriel (SCI) et audit. Chaque programme offre une progression de cours qui conduit les professionnels des bases fondamentales du sujet jusqu'aux spécialisations de haut niveau.

SANS propose ses formations en présentiel, OnDemand (en ligne à votre rythme), Live Online (live streaming) ou en intra-entreprise.

Security Awareness Training
Formations de sensibilisation à la sécurité, qui se présentent sous forme de vidéos interactives, préparant vos salariés à reconnaître et à réagir correctement aux cybermenaces prédominantes d'aujourd'hui.

Cyber Academy
SANS Cyber Academy identifie des candidats à fort potentiel pour les former de façon intensive à la certification GIAC, avant de les affecter à des postes clés.

Cyber Start
Une suite de défis, d'outils et de jeux conçus pour initier les enfants et les jeunes adultes au domaine de la cybersécurité.

NetWars
Une série de défis pratiques conçus pour tester les compétences et l'expérience des participants : Core NetWars (fondamentaux de la sécurité) et DFIR Netwars (l'inforensique et la gestion d'incidents).

Novice en Cyber
Divers et variés, les rôles en cybersécurité correspondent à de nombreux profils selon le degré d'intérêt de chacun. Le programme New to Cyber de SANS propose des ressources gratuites, des formations et des certifications à qui veut se lancer dans la cybersécurité.

Certifications

De nombreux cours SANS s'alignent sur les examens GIAC (Global Information Assurance Certification). GIAC valide les compétences des professionnels de la sécurité des informations, attestant que les personnes certifiées possèdent les compétences et connaissances techniques nécessaires. Plusieurs certifications GIAC sont accréditées ANSI / ISO / IEC 17024.

- Un ciblage spécialisé, adapté à un poste particulier
- Des connaissances approfondies du monde réel
- La certification dont le concept est réputé être le plus fiable

GIAC CERTIFICATIONS

SANS The most trusted source for cybersecurity training, certifications, degrees, and research

GIAC CERTIFICATIONS



SE588 at SANS Paris November 2022

28 Nov - 3 Dec 2022 | CET | Cybersecurity Training

Protect Your Organisation and Advance Your Career

SEC588: **Cloud Penetration Testing**

GCPN
Cloud Penetration Tester
giac.org/gcpn

SEC588 will equip you with the latest in cloud-focused penetration testing techniques and teach you how to assess cloud environments. The course dives into topics like cloud-based microservices, in-memory data stores, serverless functions, Kubernetes meshes, and containers, as well as identifying and testing in cloud-first and cloud-native applications. You will also learn specific tactics for penetration testing in Azure and Amazon Web Services, particularly important given that AWS and Microsoft account for more than half the market. It's one thing to assess and secure a data center, but it takes a specialized skillset to truly assess and report on the risk that an organization faces if its cloud services are left insecure.

"The SANS course SEC588 taught me more than I expected. With the rapid development of new technologies offered by cloud providers, SEC588 has given me an important framework for cloud pen testing."

— Jonus Gerrits, **Phillips66**

Enhance your training experience. Add a GIAC Certification attempt and OnDemand Bundle to your course.

Distinguish yourself as an information security leader and get certified with **GIAC Certifications**. **giac.org**

Extend your training experience with an **OnDemand Bundle**. Receive four months of supplemental online review and 24/7 online access to your course lectures, materials, quizzes, and labs. **sans.org/ondemand/bundles**

Follow **@SANSEMEA** on Twitter!
Join the conversation at **#SANSParis**

Course offerings are subject to change. For up-to-date agenda see **https://www.sans.org/cyber-security-training-events/paris-november-2022/**

emea@sans.org +44 203 384 3470 www.sans.org @SANSEMEA

SCASSI cybersecurity GROUP

Toulouse
Paris
Madrid
Valencia

Sécuriser les systèmes critiques et embarqués

Qualifié PASSI LPM SCASSI est spécialisé sur les systèmes critiques et embarqués

Nos centres d'expertises :

- **AÉRONAUTIQUE & CONTRÔLE AÉRIEN**
- **DÉFENSE & SPATIAL**
- **AUTOMOTIVE**
- **BANQUE & MONÉTIQUE**

Nos offres techniques :

GOUVERNANCE & CONFORMITÉ

- Audits PASSI LPM organisationnels & physiques
- Analyse de risques ISO 27005 et ISO 21434 de systèmes critiques (calculateur embarqué, système opérationnel)
- Mise en conformité LPM, ISO 27001/HDS, NIST, CMMC,
- Accompagnement RSSI
- Gestion de crise (PCA/PRA)

VISA DE SÉCURITÉ – ANSSI

ARCHITECTURE ET INFRASTRUCTURE SI

- SIEM managé
- Audit d'architecture et de configuration
- Etudes techniques
- AMOA/AMOE Cyber de systèmes critiques
- Maintien en Condition de Sécurité (MCS)

EVALUATION TECHNIQUE

- Sécurité offensive
- Test d'intrusion externes et internes
- Audits de codes et techniques, mobiles, IOT
- COTS assessment sur composants avioniques, spatiaux et défense
- Forensic & gestion des incidents

june cybersec factory

LOGICIEL AUDITOOL

LOGICIEL D'AUDIT POUR PILOTER SIMPLEMENT LA CONFORMITÉ D'UNE ORGANISATION et de son réseau de fournisseurs/partenaires

Garantissez que vos partenaires et fournisseurs respectent les engagements de cybersécurité, de procédures internes, de qualité, de conformité opérationnelle...

phosforea

SENSIBILISATION

Plus d'1 million de collaborateurs formés !

E-LEARNING - CYBERSÉCURITÉ

Facilitez l'apprentissage grâce à une approche pédagogique complète :

CUSTOM LEARNING

- Un parcours de sensibilisation personnalisé pour chaque collaborateur
- Un radar de maturité des compétences SSI de votre entreprise
- +60 contenus en 8 langues
- Contenus à façon avec accompagnement chefferie de projet

SIMULATION DE PHISHING

- Segmentation avancée des utilisateurs
- Librairie de modèles
- Statistiques de clics et d'envoi de formulaires

Qualiopi processus certifié
RÉPUBLIQUE FRANÇAISE

FORMATION

ISO 27001 /ISO 27005 / EBIOS / CEH / CRITÈRES COMMUNS DEVELOPPEURS, EQUIPES IT et CHEFS DE PROJETS



Références Clients :

Airbus Defence & Space, ESSP, CNES, Thales Alenia Space, Airbus, Rockwell Collins, DGAC DSNA, GCB, MAAF, Banque de France, Ministère de la Défense, Groupama, Continental, Renault, Actia, Saint Gobain, Naval Group, Michelin, Hôpitaux de Toulouse, IAD, Ministère de la Culture



Laurent PELUD
Fondateur Groupe



Pierre NICOLAS
DG SCASSI FR



Jesus FRIGINAL
DG SCASSI ES



Laetitia MAYNARD
DG PHOSFOREA



Auditool.

Standardiser la production d'audit SSI est un levier de croissance.

Organisez, réalisez et restituez tous vos audits sans perdre de temps :

- Génération automatisée de rapport d'audit
- Référentiels intégrés de normes techniques et organisationnelles
- Mode pentest
- Mode collaboratif / déconnecté
- Statistiques avancées de mission
- Gestion du plan d'action



Mode saaS ou on premise.

Données hébergées sur cloud français.

Logiciel cybersécurisé.

June factory est une filiale du groupe SCASSI
En savoir plus : **www.june-factory.com**
contact@june-factory.com
05 61 17 08 54

june cybersec factory

SECKIOT

Sonde de détection OT & IOT

Société : SECKIOT
Adresse : 10 rue de Penthièvre, 75008 PARIS
Tél : 01 84 60 78 20
Mail : **contact@seckiot.fr**
Site Web : **www.seckiot.fr**

Née en 2020, la société SECKIOT est une start-up française innovante qui a vocation à devenir le leader européen sur le marché de la cybersécurité dédiée aux systèmes cyber-physiques (systèmes industriels & IoT). Notre solution vous fournit un inventaire précis de vos équipements industriels, analyse vos vulnérabilités afin de réduire votre surface d'attaque et détecte les tentatives d'intrusion sur votre réseau. SECKIOT est soutenu et financé par Bouygues. Nous sommes membre du Pôle d'Excellence Cyber.

Notre mission :

Contribuer à la sûreté et à la disponibilité des systèmes OT et IoT avec une solution souveraine

Spécialisations :

Renforcer la cybersécurité des systèmes industriels & IoT par le biais d'une sonde :

- **Cartographie les équipements et flux réseaux**
- **Surveiller les vulnérabilités**
- **Détecter les intrusions**

Chiffres clés :

Effectifs : 35



Dirigeant
Nicolas GASCHY
Fondateur et CEO

« Il est primordial que les industriels français et européens puissent disposer d'outils souverains efficaces aussi essentiels au moment où les attaques visent de plus en plus de systèmes critiques »

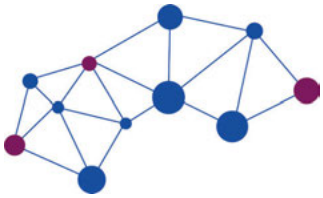
Nicolas Gaschy - *PDG*

Offres

Procéder à une analyse de risque pour vos réseaux OT & IoT, c'est dans un premier temps la réalisation d'une cartographie des équipements et la construction d'une matrice des flux via la captation passive sur les réseaux industriels. Cet inventaire permet de mettre en évidence des comportements anormaux sur le réseau.

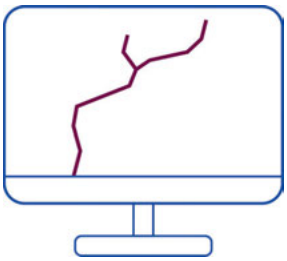
L'objectif est de fournir une visibilité à 100% pour éliminer les zones d'ombres qui sont propices aux cyberattaques.

Afin de réduire la surface d'exposition et colmater les brèches, le module de gestion des vulnérabilités permet de découvrir et de suivre les vulnérabilités critiques des assets sur le réseau et d'y apporter une remédiation. Le module de détection permet de réagir face à une cyberattaque en détectant les tentatives d'intrusions via l'analyse temporelle des communications et la détection des anomalies comportementales entre les différentes entités du réseau.



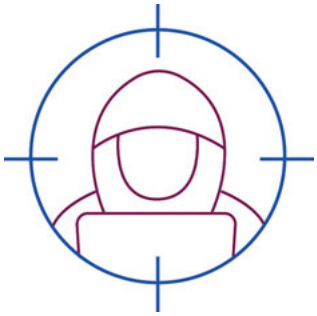
Cartographie

- Inventaires des équipements
- Matrice des flux
- Analytics avancées
- Enrichissement avec intégration des données clients



Surveillance des vulnérabilités

- Priorisation en fonction du niveau de risque et du contexte
- Des rapports configurables pour les opérateurs et les manageurs



Détection des menaces

- via iOC & signatures pour les menaces connues
- Via machine learning temporel et analyse de graphe pour les menaces inconnues

SECKIOT

Renforcer la sécurité de vos réseaux industriels & IoT



Cartographie des réseaux

Surveillance des vulnérabilités

Détection des menaces

Demandez une démo à contact@seckiot.fr

www.seckiot.fr

secuserve
email & security as a service

Société : SECUSERVE
Marques : e-securemail

e-securemail

Adresse : 68 rue de Rivoli 75004 Paris
Tél : 01 41 27 17 17

Labo R&D : 74 bvd du 11 Nov 1918 69100 Villeurbanne

Mail : **contact@secuserve.com**
Site Web : **www.secuserve.fr / www.e-securemail.com**

Spécialisations :

Services SaaS de sécurité de la messagerie, plan de continuité de messagerie, délivrabilité messagerie, messagerie collaborative sécurisée

Chiffres clés :

CA : entre 1 et 5 M€
Effectifs : 15 – 20 personnes

Historique :

Date de création : juin 2003, 100% français (capitaux, R&D, hébergement et support)



Dirigeants
Stéphane BOUCHÉ
Président fondateur
sbouche@secuserve.com



Jean-Michel POMME
Directeur général
jmpomme@secuserve.com

Fondée en 2003, SECUSERVE est la première société française à éditer des services de sécurité de la messagerie en mode SaaS. Les équipes Secuserve sont appréciées par leurs clients pour leur excellence dans l'accompagnement des projets de cybersécurité et de messagerie, et pour leur innovation et R&D continuelle autour de ces produits phares : e-securemail, optimails et sharecan.

Les solutions de SECUSERVE et particulièrement les solutions de sécurité de la messagerie e-securemail, e-securemail for M365 et e-securemail Continuity sont essentiellement développées, hébergées et supportées en France par des équipes françaises, avec des SLA inégalés et une disponibilité constatée de 100% depuis plus de 19 ans.
e-securemail permet de sécuriser vos emails simplement et efficacement. A la fois sur les flux entrants (protection et classification) et sortants (communication et délivrabilité).

Bien plus qu'un antispam, e-securemail est la solution de sécurisation de la messagerie **la plus complète du marché :**

- Filtrage SMTP Entrant & Sortant
- Antivirus X4
- Technologie Anti-spam X16
- Technologie Humail : test Robot / Humain et lever de doute
- Analyse taille et contenu
- Gestion des listes et zones géographiques
- MAX : extraction des pièces jointes
- Quarantaines individuelles
- Catégorisation par I.A : VIP, NEWS, SOCIAL, PUB…
- Unisign : Signature unifiée & centralisée
- Mentions légales & bandeaux de rétro-action
- DAD : Droit à la déconnexion
- Politique de sécurité granulaire
- Double console
- Suivi et reporting

« Spécialisées en développement et livraison de services de sécurité de la messagerie en mode SaaS depuis 2003, nos équipes ont à cœur d'innover et de défendre des SLAs inégalés. Dans les prochains mois, nous serons mobilisés sur la certification ANSSI de nos solutions et la certification qualité de nos process de développement et d'exploitation. »

Stéphane Bouché,
Président-fondateur



- RGPD, contrôle de conformité SPF, DKIM, DMARC, etc.
- Plan de continuité de la messagerie

Solutions

e-securemail : service de sécurisation pour toutes les messageries
e-securemail for M365 : Service spécifique pour Microsoft365
e-securemail continuity : Service de sécurisation ET PLAN DE CONTINUITE de messagerie

Certification

Labels, certifications et référencements : labellisés France Cyber Security, FFCYBER, NUMEUM, UGAP, SOLAINN.

Points Forts

- 100% français
- Pure player 100% sécurité et messagerie depuis 2003
- Niveaux de service inégalés
- Support de proximité et réactivité
- R&D et innovation permanente

Références Clients

+ 12 000 sociétés clientes protégées dont Château de Versailles, région Grand Est, département de la Vienne, Orléans Métropole, AEFE (réseau mondial « Alliance française »), OFII, groupe SNCF, réseau Intersport, réseau ERA immobilier, réseau Bureau Vallée, CH Aulnay, CH Montreuil…

Le cocktail survitaminé pour sécuriser votre messagerie depuis 2003

#CYBERSECURITE #EMAIL #ANTISPAM

e-securemail

pour toutes les messageries // version spéciale Microsoft 365

#100% FRANCAIS

#100% SAAS

antivirus x 4

technologies antispam x 16

Humail



communications avancées

délivrabilité

extraction pièces jointes

#granularité

.....conformité règlementaire/RGPD/SMTP/DKIM/SPF/DMARC.....

UGAP

SOLAINN ACHATS INNOVANTS

FRANCE CYBER SECURITY

numeum Engager le numérique

FF CYBER FÉDÉRATION FRANÇAISE DE LA CYBERSÉCURITÉ

secuserve

email & security as a service

www.secuserve.fr

www.e-securemail.com

LANCEMENT D'UN NOUVEAU SERVICE :

LES TABLES RONDES DE LA RÉDACTION

SOLUTIONS numériques



WEBCAST AUTOUR D'UNE THÉMATIQUE

En live ou en replay

CYBERSÉCURITÉ

Découvrez nos évènements en ligne

SE PRÉMUNIR DES RANSOMWARES : BONNES PRATIQUES, OUTILS, ORGANISATION ?

REPLAY du 29 septembre 2022
Avec Tehtris et Ignition Technology

GRC – SURVEILLANCE, VISIBILITÉ, AUTOMATISATION : MAÎTRISER LA GESTION DES RISQUES

REPLAY du 6 octobre 2022
Avec OneTrust

CYBERATTAQUES, RANSOMWARE, DDOS : COMMENT SE PROTÉGER ET ÊTRE ÉLIGIBLE À UNE CYBER-ASSURANCE ?

REPLAY du 2 juin 2022

LES CYBERMENACES EN 2022 & BILAN 2021

LIVE du 24 mars 2022 - **REPLAY**
Avec ANSSI, Cybermalveillance.gouv, Stormshield, Palo Alto, Cisco

CONNAITRE & CORRIGER SES VULNERABILITES LOG4SHELL : RETOUR D'EXPERIENCE D'UN HACKER ETHIQUE

REPLAY du 17 Mars 2022
Avec TENABLE , YES WE HACK

Replay : solutions-numeriques.com/webinar

SERMA
SAFETY & SECURITY

Société : SERMA Safety and Security
Adresse : 14, rue Galilée
CS10071 33608 PESSAC
Tel : 05 57 26 08 88
Mail : contact-s3@serma.com
Site Web : www.serma-safety-security.com

Spécialisations :

- **Evaluations de sécurité (multi-schémas)**
- **Audits techniques (Tests d'intrusion, RedTeam, PASSI RGS*, Sécurité du code…)**
- **SOC On-Premise & Cloud et services managés (EDR, Sécugérance, Support)**
- **Intégration de solutions On-Premise & Cloud (EDR, SASE, Microseg, MFA, IAM, WAF, NG-FW, DevSecOps ...)**
- **Conseil (Safety, Security by design, PSSI, PCA …)**
- **Conformité (CC, ISO 26262 / 21434 / 2700X / EN50128 / CEI 61508…)**
- **Analyses de risques et maturité SI, AMDEC SdF, MTBF SdF …**

Chiffres clés :

CA : +31M€
Effectifs : +220 ingénieurs
Historique : +25 ans d'expérience
150 clients actifs
7 sites en France



Contacts
Xavier MORIN
Directeur général
x.morin@serma.com



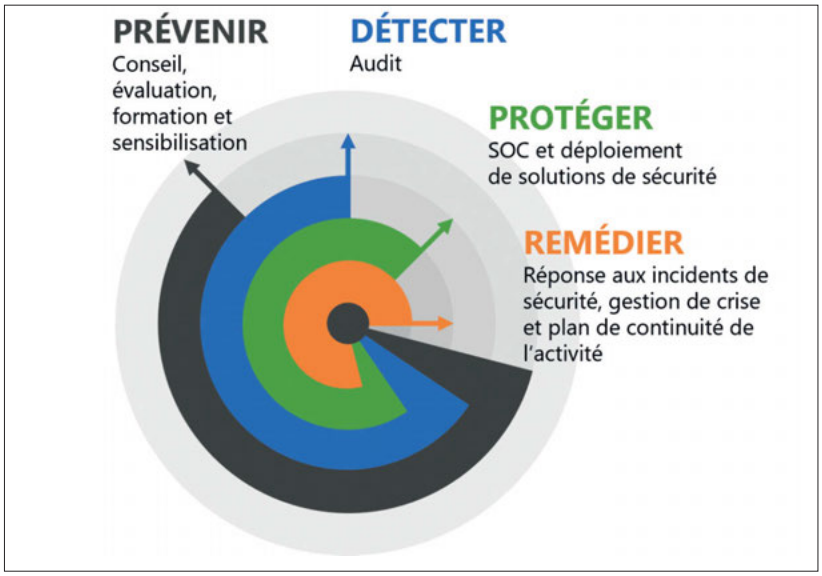
Pascal RASSENEUR
Directeur commercial
p.rasseneur@serma.com

« Avec près de 220 experts des métiers de la sécurité, SERMA Safety and Security est l'un des rares acteurs capables d'adresser les problématiques sécuritaires sur les systèmes d'information, industriels, embarqués et IoT.»

Xavier MORIN, *Directeur général*

En tant qu'entreprise française et indépendante, SERMA Safety and Security propose une offre complète permettant d'accompagner ses clients pour la sécurité et la sûreté de fonctionnement (SdF) des produits et des systèmes IoT, embarqués, industriels et d'information.

UNE OFFRE COMPLÈTE



COMPÉTENCES

CONSEIL, RISQUES ET CONFORMITÉ

Support à haut niveau dans de nombreux secteurs d'activités en termes de :

- Gouvernance (état des lieux, plan de continuité d'activité, politique de sécurité, plan d'assurance sécurité, rédaction du socle documentaire, …).
- Risques (analyse de risques, ISO 2700X, EBIOS RM, tests d'intrusion, AMDEC, fiabilité …).
- Conformité (ISO 27001, ISO 21434, ISO 26262, IEC 61508, EN 62304, ARP 4761, …).

LABORATOIRE DE SECURITÉ ET SÉCURITÉ OFFENSIVE

- Evaluation du niveau de sécurité et de la robustesse des produits et logiciels face à une attaque.
- Audits PASSI RGS*

Le laboratoire dispose de nombreuses accréditations sur des schémas publics ou privés (Critères Communs, EMVCo, GlobalPlatform, PCI PTS, FIPS140-3, SESIP, SBMP, tests d'intrusion…).

PROTECTION DES ACTIFS ET SERVICES MANAGÉS

- Étude, audit, conseil, déploiement, migration, évolution, support et maintenance de solutions de cybersécurité
- SOC (dédié ou mutualisé) et services managés (EDR, sécugérance et support)

Nous intervenons sur tout type d'équipements qu'ils soient On-Premise ou Cloud et sur tout type de solutions IT/OT.

SERVICES DE SECURITÉ

Nous mettons à disposition de nos clients des experts en sécurité et sûreté de fonctionnement pour les assister à temps plein en fonction de leurs besoins.

Certifications

- Accrédité CESTI, Critères Communs et CSPN depuis 1998
- *Qualifié PASSI RGS (Audit de configuration – Audit d'architecture – Audit de code source – Audit d'intrusion) depuis 2017
- ISO 9001
- Reconnaissance CERTIFER
- NIST, MIFARE, EMVCO, PCI, FIPS, SESIP, ARM PSA,...

SIEMENS

Ingenuity for life*

Société : SIEMENS SAS
Adresse : 40, avenue des Fruitiers
93210 Saint-Denis (France)
Tel : +33 1 85 57 00 00
Site Web :
https://new.siemens.com/fr/fr/entreprise/thematiques/la-cybersecurite-chez-siemens.html

Spécialisations :

Grâce à son approche holistique, Siemens est le partenaire de référence et de confiance pour répondre aux enjeux de la digitalisation et de la cybersécurité des systèmes industriels. En effet, Siemens est le premier équipementier – le seul à ce jour – à avoir obtenu en France la qualification de l'Anssi pour une gamme complète d'automates programmables (Simatic S7-1500).
Par ailleurs, Siemens accompagne la sécurisation des installations au travers d'un large portfolio de services : cartographie, conseil (IEC 62443, analyse de risques, référentiels Anssi…), durcissement des configurations, cloisonnement des réseaux, automates industriels sécurisés, switch industriels sécurisés, accompagnement à l'homologation et maintien en condition de sécurité.

Contact :
Fabien MIQUET
PSSO Siemens Digital Industries France
fabien.miquet@siemens.com

Depuis plus de 170 ans en France, le nom de Siemens est synonyme de performance technique, d'innovation, de qualité et de fiabilité. Siemens opère dans les domaines de l'électrification, de l'automatisation et de la digitalisation et compte parmi les principaux fournisseurs de technologies à haute efficacité énergétique, qui contribuent à préserver les ressources naturelles. L'entreprise est pionnière en matière d'équipements d'automatisme, de systèmes d'entraînement et de solutions logicielles destinées à l'industrie. Avec plus de 7000 collaborateurs, 8 sites industriels et 11 centres de R&D, dont huit à responsabilité mondiale, Siemens France s'engage activement dans les filières stratégiques pour l'industrie française. Depuis 2017, Siemens est le seul équipementier dont les process de développement sont certifiés sur la base de la norme internationale IEC 62443-4-1 par le TÜV Sud, et également le seul à offrir des automates programmables industriels qualifiés par l'Anssi.
Excellence par ailleurs renouvelée :

- *avec le maintien en qualification obtenue en 2019 pour la gamme des automates S7-1500 ;*
- *avec la qualification Anssi de trois nouvelles références (CPU 1500 redondantes) décrochées en octobre 2020 ;*
- *avec la labellisation SecNumEdu de sa formation Cybersécurité des systèmes industriels (SITRAIN DI-CYBER) ;*
- *avec notre SCADA WinCC Open Architecture (WinCC OA) doublement certifié, autant côté process de développement que côté produit.*

L'ensemble de ces distinctions montre combien le sujet cybersécurité est un enjeu stratégique pour le groupe. Associant la parole aux actes, Siemens est l'initiateur de la Charter of Trust pour promouvoir le sujet cybersécurité au plus haut niveau au sein des entreprises.

Suivez-nous sur Twitter
@Siemens_France

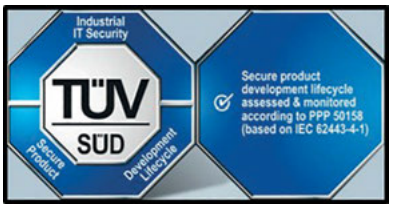


Gamme complète d'automates industriels S7 1500 qualifiée

Offre

Gamme complète d'automates industriels sécurisés, switch industriels sécurisés, surveillance de la sécurité des systèmes industriels.

Certifications





Switch industriel SCALANCE XM400, certifié



Services

Un ensemble de services pour un accompagnement personnalisé :

- Diagnostic (cartographie, analyse de risques, évaluation de la maturité…)
- Conseil (gouvernance, formation…)
- Déploiement (cloisonnement réseau, durcissement des configurations…)
- Contrôle, validation, conformité (préparation à l'homologation, audit de conformité…)
- Maintien en condition de sécurité (mise à jour, gestion des vulnérabilités…)



« La certification TÜV SÜD IEC62443-4-1 de nos sites de développement, associée à la certification Anssi, permet à Siemens d'atteindre le niveau le plus exigeant préconisé par l'ICCF Framework issu du groupe de travail de la Commission Européenne JRC dans le cadre de ses propositions pour une certification européenne des produits pour les systèmes industriels. Nous nous félicitons de cette nouvelle avancée. ».

Vincent Jauneau, directeur Digital Industries chez Siemens France. Ⓟ photo Vincent Jauneau

* L'ingéniosité au service de la vie

STORMSHIELD

La cybersécurité européenne de confiance

Stormshield Network Security
Stormshield Endpoint Security
Stormshield Data Security

Société : STORMSHIELD
Adresse : 22, rue du Gouverneur Général Éboué
92130 Issy-les-Moulineaux
Tél : + 33 (0)9 69 32 96 29

Site Web : **www.stormshield.com**
Mail contact : **commercial@stormshield.eu**

Spécialisations :

Firewall, UTM, IPS, VPN
Device control, APT Detection
Protection Réseau, Cloud, Endpoint, Infrastructures virtualisées, Chiffrement de données (Microsoft et Google Workspace)
Accès distant sécurisé,
Sécurité OT

Chiffres clés :

CA : non communiqué
Effectifs : 400 collaborateurs



Dirigeant
Pierre-Yves Hentzen
Président



Contacts
Eric HOHBAUER
Directeur des Ventes - Directeur Général Délégué
eric.hohbauer@stormshield.eu



Alain DUPONT
Directeur des Services Clients
Directeur général délégué
Alain.dupont@stormshield.eu

Partout dans le monde, les entreprises, les institutions gouvernementales et les organismes de défense ont besoin d'assurer la cybersécurité de leurs infrastructures critiques, de leurs données sensibles et de leurs environnements opérationnels. Nos technologies répondent aux enjeux de l'IT et de l'OT afin de protéger leurs activités.

Notre mission : cyber-séréniser nos clients pour qu'ils puissent se concentrer sur leur cœur de métier, si cruciale pour la bonne marche de nos institutions, de notre économie et des services rendus aux populations.

Une protection innovante de bout en bout

Stormshield, premier éditeur français pure-player en cybersécurité, associe trois grandes expertises pour protéger durablement les entreprises et les organisations contre les menaces les plus avancées :

- Protection des infrastructures informatiques et industrielles ;
- Protection des postes de travail, des serveurs et des terminaux ;
- Protection des données (on-premise, cloud et mobilité).

Certifications

Les technologies Stormshield sont certifiées au plus haut niveau européen pour garantir une protection optimale (UE - OTAN Restreint - Visas de sécurité ANSSI - Producto CCN Aprobado – Producto CCN Cualificado).

Stormshield s'est engagé dans un process de qualification continue de ses produits Stormshield Network Security, au niveau Standard de l'ANSSI, et est le seul éditeur de pare-feux à obtenir à la fois les qualifications espagnoles « Producto CCN Aprobado » et « Producto CCN Cualificado ».

« La notion de confiance n'est pas un vain mot en cybersécurité. C'est même un critère de choix essentiel pour éviter tout risque d'exploitation des données à des fins malveillantes. C'est pourquoi, s'appuyer sur des technologies européennes de confiance permet aux entreprises et organisations de l'UE de garder la maîtrise de leur protection.

Les qualifications délivrées par l'ANSSI vont dans ce sens puisqu'elles attestent de la robustesse des produits face aux attaques mais aussi de la confiance qu'à l'Etat envers l'éditeur, par une analyse de code source et un audit de l'environnement de développement.

Il est donc primordial aujourd'hui de continuer à renforcer la souveraineté dans le domaine de la cybersécurité, via une mobilisation forte de tout l'écosystème et une coopération étroite de l'ensemble des acteurs européens. Mais aussi, de conserver et développer encore plus notre expertise européenne, en soutenant nos startups et l'ensemble de la filière cyber via des organisations nationales, l'investissement dans l'économie cyber locale via des fonds dédiés, mais aussi l'enseignement. Ceci aussi, afin d'éviter que notre savoir-faire ne parte à l'étranger.

Eric HOHBAUER - *Directeur Général Délégué*

SysDream
Cybersécurité Hub One



Grégory Mauguin
Directeur général SysDream

SysDream sera présent aux **ASSISES DE LA CYBERSÉCURITÉ**

À Monaco
du 12 au 15 octobre 2022

STAND 194

SysDream au travers de sa maison mère Hub One est membre associé du Campus Cyber

CAMPUS CYBER
ASSOCIÉ

Société : SysDream
Adresse : 14 pl Marie-Jeanne Bassot
92300 Levallois Perret
Tel : 01 78 76 58 00
Siteweb : SysDream.com
Mail : Lead@SysDream.com

Accompagner les entreprises dans leurs défis en Cybersécurité

SysDream, filiale Cybersécurité de Hub One, est présente tout au long du cycle de vie de la sécurisation de votre système d'information. Pure player français de la sécurité informatique, SysDream propose une offre globale et des solutions sur mesure alignées sur vos enjeux.

3 offres pour votre CYBERSÉCURITÉ

1/ ÉVALUATION ET CONCEPTION DE LA SÉCURITÉ DU SI , AUDIT ET CONSEIL EN GRC (Gouvernance, Risques et Conformité)

Les Audits techniques (PASSI) et organisationnels vous permettent d'évaluer la conformité et d'identifier le niveau de robustesse de votre SI.

Nos formations et cyber-entrainements sont réalisée par nos experts pour sensibiliser vos collaborateurs et développer leurs compétences face aux risques cyber.

2/ SÉCURISATION DU SYSTÈME D'INFORMATION

Notre solution OVELIANE offre une vision complète de l'état de conformité et d'intégrité de vos serveurs.

Intégrateur de solutions en cybersécurité, nos 80 experts vous conseillent dans le choix des solutions les plus adaptées à vos risques, à votre environnement et à votre budget.
Nous déployons et maintenons en conditions opérationnelles de sécurité les outils adaptés à vos usages.

3/ SURVEILLANCE DU SI ET REMÉDIATION

Notre **Security Operation Center** (plateforme centralisée), situé en France opère la surveillance de votre système d'informations. Ainsi vous anticipez les menaces et détectez les incidents de sécurité pour assurer la continuité de votre activité.

Le **CERT (Computer Emergency Response Team)** de SysDream est mis à votre disposition en cas d'incidents de sécurité.

SysDream

Cybersécurité Hub One



RELEVEZ LE DÉFI **DE LA CYBERSÉCURITÉ** POUR VOTRE ENTREPRISE

- **Évaluation, conception de la sécurité du SI, Audit et Conseil en GRC (Gouvernance, Risques et Conformité)**
- **Sécurisation de vos Systèmes d'information**
- **Surveillance et remédiation SOC / CERT**

Nous soutenons Manon Brunet, double médaillée au Sabre aux Jeux Olympiques de Tokyo 2020 et l'accompagnons pour relever ses défis jusqu'en 2024.

La cybersécurité est un enjeu majeur pour votre entreprise. C'est pour cela que SysDream filiale à 100% de Hub One, vous propose une offre globale en cybersécurité pour lutter contre les cyberattaques : sensibilisation et formation de vos équipes, audit de vos systèmes d'information, GRC, intégration de solutions de cybersécurité, supervision continue de votre système d'information via notre SOC (Security Operation Center) et la gestion des incidents de sécurité par notre CERT (Computer Emergency Response Team).

SysDream sera présent aux **ASSISES DE LA CYBERSÉCURITÉ**

À Monaco
du 12 au 15 octobre 2022

STAND 194

Qualiopi processus certifié
RÉPUBLIQUE FRANÇAISE

Centre de formation SysDream SAS, filiale cybersécurité de Hub One

VISA DE SÉCURITÉ

PASSI : Prestataire d'Audit de la Sécurité des Systèmes d'Information SysDream SAS

VISA DE SÉCURITÉ

PDIS : Prestataire de Détection des Incidents de Sécurité*

* SOC Hub One en cours de qualification PDIS

SysDream.com | 01.78.76.58.00
lead@SysDream.com
14 place Marie-Jeanne Bassot,
92300 Levallois-Perret - FRANCE

SYSTEMIS intègre la gouvernance du CAMPUS CYBER

Société : SYSTEMIS
Adresse : 108 avenue de Fontainebleau, 94270 Le Kremlin-Bicêtre
Tel : (0) 820 222 302
Mail : **contact@systemis.eu**
Site Web : **https://www.systemis.eu/**

CAMPUS CYBER
ACTEUR ENGAGÉ

1. **Opérations**
2. **Innovation**
3. **Formation**
4. **Mobilisation**

« Nous œuvrons d'ores et déjà sur les 4 piliers essentiels du CAMPUS CYBER. Cet engagement est supporté par l'ensemble de nos collaborateurs qui se traduit aujourd'hui par un véritable sentiment d'accomplissement professionnel », Cyril MAGLIANO, août 2022

Spécialisations :

Pure Player Cybersécurité audit, conseil, expertise, intégration et solutions

Chiffres clés :

CA : 9,5 M€ en 2022

Effectifs : 80 collaborateurs

Historique : fondée en 2009, SYSTEMIS est une société 100 % autonome.

Spécialisée en Cyber-sécurité, elle s'engage dans la durée auprès de ses clients (Grands Comptes, ETI et PME)

Implantation : France

Dirigeants



Cyril MAGLIANO
PDG et fondateur
cmagliano@systemis.eu



Guillaume DEFRAIN
Directeur des opérations
gdefrain@systemis.eu

SYSTEMIS s'engage afin d'accompagner les acteurs du secteur de la santé

SYSTEMIS bénéficie d'un fort retour d'expérience grâce à ses clients grands comptes C'est pourquoi, nous avons décidé d'accompagner les PME et ETI dans la protection de leurs données avec en plus une offre dédiée aux établissements de santé.

SYTEMIS propose une offre clé en main via des solutions « endpoint » possédant une plateforme unique capable d'identifier où se trouvent toutes vos données, de corriger chaque appareil que vous possédez en quelques secondes, de mettre en œuvre des contrôles de sécurité critiques et de faire tout ça au sein d'une seule interface.

Intégrateur des solutions TANIUM spécifiques aux PME et ETI, les experts SYSTEMIS savent vous accompagner.

Notre expertise

Gouvernance – Risque – Conformité : évaluation des risques et mise en œuvre opérationnelle nécessaire à leur gestion rigoureuse et pérenne.

- Analyse de risques
- Schémas directeurs SSI
- Assistance RSSI

Confiance numérique : gestion des habilitations, des flux et des accès.

- Gouvernance des identités et des accès
- Contrôle des accès (SSO, authentification forte…)
- Accès à privilège

Sécurité opérationnelle : mise en œuvre de la sécurité dans les systèmes, les réseaux et les applications.

- Solutions de sécurité (SIEM, SOC, antivirus)
- Fuites de données
- Audit et tests d'intrusions

Nos modes d'intervention

Assistance technique : mise à disposition d'un ou de plusieurs consultants expérimentés.

Prestations forfaitaires : mise en place d'une équipe de professionnels de la sécurité pour la réalisation intégrale d'un projet.

SYSTEMIS
Cybersecurity Services



LUI, C'EST PIERRE.

VOTRE CYBERSÉCURITÉ EN TOUTE SÉRÉNITÉ !

LA CYBERSÉCURITÉ DE QUALITÉ
ACCESSIBLE À TOUS

synetis

Anticiper les menaces et renforcer sa cyber résilience

Société : SYNETIS
Adresse : 19 Rue du Général FOY
75008 PARIS
Tel : +33 01 47 64 48 66
Mail : contact@synetis.com
Site Web : www.synetis.com

Spécialisations :

Créé en 2010, Synetis est le leader français des cabinets de conseil spécialisés en Sécurité des Systèmes d'Information (SSI). Synetis se positionne comme pure-player français de la cybersécurité et propose une démarche complète à ses clients - PME et grandes entreprises de tout secteur d'activité, de l'accompagnement à la mise en œuvre et l'opération de nouvelles solutions au sein de leur SI.

Chiffres clés 2021 :

CA : 28.8M€
Effectifs : 210
Clients accompagnés : 426
Projets maîtrisés – toutes practices confondues : 742
Jours de formations dispensés : 780

Multiplication et sophistication des attaques, professionnalisation des groupes cybercriminels, généralisation du télétravail, course à la conformité et cyberguerre dans un monde ultra-connecté… Le cyberespace a évolué plus intensément que jamais, les métiers de la cybersécurité font face à de nombreux défis et à une pression accrue. Pour répondre à ces nouveaux enjeux, Synetis vous accompagne dans tous vos projets de sécurisation.

Nos offres et périmètres d'expertise :

Depuis sa création, Synetis s'engage auprès de ses clients et partenaires dans l'évolution et l'innovation permanentes. Synetis a développé une approche globale répondant aux nouvelles problématiques, proposant donc une large gamme de services et solutions, compétences organisationnelles et expertises techniques – et intervenant aujourd'hui sur :

- **L'AUDIT DE SÉCURITÉ :** connaître son niveau de risque face aux cybermenaces ;
- **LE CERT – RÉPONSE À INCIDENT :** prévenir, anticiper les menaces et réagir en cas d'incident ;
- **LA GRC (GOUVERNANCE, RISQUES, CONFORMITÉ) :** organiser et piloter sa cybersécurité (définition des exigences, identification des axes d'amélioration, analyse de la valeur des actifs et des données, etc.) ;
- **L'IDENTITÉ NUMÉRIQUE :** maîtriser ses identités et ses accès ;
- **LA SÉCURITÉ OPÉRATIONNELLE :** déployer des solutions technologiques de protection des SI.

Synetis, **organisme de formation agréé - certifié Qualiopi,** propose également une large gamme de formations couvrant les différentes expertises cybersécurité - pour permettre à tous de s'adapter et rester performant face aux nouveaux enjeux cyber.

En 2021, Synetis a - pour finir - reçu le Visa de Sécurité pour la **qualification Prestataire d'Audit de la Sécurité des Systèmes d'Information (PASSI) par l'ANSSI.**

Dirigeants

Éric DEROUET
Cofondateur & Président
eric.derouet@synetis.com

Rémi FOURNIER
Cofondateur & Directeur général
remi.fournier@synetis.com

Contact

Frédéric LE LANDAIS
Directeur des Opérations
frederic.lelandais@synetis.com



Frédéric LE LANDAIS *Directeur des Opérations*

« L'actualité Synetis est, aujourd'hui, tournée vers nos services de sécurité managés (MSSP) et notre SOC. Nous étendons également nos offres de services managés de sécurité à l'ensemble de nos expertises historiques, aussi bien en Access Management et en CIAM qu'en IGA et en PAM - afin d'accompagner nos clients en 24/7/365 sur l'ensemble de leurs solutions de sécurité.

Depuis toujours, notre volonté est d'allier le conseil et l'expertise technologique afin de proposer les solutions les plus adaptées à nos clients. Nous poursuivons dans cette optique avec notre service SOC by Synetis, en étant en mesure de proposer une approche « best-of-breed » et sur mesure. En effet, les attentes et problématiques des entreprises sont diverses et variées, nous souhaitons donc apporter des réponses adaptées à chacun, en tenant compte de leur maturité dans le domaine de la sécurité du Système d'Information.

Les menaces sont en perpétuelle augmentation et industrialisation, tandis que les Systèmes d'Information continuent de s'étendre et de s'interconnecter. Les technologies doivent donc apporter des réponses simples à mettre en œuvre et à opérer au quotidien, adaptées aux usages réels des entreprises ainsi qu'aux usagers, le tout en respectant les différentes réglementations et normes du domaine. Toutefois, les technologies ne sont qu'un outil pour lutter contre les menaces : l'humain, l'organisation et les process de sécurité sont également des points déterminants à penser lors de la sécurisation de son SI. En effet, l'humain doit être au cœur de toute stratégie de défense. »

THALES

Thales est l'un des leaders européens de la cybersécurité et le leader mondial de la protection des données

Société : Thales
Adresse : 4, avenue des Louvresses – 92622 Gennevilliers Cedex – France
Tel : +33 (0) 1 46 13 20 00
Site Web : **www.thalesgroup.com**

Spécialisations :

Leader européen de la cybersécurité et leader mondial de la protection des données, Thales contribue à la transformation digitale sécurisée de ses clients grâce à sa maîtrise des systèmes d'informations critiques.

Ses 4000 spécialistes en cybersécurité répondent aux exigences les plus poussées des clients du Groupe, publics et privés, dont les opérateurs d'importance vitale, en matière de sécurisation des systèmes d'information et de protection des données.

Ils comptent plus que jamais sur Thales dans leurs moments décisifs. Couvrant l'ensemble du référentiel du NIST (National Institut of Standards and Technology), les solutions proposées par Thales protègent l'intégrité des technologies qui font avancer le monde en conservant une avance sur toutes les formes de menace numérique.

Chiffres clés :

CA Groupe : 16,2 milliards d'euros (2021)
Effectifs Groupe : 81 000
Présence mondiale : 68 pays

Dirigeant



Pierre-Yves Jolivet
Directeur général
Thales Cyber Solutions

Fort de 81 000 collaborateurs dans 68 pays, Thales a réalisé en 2021 un chiffre d'affaires de 16,2 milliards d'euros. Thales offre une capacité unique pour créer et déployer des équipements, des systèmes et des services répondant aux besoins de sécurité les plus complexes. Son implantation internationale exceptionnelle lui permet d'agir au plus près de ses clients partout dans le monde. S'appuyant notamment sur ses compétences fortes en cryptographie, Thales est l'un des leaders mondiaux des produits et solutions de cybersécurité pour la défense, les organismes gouvernementaux, les opérateurs d'importance vitale et les opérateurs de services essentiels, l'internet des objets, notamment du monde industriel et plus largement des systèmes critiques de secteurs d'activité clés (bancaire, transport, spatial, industrie, etc).
Présent sur l'ensemble des prestations de cybersécurité, Thales propose une plateforme complète de solutions, de produits et de services, pour des environnements souverains ou critiques, depuis le conseil et les audits de sécurité, la protection des données, l'analyse des menaces, la confiance numérique, la conception, la mise au point, l'intégration, la certification et le maintien en conditions de sécurité (MCS) des systèmes, jusqu'au dépistage des cybermenaces, à la détection d'intrusions et à la supervision de la sécurité (9 centres opérationnels de cybersécurité en France et à l'international).

Offres

PRODUITS et SOLUTIONS :

Cybels Protect :
- Passerelles de sécurité (Cybels elips-SD et Elips Gateway)
- Protection des réseaux (Cybels Mistral)
- Gestion des accès et authentification multi facteurs (SafeNet Trusted Access)
- Protection de données cloud et serveurs, Gestion d'infrastructures PKI, (Cybels Authenticate, hSM Luna, CipherTrust Data Security Platform)
- Sécurisation des communications mobiles (Cryptosmart), du partage et du stockage de données (Cryptobox), des applications collaboratives de messagerie (Citadel)

Cybels Detect & Respond :
- Sonde de détection d'intrusion (Cybels Sensor)

Services

Cybels Risk & Threat Evaluation :
- Conseil et audit cyber (qualification PASSI)
- Evaluation de la Sécurité des Technologies de l'Information (CeSTI),

Cybels Train & Experiment :
- Formation et entraînement contre les attaques cyber et test des infrastructures IS/IT/OT grâce à des scénarios d'attaque virtualisés (Cybels Train & Experiment),

Cybels Detect & Respond :
- Service de renseignements sur les menaces (Cybels Threat Intelligence)
- Plateforme big data pour la recherche d'attaques avancées (Cybels Analytics)
- Détection et réponse aux menaces (Cybels Security Operation Centres, qualification PDIS)
- Service d'alerte et de réaction rapide aux attaques informatiques (CSIRT/CeRT-IST, qualification PRIS).

Qualifications

Visas de sécurité de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) pour les qualifications de :
- Prestataire d'Audit de Sécurité des Systèmes d'Information (PASSI)
- Prestataire de détection d'incident de sécurité (PDIS)
- Prestataire de Réponse aux Incidents de Sécurité (PRIS)
- La sonde de détection Cybels Sensor.
- La protection des réseaux
- CESTI qualifié.
- Critères Communs, CSPN, Bancontact.
- Cryptosmart, agréé Diffusion Restreinte

TIXEO
SECURE VIDEO CONFERENCING

Société : TIXEO
Adresse : 244 Rue Claude François, 34080 Montpellier
Tel : +33(0)4 67 75 04 31
Mail : **contact@tixeo.com**
Site web : **www.tixeo.com**

Spécialisations :

Solutions de visiocollaboration sécurisées

Historique :

- **2003 : création de la société**
- **2017 : certification CSPN et Qualification par l'ANSSI**
- **2022 : ouverture d'une filiale allemande**

Dirigeants :
Renaud GHIA
Président, co-fondateur

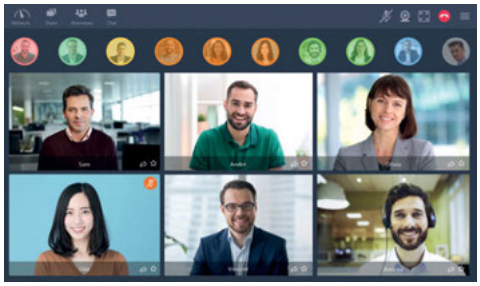
Sébastien JEANJEAN
Directeur Général, co-fondateur



« Depuis bientôt 20 ans, Tixeo développe des solutions innovantes de visiocollaboration, en prenant en compte la sécurité dès leur conception et à tous les niveaux (Secure by design). De plus, nous sommes attachés à la souveraineté européenne en matière de cybersécurité. Contrairement à la plupart des autres éditeurs, Tixeo n'est soumis à aucune législation étrangère imposant des capacités d'écoute susceptibles d'être exploitées. »

Renaud Ghia, *Président Tixeo*

Créée en 2003, Tixeo est leader européen de la visioconférence sécurisée. Entreprise française engagée pour la cybersécurité, Tixeo développe une technologie qui assure un niveau de sécurité jamais atteint pour des réunions en ligne. Ses solutions sont les seules à être certifiées et qualifiées par l'ANSSI. Le siège, la R&D, l'hébergement et le support sont exclusivement localisés en France. Son ambition : garantir la confidentialité absolue des flux de communication de ses clients.



VISA DE SÉCURITÉ — ANSSI

Technologie unique de visiocollaboration

Tixeo propose une approche simple et conviviale de la visioconférence, en offrant de nombreuses fonctionnalités de collaboration depuis n'importe quel équipement. Ses **trois modes de communication** avancée offrent une nouvelle approche de la collaboration et du télétravail en équipe.

La technologie Tixeo, labellisée ANSSI, se base sur des mécanismes innovants qui assurent **un niveau de sécurité encore jamais atteint** dans la visioconférence. Tixeo propose un réel **chiffrement de bout-en-bout** des flux audio, vidéo et data en multipoint, tout en gardant une grande adaptabilité aux variations réseau. Une innovation rendue possible grâce à la technologie unique «SVC on Demand» de Tixeo. Même en cas d'attaque ciblant le serveur Tixeo, la confidentialité des communications est garantie.

À la différence des offres traditionnelles de visioconférence (H.323/SIP), la solution Tixeo ne nécessite l'ouverture que d'un seul port (pas d'impact sur la politique de sécurité du réseau).

À ce jour, contraint par leur architecture technologique, aucun autre acteur de visioconférence ne propose un tel niveau de sécurité.

Offres

Toutes nos offres intègrent la technologie Tixeo, certifiée CSPN et qualifiée par l'ANSSI et sont 100% conformes au RGPD.

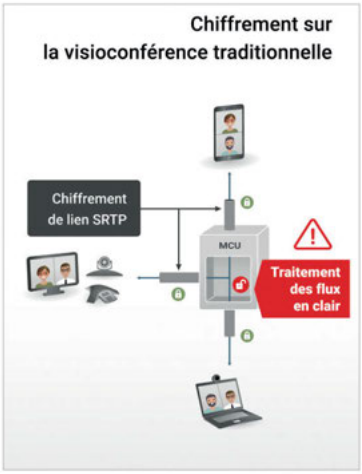
TixeoCloud : la visioconférence sécurisée Tixeo est disponible en mode Cloud pour un déploiement simple, rapide et sécurisé. **L'hébergement des serveurs Tixeo est localisé en France** métropolitaine selon une stratégie multi-cloud, pour garantir une haute disponibilité de service.

TixeoPrivateCloud : le Cloud privé Tixeo vous offre votre propre serveur de visioconférence hébergé dans le Cloud, sans passer par de lourdes étapes de déploiement. Ce Cloud dédié, infogéré par Tixeo, offre une connectivité optimale en supprimant les désagréments de maintenance.

TixeoServer : l'approche on-premise du serveur de visioconférence Tixeo permet de répondre aux exigences les plus strictes en matière d'intégration. En installant TixeoServer au cœur de votre infrastructure, vous gardez une totale maîtrise de votre installation et bénéficiez d'une sécurité optimale pour vos visioconférences.

Certification

- Technologie certifiée (CSPN) et qualifiée par l'ANSSI
- Labellisé FRANCE CYBERSECURITY et CYBERSECURITY MADE IN EUROPE
- **Tixeo est membre de :** HEXATRUST, ALLIANCE POUR LA CONFIANCE NUMERIQUE, CLUSIF
- Tixeo intègre l'offre de visioconférence SFR Business sélectionnée par l'UGAP





Ils nous font confiance

MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES — EDF — nexter — NAVAL GROUP — SEM SAINT-ÉTIENNE la métropole

Protégez vos applications Web et API

Société : UBIKA
Adresse : Parc Tertiaire de Meudon,
9 rue Jeanne-Braconnier,
92366 Meudon
Tél : +33 1 46 20 96 00
Mail : **info@ubikasec.com**
Site Web : **https://www.ubikasec.com/fr/**

UBIKA, acteur souverain de la sécurité est le leader européen de la protection des applications Web et des APIs. Connu précédemment sous les étendards de Bee Ware, DenyAll ou plus récemment Rohde & Schwarz Cybersecurity, la société fournit des solutions innovantes de protection des applications Web & des APIs contre les nouvelles menaces comme le DDOS volumétrique ou applicatif, les injections de code malveillant, les défacements et en général contre le TOP 10 de l'OWASP. Agnostique des fournisseurs de cloud, les solutions peuvent être déployées en mode multi-cloud, On-Premise et même en mode SaaS afin de prévenir les cyberattaques de manière proactive plutôt que réactive. Les solutions proposées permettent de protéger les applications Web, d'authentifier les utilisateurs avec un module SSO et de protéger les APIs avec un module spécifique pour les flux de type Web Services & WebSockets.

Spécialisations :

Pare-feu applicatif (WAF) en mode SaaS et Multi-Cloud, Web SSO (MFA, OpenIdConnect, OAuth, Certificat...)
Pare-Feu API (WebServices OpenAPI3)



OFFRES

UBIKA
WAAP Gateway/Cloud

- Sécurise les applications web, services web et API
- Bloque les attaques sur la couche applicative y compris celles du Top 10 OWASP
- Surveille l'utilisation des applications web pour prévenir toute menace interne ou externe
- Intègre de multiples moteurs de sécurité et un workflow graphique et intuitif
- On-premises et multi-Cloud

UBIKA
Web Access Manager

- Déploie un portail centralisé d'authentification pour un accès instantané à toutes les applications de l'entreprise (Web SSO)
- Renforce l'authentification des utilisateurs grace à l'ajout d'un MFA
- Permet d'ajouter des mécanismes modernes d'authentification SAML, OAuth ou OpenIdConnect

UBIKA
Extended API Security

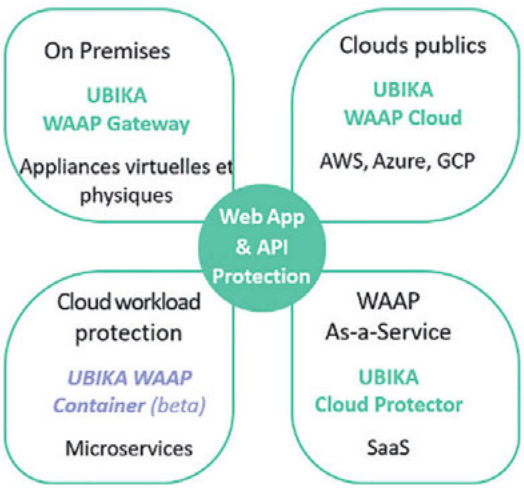
- Sécurise spécifiquement les APIs
- Permet de chiffrer/déchiffrer des messages webservices
- Permet d'offusquer des données dans les flux API
- Permet de sécuriser les websockets, protocole de communication temps réel

UBIKA
Cloud Protector

- Service SaaS souverain hébergé en France garantissant la confidentialité des données, la conformité RGPD
- Société et hébergeur de droit française non soumis au cloud Act
- Anti-DDOS volumétrique et applicative pour des applications toujours disponibles
- Engagement de disponibilité de 99,95% avec pénalités

Avantages de nos solutions

- **Souveraineté & Confiance**
  Faites confiance à un acteur souverain
- **Facilité & Ergonomie**
  Définition des politiques de sécurité grâce à un workflow graphique
- **Haute sécurité**
  Automatisez la sécurité de vos API, services critiques et Web
- **Innovation**
  Pionnier du WAF dans le monde, toujours à la pointe





Dirigeant
Stéphane de SAINT ALBIN
Directeur Général
UBIKA

Contacts
Christine Amory
VP Sales & Marketing
christine.amory@ubikasec.com

Sécurisez votre avenir numérique

WALLIX protège les identités et les accès aux infrastructures informatiques, aux applications et aux données. Spécialisée dans la gestion des accès à privilèges, la solution WALLIX PAM4ALL garantit la conformité aux dernières normes de sécurité informatique et protège contre les cyberattaques, les vols et les fuites de données liés aux identités volées et aux abus de privilèges.

Société : WALLIX
Adresse : 250 bis, rue du Faubourg St Honoré
75008 PARIS
Tel : +33 1 53 42 12 81
Site Web : **www.wallix.com**



Dirigeant
Jean-Noël de GALZAIN
Président,
Directeur général



Contact
Jean-Pierre BARRE
Directeur
Commercial France
jpbarre@wallix.com



Témoignage client

Un responsable technique du secteur des médias et de l'édition - 2021 Gartner Peer Insights :

" La solution est facile à utiliser. Nos prestataires de services peuvent désormais accéder à nos machines Linux en toute sécurité. Le support WALLIX est de grande qualité. "

Twitter : **@wallixcom**
Linkedin : **WALLIX Group**

Essayez gratuitement notre solution pendant 30 jours !

Produits

WALLIX PAM4ALL : Solution de gestion unifiée des privilèges et des accès.

PAM4ALL réduit les risques liés aux accès et aux privilèges associés, permet une gestion granulaire de vos accès distants et offre des accès uniquement pour des usages et des durées spécifiques réduisant ainsi considérablement les surfaces d'attaques, sans affecter la productivité et en respectant les directives réglementaires.

PAM4ALL sécurise, contrôle et administre les accès de tous les utilisateurs, pour toutes les sessions sur tous vos actifs, et pour tous vos terminaux, au bon moment et de n'importe où.

WALLIX PAM4ALL réunit les technologies WALLIX en une solution :

- L'authentification multi-facteurs (MFA)
- La sécurisation des accès à distance
- La traçabilité des sessions
- La gestion du moindre privilège
- La protection des mots de passe

Usages métiers

- **Transformation Digitale :** automatisez la sécurité pour garantir la productivité de vos équipes IT et DevOps et sécurisez votre transformation digitale quelle que soit la localisation de vos ressources IT.
- **Audit & Conformité :** relevez le défi de la conformité en répondant aux exigences des standards et réglementations sectorielles, nationales et européennes (RGPD, PCI DSS, Directive NIS, ISO 27001).
- **Gestion des Risques et Sécurité :** assurez-vous que vos systèmes les plus vulnérables sont protégés des utilisateurs (internes et externes) pour garantir la continuité d'activité et la productivité de votre société.
- **Cybersécurité à la conception :** renforcez la sécurité de vos solutions en intégrant les technologies de gestion des accès et des identités de WALLIX dès leur conception avec **WALLIX Inside.** Concentrez-vous sur votre métier en toute sécurité.

A propos de WALLIX

- Leader Européen du PAM
- Solutions certifiées CSPN par l'Anssi
- Un réseau mondial de partenaires technologiques et commerciaux
- Coté en bourse sur Euronext Growth (ALLIX)

Sécurisez votre avenir numérique

WALLIX PAM4ALL

Gardez la visibilité et le contrôle de vos accès !

Le télétravail, la migration vers le cloud, la multiplication d'équipements et les nouveaux usages numériques... engendrent une explosion du nombre et type d'accès aux actifs stratégiques des entreprises. Faites face à ce défi avec WALLIX PAM4ALL, la plateforme de gestion unifiée des privilèges qui vous permet de sécuriser, contrôler et manager l'ensemble de vos accès. PAM4ALL réduit les risques liés aux accès et aux privilèges associés, permet une gestion granulaire de vos accès distants et offre des accès uniquement pour des usages et durées spécifiques réduisant ainsi considérablement les surfaces d'attaques, sans affecter la productivité et en respectant les directives réglementaires.

WWW.WALLIX.COM



Pour plus d'informations
sur les solutions WALLIX contactez
Jean-Pierre Barré : jpbarre@wallix.com

WALLIX
CYBERSECURITY SIMPLIFIED

W / T H secure | Formerly F-Secure Business

30 ans d'expérience en cybersécurité Avec toujours le même moteur : l'innovation

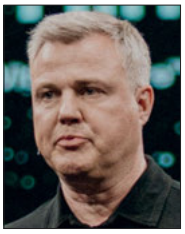
Société : WithSecure™
Adresse : Immeuble Seine Way - Bât G
12-14 rue Louis Blériot
92500 Rueil-Malmaison
Tel : 01 41 29 23 23
Site Web: **www.withsecure.com/fr**
Mail contact: **corporate-france@f-secure.com**

Chiffres clés :

Effectifs : 1700 employés dans le monde.

CA 2022 : NC.
CA 2021 : 120,1 M€

Dirigeants



Juhanni INTIKKA
President and Chief Executive Officer chez WithSecure™. Membre de l'équipe dirigeante depuis 2020.



Guillaume GAMELIN
Vice-President France chez WithSecure™ il possède une expérience de plus de 15 ans sur le marché de la sécurité informatique.

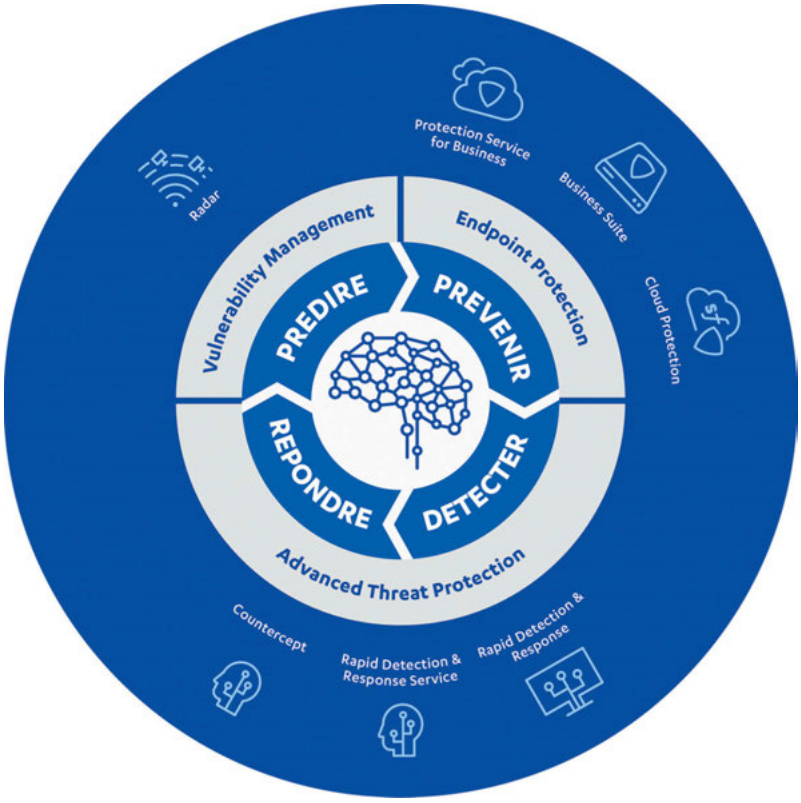
Relations médias WithSecure™
Françoise Amon KOUTOUA
06 43 62 98 12

L'Agence RP
Justine Boiramier
justine@lagencerp.com
06 50 31 86 24

Lucille Lavigne
lucille@lagencerp.com

Mélina Dahmane
melina@lagencerp.com

Les Offres



WithSecure™, anciennement F-Secure Corporation, a été fondée en 1988 et est cotée au NASDAQ OMX Helsinki Ltd.

WithSecure™ inaugure une nouvelle ère pour les services et solutions de sécurité destinés aux entreprises. Ceux destinés au grand public, quant à eux, resteront proposés aux particuliers et partenaires via la marque F-Secure.

WithSecure™ s'appuie sur les décennies d'expertise, de recherche et de technologie de F-Secure pour fournir aux entreprises une sécurité optimale en toute simplicité. Nous accompagnons les fournisseurs de services informatiques, les MSSP et des multinationales, qui nous font confiance, à travers des modèles commerciaux flexibles et adaptés au marché.

Récompenses

En mars 2022, WithSecure a remporté les Silicon Cybersecurity awards dans la catégorie Prix du Public, et a également été nommé « Leader stratégique » pour la protection des endpoints et les capacités de détection et réponse par AV-Comparatives.

Références Clients

GROUPE serap

MAIRIE DE NANTERRE

SALINS

RECTOR® MIEUX CONSTRUIRE ENSEMBLE

MANHATTAN

VOUS PRÉFÉREZ VOTRE INFRASTRUCTURE AVEC...



OU SANS SÉCURITÉ?



WITH™ secure

Co-sécuriser les infrastructures critiques pour une meilleure résilience

Notre marque est notre promesse
withsecure.com

La première plateforme européenne de Bug Bounty et de *Vulnerability Disclosure Policy* (VDP)

Société : YESWEHACK
Adresse : 14 Rue Charles V
75004 PARIS
Mail : **contact@yeswehack.com**
Site Web : **https://www.yeswehack.com**

Fondée en 2015, YesWeHack est la première plateforme européenne de Bug Bounty et de Vulnerability Disclosure Policy (VDP). YesWeHack connecte plus de 40 000 hackers éthiques répartis dans 170 pays avec des organisations de toutes tailles et de tous secteurs pour rechercher les vulnérabilités (bugs) de leurs sites web, applications mobiles, infrastructures et objets connectés, et sécuriser leurs périmètres exposés.

Spécialisations :

Bug Bounty, VDP et Pentest Management

Chiffres clés :

Effectifs : 95 salariés – 40 000+ hackers éthiques

Historique :

Fondée en 2015, YesWeHack est la première plateforme européenne de Bug Bounty et VDP. Avec des bureaux en France, Suisse et à Singapour, YesWeHack sécurise des organisations de toutes tailles et de tous secteurs dans plus de 40 pays.

Dirigeants



Guillaume VASSAULT HOULIÈRE
CEO & co-fondateur, YesWeHack



Romain LECOEUVRE
COO & co-fondateur, YesWeHack

Popularisé dans les années 90 par Netscape, le Bug Bounty devient une pratique courante d'un nombre croissant d'organisations, des start-ups aux administrations, en passant par des entreprises du CAC40.

Le Bug Bounty consiste, pour une organisation, à récompenser – avec des primes, ou Bounties – des chercheurs, ou «hackers éthiques», pour les vulnérabilités – les «bugs» – qu'ils lui rapportent. Le Bug Bounty se déroule dans le cadre d'un programme qui définit les règles à respecter par l'organisation et les chercheurs. Ces règles précisent principalement :

- le(s) périmètre(s) du programme : sur lequel les vulnérabilités peuvent être recherchées. Il s'agit le plus souvent d'applications web ou mobiles, d'API ou d'infrastructures, mais également – de plus en plus fréquemment – d'objets connectés
- les types de vulnérabilités à rechercher ou «vulnérabilités qualifiantes», et qui donnent droit à une prime
- la grille de primes applicable – en fonction de la gravité de la vulnérabilité remontée
- toute autre spécificité du programme, que l'organisation souhaite préciser

Offres

Les services YesWeHack :

- **Programmes de Bug Bounty privés :** sélectionnez, pour chaque programme, des chercheurs selon vos critères d'expertise, de compétence, de nationalité. YesWeHack gère à ce jour plus de 500 programmes privés en Europe et en Asie.
- **Programmes de Bug Bounty publics :** mobilisez l'intégralité de la communauté YesWeHack et communiquez sur votre stratégie de sécurité.
- **Vulnerability Disclosure Policy (VDP) :** offrez aux chercheurs un canal sécurisé et structuré pour remonter les vulnérabilités de vos systèmes d'information, avant qu'elles ne soient découvertes et exploitées par des personnes malveillantes.
- **Pentest Management Solution :** pilotez et orchestrez l'ensemble de vos tests d'intrusion à travers une plateforme unique.

Un accompagnement complet et personnalisé :

En complément d'une communauté de confiance et de qualité, ainsi que d'une interface puissante et conviviale, la plateforme YesWeHack intègre un support client avancé, gérant vos programmes de bout en bout : définition et mise à jour des règles, sélection et rotation des chercheurs, triage des rapports de vulnérabilités, suivi des budgets et indicateurs des programmes en ligne avec les objectifs du client, etc.

Références Clients

- Plus de 500 programmes privés dans plus de 40 pays
- Programmes publics : Blablacar, Doctolib, Swiss Post, Lazada, Deezer, OVHcloud, ZTE, Dailymotion, Ministère de la Cybersécurité et du Numérique du Québec, TousAntiCovid, Prestashop, Cybermalveillance.gouv.fr, Olvid…

Les acteurs du marché

Index des offreurs de solutions et de services de cybersécurité en France



- **Fournisseurs de solutions** fiches alphabétiques p154
- **Prestataires de services** fiches alphabétiques p168

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction.
L'éditeur ne peut pas garantir l'exactitude des informations et décline toute responsabilité.

Consultez le site web, qui peut comporter des mises à jour :
www.solutions-numeriques.com/securite/annuaire-cybersecurite/.

Les éditeurs et sociétés de services peuvent se référencer ou mettre à jour leur fiche existante sur la même page.

EC Label ExpertCyber
CL CLUSIF
CS CESIN
N Adhérents Numeum
H Adhérents Hexatrust

Fournisseurs de solutions

3D-OXIDES

Nous développons un chip sécuritaire couplé à une blockchain user-centric pour faire des identités physiques et digitales pour tous types d'utilisateur incluant aussi les objets.

01630 Saint-Genis Pouilly France

http://www.3d-oxides.com

3M FRANCE

Notre promesse : travaillez sereinement grâce à des appareils protégés du piratage visuel avec les filtres de confidentialité 3M.

95006 Cergy-Pontoise France

42CRUNCH

42Crunch est le spécialiste de la sécurité des APIs, en fournissant une plateforme DevSecOps permettant de fournir de la sécurité positive et permettant d'implémenter du Shift Left et du Shield Right.

34170 Castelnau le Lez France

https://42crunch.com

6CURE H

Appliances physiques et virtuelles: 6cure Threat Protection® : détection et neutralisation des attaques DDoS - 6cure DNS Protection® : mitigation des menaces DNS - DDoS Assessment : Plateforme de Test.

14200 Hérouville-Saint-Clair France

http://www.6cure.com

8MAN

Suite intégrée permettant de visualiser la structure de l'annuaire et des ressources informatiques afin de le modifier dynamiquement pour prévenir en temps réel de toute faille de sécurité.

10555 Berlin Allemagne

A10 NETWORKS

A10 Networks fournit des solutions ADC, FIREWALLS, PROXY, ANTIDDOS, DECHIFFREMENT DE FUX SSL/TLS pour les Data-Centers et Multi-Clouds (privés/publics) aux formats Appliance, VM, BareMetal, Container.

92974 Paris-La Défense France

https://www.a10networks.com

ACG CYBERSECURITY

Conseil en sécurité de l'information, conseil en cybersécurité, gouvernance SSI, diagnostic cybersécurité, analyse de risques, audits de sécurité & tech, mise en conformité.

92800 Paris Île de France France

https://acgcybersecurity.fr

ACRONIS

Acronis édite des solutions de protection des données Cloud hybride : sauvegarde, reprise d'activité après sinistre et synchronisation et partage sécurisés des fichiers.

92300 Levallois-Perret France

http://www.acronis.com

ADVANCED TRACK & TRACE

ATT développe des solutions d'authentification, de traçabilité et de sécurité documentaire. SealCrypt, cachet électronique visible, permet de protéger tout document, à la fois physique et numérique.

92500 Rueil-Malmaison France

AF SOFTWARE

2 modules principaux : - MySUSI : « Sensibilisation des utilisateurs à la sécurité informatique » - GRC : « GDPR Registry Console ». Outil numérique novateur pour la tenue des registres imposée par la GDPR.

13100 Aix-en-Provence France

https://www.afsoftware.fr

AFFINION INTERNATIONAL

Nous proposons une approche 360° de la cyber protection en réponse aux nouveaux risques auxquels s'exposent les consommateurs. Cette offre s'adresse aux banques, assurances et télécoms.

75002 Paris France

https://affinion.fr

AIRBUS CYBERSECURITY

Airbus CyberSecurity fournit des produits et des services de sécurité de confiance sur mesure, permettant d'anticiper, détecter, analyser et répondre aux cyber-attaques les plus sophistiquées.

78990 Élancourt France

https://www.cybersecurity-airbusds.com/fr

ALGOSEC

Aligner la gestion de la politique de sécurité réseau sur vos processus métiers avec AlgoSec Security Management Suite.

EC2R 5 BJ Londres Royaume-Uni

ALHAMBRA SYSTEMS SA

OneseQ (Alhambra, Groupe PROLOGUE) apporte et intègre des solutions blockchain et de cybersécurité, pour proteger les données, la continuité des processus et la sécurité des procédures de décision.

28037 Madrid Espagne

https://oneseq.es

ALINTO

Alinto sécurise et optimise les Emails des organisations. À la fois éditeur et opérateur nous assurons un service premium aux entreprises désireuses de travailler avec des spécialistes.

69002 Lyon France

https://www.alinto.com

ALL4TEC CL

ALL4TEC conçoit et distribue Agile Risk Manager et Agile Risk Board, des outils d'analyse et de pilotage des risques accompagnant la méthode EBIOS Risk Manager promue par l'ANSSI.

Changé 53810 France

https://www.all4tec.com

APICEM SARL N

APICRYPT, messagerie sécurisée en santé, facilite la communication entre les professionnels de santé tout en préservant la confidentialité des informations transmises par un cryptage de haut niveau.

59412 Coudekerque Cedex 2 France

https://www.apicrypt.org

AQUA SECURITY

Aqua propose une solution permetttant de sécuriser tout le cycle de vie des applications Cloud Natives (du pipeline CI/CD au runtime et à la micro segmentation) quel que soit le type d'environnement.

75000 Paris France

https://www.aquasec.com

ARCAD SOFTWARE H

DOT, outils de gestion des données de test. Automatisez votre gestion des données personnelles et identifiantes. Détection, anonymisation et extraction de toutes vos données et bases de données !

74650 CHAVANOD France

https://www.dot-anonymizer.fr

ARCSERVE

Nos solutions de protection des données, PRA/PCA, sur site et dans le Cloud, ainsi que notre stockage immuable offrent une récupération instantanée, fiable et complète.

75001 Paris France

https://www.arcserve.com/fr/

ARMIS CL

Armis réalise sans agent un inventaire des actifs connectés IT, OT, IoT- évalue vulnérabilités, risques et comportement des actifs- pour aider à la décision les outils sécu existants.

75016 PARIS France

https://www.armis.com

ARS NOVA SYSTEMS

TinyMDM : logiciel français de gestion d'appareils mobiles professionnels dédié à Android et partenaire Android EMM. Il possède trois modes de gestion : mode kiosque, 100 % managé et profil de travail.

44300 NANTES France

https://www.tinymdm.fr

ARSEN C L

Arsen permet de tester et améliorer le niveau de réaction des collaborateurs face à des attaques d'ingénierie sociale, à commencer par le phishing.

94160 Saint-Mandé France

https://arsen.co

ARUBA

A Hewlett Packard Enterprise company

Aruba 360 Secure Fabric assure détection et riposte, Aruba IntroSpect (UEBA) pour la détection des comportements et renforce ClearPass, sa gamme de contrôle d'accès.

91947 Les Ulis France

http://www.arubanetworks.com/fr

ARX ONE

Sauvegarde en ligne professionnelle : service de sauvegarde assurant la protection des données et le respect de leur confidentialité. Flexibilité, polyvalence et reprise rapide après sinistre.

44300 Nantes France

www.arxone.com

ATEMPO H

Éditeur de solutions de protection de données, Atempo dispose d'une expertise forte pour sauvegarder, archiver, restaurer et déplacer les gros volumes de données critiques de milliers d'entreprises.

91300 Massy France

http://www.atempo.com

ATOS N

Services et produits : Evidian (gestion identités/accès), Trustway (chiffrement - HSM), IDnomic (sécurité de l'IoT, infrastructures de confiance), SOC, conseil, intégration, MDR, CERT, audit, infogérance.

95870 Bezons France

https://atos.net/en

AVANT DE CLIQUER N

Solution intelligente et automatique de sensibilisation des utilisateurs à la cybersécurité et au phishing. Montée en compétence par le biais d'un programme d'apprentissage par l'action individualisé.

76000 Rouen France

https://www.avantdecliquer.com

AVAST BUSINESS

Avast Business offre des solutions de sécurité intégrées pour les réseaux et les terminaux des PME et prestataires de services informatiques.

140 00 Prague 4 République tchèque

https://www.avast.com/fr-fr/business#pc

AVAST SOFTWARE

Avast fournit des solutions de sécurité digitale pour protéger ordinateurs, terminaux mobiles et IoT, utilisant le machine learning et l'IA pour détecter et contrer les menaces en temps réel.

14000 Prague 4 République tchèque

http://www.avast.com

AVIRA

Avira protège les individus en leur permettant de gérer, de sécuriser et d'améliorer leur vie numérique via toute une gamme d'applications de sécurité et de performance (Windows, Android, Mac, et iOS).

88069 Tettnang Allemagne

https://www.avira.com/fr

AXONIUS

Axonius offre une visibilité totale sur tous les actifs grâce aux intégrations d'API avec les outils existants, d'interroger les données consolidées, et d'identifier l'étendue des vulnérabilités.

RG27 8ZF Hartley Wintney Royaume-Uni

https://axonius.com

AXWAY SOFTWARE N

La gamme comprend deux offres : « API Gateway » pour gérer le cycle de vie des API et protéger l'accès aux services Web, et « Syncplicity » pour la synchronisation et le partage sécurisés des fichiers.

92085 Paris-La Défense France

https://www.axway.com/fr

B<>COM N

b<>com est un centre d'innovation privé conçu pour accélérer l'innovation dans les technologies numériques.

35530 Cesson-Sévigné France

http://www.b-com.com

BALABIT

Éditeur de solutions de gestion des accès privilégiés et de gestion des logs, Balabit permet aux entreprises de réduire les risques de failles de données liées à des comptes privilégiés.

92300 Levallois-Perret France

http://www.balabit.com

BARRACUDA NETWORKS

Sécurité Réseau/Infra avec protection complète du périmètre sur tous les vecteurs d'attaques. Firewall Next Gen - Web Application Firewall - Sécurité Email - VPN - Reverse Proxy - Etc.

92974 Paris-La Défense France

https://barracuda.com

BEEMO TECHNOLOGIE N

Beemo Technologie propose des solutions complètes et fiables pour assurer la sauvegarde des données et la reprise d'activité en cas de sinistre. Solution 100 % française.

34470 Pérols France

http://www.beemotechnologie.com

BERTIN IT

Bertin IT propose des solutions d'anticipation des menaces cyber et de détection de fuites de données (MediaCentric) et une passerelle de sécurisation des interconnexions de réseaux (CrossinG).

78180 Montigny-le-Bretonneux France

http://www.bertin-it.com

BETA SYSTEMS C L

Logiciels de gestion des data-centers et de la sécurité informatique : sécurisation des procédures de traitement des données et de la gouvernance d'entreprise basée sur l'identité & l'accès utilisateur.

94200 Ivry-sur-Seine France

BEWARE CYBERLABS

Solutions de formation et d'entraînement à la cybersécurité, de cyber-déception, de génération de trafic, de scan de vulnérabilités et de pentesting développées en France.

33000 Bordeaux France

https://www.beware-cyberlabs.eu

BEYONDTRUST

BeyondTrust propose une offre PAM intégrée alliant sécurité et productivité : gestion des sessions, des comptes privilégiés et des droits sur endpoints/serveurs, cartographie des comptes & assets etc.

75012 Paris France

https://www.beyondtrust.com/fr

BE-YS SOFTWARE

Nous proposons une gamme outils en SAAS : de Customer Identity Access Management (Be-e IAM) ; d'échanges et traitement de données (Be-e Exchange) ; d'Api Management (GexRT).

63967 Cedex 9 Clermont-Ferrand France

https://www.be-ys-software.com

BITDEFENDER

Bitdefender est un leader mondial de cybersécurité qui fournit des solutions de pointe en matière de prévention, de détection et de réponse aux menaces.

92120 Montrouge France

https://www.bitdefender.fr

BKUBE

Système de box pour PME/TPE de sauvegarde, invisible sur le réseau protégeant vos données contre les ransomwares. Répliqué sur nos serveurs hébergés en France, sécurise contre le vol ou l'incendie.

Nice 06200 France

http://bkube.fr

BLOCKPROOF

Blockproof est un logiciel en ligne pour la mise en conformité RGPD qui convient à différents types de profils.

31400 Toulouse France

https://blockproof.fr

BMC SOFTWARE N

BMC SecOps réunit grâce à un portail intégré et automatisé, la Sécurité et les Opérations IT pour réduire les risques, cerner les priorités et les vulnérabilités et répondre à toutes les violations.

92931 Paris-La Défense Cedex France

http://www.bmc.com/it-solutions/secops-security-operations.html

BOARD OF CYBER

Board of Cyber propose une solution SaaS rapide et non-intrusive, qui permet d'évaluer en continu, et automatiquement, l'exposition des organisations aux risques cyber : le Security Rating®.

92310 SEVRES France

https://www.boardofcyber.io

BOLDON JAMES

Boldon James est un éditeur de logiciels leader dans le domaine de la classification de données et de la sécurisation de messagerie, applicable pour la conformité aux réglementations RGPD, LPM, II 901.

92400 Courbevoie France

http://www.boldonjames.fr

BOX N

Box, l'entreprise de gestion de contenu dans le cloud qui permet de révolutionner la façon de travailler en connectant en toute sécurité les personnes, leurs informations et leurs applications.

75008 Paris France

http://www.box.com

BRAINWAVE GRC H N

Brainwave GRC analyse les droits d'accès aux infrastructures, applications et données. Automatisez vos revues avec l'offre Identity Analytics. Obtenez le meilleur de CyberArk avec PAM Booster.

92600 Asnières-sur-Seine France

CA TECHNOLOGIES

Les solutions de sécurité de CA Technologies permettent d'assurer la sécurité du digital tout en ouvrant les portes à l'expérience utilisateur.

92914 La Défense France

http://www.ca.com

CAILABS

Solution de sécurisation des liaisons en fibre optique très haut débit (10 Gb/s ou plus), par une technique unique d'obfuscation modale des données et détection innovante des tentatives d'intrusion.

35200 Rennes France

http://www.cailabs.com

CECURITY.COM N

Avec ses offres de dématérialisation, d'échanges sécurisés et de conservation, Cecurity.com garantit à ses clients la sécurité, la confidentialité, l'intégrité et la traçabilité de leurs données.

75009 Paris France

https://www.cecurity.com

CERTIGNA

CERTIGNA, prestataire de service de confiance et autorité de certification propose des solutions d'authentification, de chiffrement, de signature et d'horodatage électronique conformes eIDAS et RGS.

59650 Villeneuve d'Ascq France

https://www.certigna.con

CERTINOMIS N

Solution complète pour externaliser votre PKI : à partir de 50 identités, pilotez par une IHM Web et/ou des webs services la gestion de vos certificats, logiciels ou sur carte à puce et clef USB.

94673 Charenton-le-Pont Cedex France

https://www.certinomis.fr

CHAMBERSIGN FRANCE

Autorité de certification, ChamberSign garantit l'identité numérique des personnes physiques et morales. Tiers de confiance, elle délivre des certificats électroniques conforme eIDAS et RGS.

69002 Lyon France

https://www.chambersign.fr

CHECK POINT SOFTWARE TECHNOLOGIES

Check Point Software Technologies fournit exclusivement des solutions de sécurité de pointe qui protègent les entreprises des cyberattaques.

92200 Neuilly-sur-Seine France

http://www.checkpoint.com

CHECKMARX

Éditeur de solutions de sécurité applicative permettant la conception d'applications sécurisées sans retarder le cycle de développement. Reconnu leader par le MQ Gartner 2020 en AST.

92200 Neuilly-sur-Seine France

https://www.checkmarx.com

CISCO SYSTEMS FRANCE CL

Cisco propose une offre réseau et de sécurité à la fois intégrée, automatisée, ouverte et facile d'utilisation.

92130 Issy-les-Moulineaux France

https://www.cisco.com/c/fr_fr/index.html

CITALID CS

Citalid propose un produit permettant aux RSSI et Risk Managers de quantifier leurs risques cyber, puis de construire une politique d'investissements de défense rationalisée, efficace et rentable.

92300 Levallois-Perret France

https://www.citalid.com

CLOUD ECO

Spécialiste des PME, Cloudeco vous conseille dans la sécurisation de vos équipements fixes (PC/serveur) et mobiles (téléphones/tablettes) grâce à ses solutions de sauvegarde, d'antivirus et firewall.

93210 Saint-Denis France

http://cloudeco.fr

COFENSE

Cofense® fournit des solutions de détection et de réponse au phishing. Nous misons sur un réseau de personnes de 25M rapports Phish suspects, et la technologie, aux attaques d'arrêt rapide.

365x24x7 Londres Royaume Uni

https://www.codefense.com

COHESITY

Protégez votre infrastructure, isolez et détectez les données infectées et, restaurez rapidement les données saines afin de réduire les temps d'arrêt et garantir la continuité de l'activité.

D01 H104 Dublin Irlande

https://www.cohesity.com/fr

CONPAL

Conpal GmbH est un fournisseur européen indépendants de solutions de sécurité informatique pour la protection des données confidentielles par le biais du chiffrement et de l'authentification.

63263 Neu-Isenburg Allemagne

https://www.conpal.de

CROWDSEC H

CrowdSec édite un agent open-source de détection et réponse à incident, une console pour visualiser les attaques sur vos serveurs en temps réel et vous donne accès à la plus grande base CTI au monde.

92120 Montrouge France

https://crowdsec.net

CROWDSTRIKE

Protection des postes de travail, serveurs et workloads, identité et données. Détections précises, protection et remédiation automatisées, chasse aux cybermenaces de haut niveau.

75009 Paris - France

https://crowdstrike.com

CRYPTONEXT SECURITY H

CryptoNext offre une suite logicielle de solutions de cryptographie post quantique permettant aux organisations de migrer vers des infrastructures IT/OT résistantes au quantique.

75005 Paris France

https://cryptonext-security.com

CYBELIUS

Première société française dédiée à la cybersecurité des systèmes industriels, nous proposons plusieurs offres de produits et de services et notamment CyPRES solution de détection des cyberattaques.

69002 Lyon France

CYBERARK

Entreprise spécialiste de la sécurité des accès à privilèges, les infrastructures et les outils dans l'entreprise, le cloud et à travers le réseau DevOps.

92400 La Défense France

https://www.cyberark.com

CYBERNETECH SAS

CyberDetection SIEM propose la surveillance de l'activité interne et externe du système d'information de votre entreprise, à travers son logiciel software as a service (SAAS).

06210 Mandelieu France

http://www.cyberdetection.net

CYBEREASON

Cybereason offre une plateforme de protection des endpoints. Elle offre un logiciel antivirus de nouvelle génération, Endpoint Detection and Response, avec un agent et une suite de services managés.

75008 Paris France

www.cybereason.com

CYBERRES MICRO FOCUS

C L

Application Security - DevSecOps : Fortify. Security Operations & Analytics : ArcSight & Interset. Data Governance & Protection: Voltage. Identity and Access Management - Zero Trust : NetIQ.

92098 Paris La Défense Cedex France

http://www.cyberres.com

CYBERVADIS

C L H

Solution de gestion des risques cybersécurité liés aux tiers. CyberVadis engage vos tiers et les évalue sur la base de revues de preuves effectuées par des experts cybersécurité.

75016 Paris France

https://cybervadis.com

CYBERWATCH

C L H

Éditeur français, notre logiciel comporte 2 modules : supervision de vulnérabilités (CVE) ; gestion des conformités (règles de durcissement, PSSI...). On Premise, avec/sans agent ou déconnecté.

75008 Paris France

https://www.cyberwatch.fr

CYBONET

Cybowall, une plate-forme de détection et de réponse aux menaces conçue pour les petites et moyennes entreprises (PME). Combinant à la fois l'accessibilité et la fonctionnalité.

3190501 Haifa Israël

http://www.cybonet.com

CYNET - HOLISTIC SECURITY SIMPLIFIED

Cynet est une plateforme de sécurité qui protège les organisations contre les violations par découverte et atténuation automatiques des menaces,- durant toutes les étapes d'attaque dans tout le SI.

92200 Neuilly-sur-Seine France

https://www.cynet.com

DANTOOIN

Solution d'anticipation, prévision et lutte en Cyber-sécurité/Cyber-défense liant l'IA et les Données.

44000 Nantes France

http://dantoo.in

DARKTRACE

C L

l'Enterprise Immune System utilise des algorithmes d'intelligence artificielle qui imitent le système immunitaire humain et permettent de défendre les réseaux d'entreprise de tout type et toute taille.

75008 Paris France

https://www.darktrace.com

DATALOCKER

DataLocker, leader des solutions de stockage chiffrées, offre une gamme de produits certifiés facilement déployables : disques durs, clés USB , stockage Cloud et la gestion à distance des périphérique.

KS 66210 Overland Park États-Unis

https://datalocker.com

DATAXIUM

C L

DATAXIUM propose un NextGen SOC pour PME/ETI. Un service clef en main (expert cyber, outils SIEM et EDR, règles de détection) pour vous défendre contre les les menaces complexes dont les ransomwares.

92800 Puteaux France

https://www.dataxium.com

DATTO

Datto est le premier fournisseur mondial de solutions logicielles basées sur le cloud offrant des solutions de continuité d'activités, de gestion, d'automatisation et de centralisation.

CT 06851 Norwalk États-Unis

https://www.datto.com

DHIMYOTIS

N

Tiers de Confiance et autorité de certification reconnue au niveau Européen, Dhimyothis sous Certigna sécurise les transactions électroniques, protège et authentifie les identités et informations.

59650 VILLENEUVE D'ASCQ France

http://www.dhimyotis.com

DIGITAL GUARDIAN

Digital Guardian est la seule plateforme de sécurité véritablement axée sur les données conçue pour empêcher le vol de ces dernières.

EC3V 1LP London Royaume-Uni

https://digitalguardian.com/fr

DIGITALBERRY

H

BerryCert est une solution CLM (Certificate Lifecycle Management) qui permet aux entreprises de centraliser et simplifier la gestion des certificats numériques à grande échelle.

13002 Marseille France

https://www.digitalberry.fr

DIGITEMIS SOFTWARE

H N C L

Make IT Safe est une plateforme modulaire (hébergée en France) qui s'adapte à tous vos besoins en cybersécurité et conformité, ainsi qu'à divers référentiels (RGPD, CCPA, Sapin 2, ISO 27001, HDS, LPM).

44400 Nantes France

https://www.digitemis.com

DISKYVER

Diskyver propose des solutions SaaS de machine learning qui vous permettent de faire les bons choix pour vous protéger contre les risques planant sur la voix sur IP.

59800 Lille France

https://www.diskyver.com

DMARC EXPERT

Le protocole DMARC permet de lutter contre la fraude au président et contre l'usurpation de marque ou de l'identité d'un de vos utilisateurs. Nous simplifions sa mise en place qui peut être complexe.

76000 Rouen France

https://www.dmarc.com

DOCAPOSTE ARKHINEO

H N C L

Nous proposons un service d'archivage électronique à valeur probante en mode SaaS. Leader depuis 20 ans, nous garantissons l'intégrité, la pérennité et la conformité des documents électroniques.

75009 Paris France

https://www.arkhineo.com

DOCTOR WEB FRANCE

Éditeur des solutions antivirus Dr.Web, sécurisant postes, serveurs, passerelles Internet, messageries, appareils mobiles. Expertise Linux, Android, Windows. Recherche en déchiffrement. Mode Saas.

67100 Strasbourg France

http://www.drweb.fr

DROPCLOUD

DropCloud propose en mode Saas et Desktop ses solutions de transfert, de partage collaboratif et de sauvegarde des données professionnelles. Solutions certifiées ISO27001 - HDS.

94120 FONTENAY SOUS BOIS France

https://www.dropcloud.fr

EGERIE SOFTWARE

C S H

EGERIE est éditeur de logiciels spécialisés dans la gestion intégrée des cyber-risques et le pilotage de la cybersécurité.

83000 Toulon France

https://www.egerie-software.com

ECHOWORX

La solution de chiffrement de courriel la plus souple et orientée utilisateurs. Elle offre 8 modes de chiffrement, supporte 27 langues, tous vos logos et s'utilise de tous les terminaux.

M2P 1N6 TORONTO Canada
https://www.echoworx.com

EDSI N

EDSI est spécialisée en sécurisation des développements embarqués reposant ou non sur du HW dédié à la sécurité : Cartes à puce, Hardening logiciel, Cryptographie, etc.

35510 Cesson-Sévigné France
http://edsisecurity.com

EFFICIENTIP CL CS

EfficientIP, fournisseur français de solutions DDI (DNS, DHCP, IPAM), aide les organisations à accroitre leur efficacité à travers des réseaux agiles, sécurisée et fiables.

92250 La Garenne-Colombes France
http://www.efficientip.com/fr

EM2B

BotProtector est une solution de détection et de protection contre les attaques des bots malveillants.

44000 Nantes France
https://www.botprotector.io

ENTRUST DATACARD

Solutions on-premise, cloud, as a service pour la PKI, les certificats numériques, la signature électronique, l'IAM, les HSM, l'IoT et l'émission de titres d'identification.

45400 Semoy France
https://www.entrustdatacard.com

EQUISIGN H N

Equisign propose 2 solutions : une offre de transfert sécurisé de fichiers utilisée par plus d'un million d'utilisateurs ; une offre de Lettre recommandée électronique qualifiée par l'Anssi.

92057 Paris La Défense France
http://www.equisign.fr

ERCOM H

Ercom, société française filiale du groupe Thales, développe des solutions simples et certifiées pour sécuriser les terminaux, communications mobiles, messageries instantanées et échanges de données.

78140 Vélizy-Villacoublay France
https://www.ercom.fr

ERCOM (THALES) CL

ERCOM propose 3 solutions de sécurisation des communications et du travail collaboratif : Cryptosmart, Cryptobox et Citadel Team

78140 VELIZY VILLACOUBLAY France
https://www.ercom.fr

ESET FRANCE CL

Au-delà du simple antivirus, ESET propose une gamme complète de solutions pour protéger le patrimoine numérique des entreprises : Machine learning, SandBoxing, EDR et Cyber Threat Intelligence.

93320 Les Pavillons-sous-Bois France
http://www.eset.com/fr

ETAS SAS

Premier fournisseur au monde de solutions de sécurité dans le domaine des systèmes embarqués, des communications M2M, de l'Internet des objets et des véhicules connectés.

93404 Saint-Ouen France
https://www.escrypt.com/en

EVERTRUST H

Evertrust propose une suite logicielle, permettant de reprendre le contrôle des certificats numériques en offrant une gestion à 360° du cycle de vie des certificats (automatisation, gouvernance...).

75003 Paris France
https://evertrust.fr

EVINA

DCB protect est une solution SaaS protégeant les opérateurs télécom & annonceurs de paiements frauduleux sur la facture opérateur. - ProxyPony est un réseau mondial de proxys 4G disponible dans 17 pays.

78000 Versailles France
https://www.evina.fr

F5 NETWORKS

F5 offre des solutions de sécurité et Cloud qui permettent aux entreprises d'adopter l'infrastructure applicative de leur choix sans pour autant sacrifier la vitesse ni le contrôle de leurs opérations.

92150 Suresnes France
https://f5.com/fr

FACTORYTHINGS

VigiCenter est un boitier IP destiné au monitoring et à la sécurisation des datacenters. VigiLock est une solution logicielle permettant de coordonner les règles d'accès et de gestion du datacenter.

45430 Checy France
http://www.vigilock.com

FEEDER

Offre vidéosurveillance, écosystème et les acteurs du marché de la vidéosurveillance.

13127 Vitrolles France
http://www.feeder.fr

FEITIAN TECHNOLOGIES

Sécurité digitale comprenant PKI, Java Cards, Lecteurs de carte à puce, OTP, Fido U2F, Dongles de protection logicielle.

06560 Valbonne France
http://www.ftsafe.com

FLASHPOINT

The Flashpoint Intelligence Platform grants access to our expansive archive of intelligence reports and Deep & Dark Web Forum data in a single, finished intelligence experience.

États-Unis
http://www.flashpoint-intel.com

FLEXERA

Évaluez votre logiciel via une base de données de 23 000+ applications pour identifier vos vulnerabilities et obtenez des correctifs de sécurité personnalisables pour votre logiciel tiers.

92671 Paris France
https://www.flexera.com

FORECOMM

BlueFiles permet de transmettre des documents sensibles en ligne avec simplicité. Transfert sécurisé, envoi chiffré et contrôle distant : une solution zero knowledge pour une confidentialité garantie.

93160 Noisy-le-Grand France
ps://mybluefiles.com

FORGEROCK

ForgeRock, le leader sur le marché de la gestion de l'identité numérique, transforme la manière dont les entreprises établissent des échanges sécurisés entre les personnes, les services et les objets.

75008 Paris France
https://www.forgerock.com

FORTINET CL CS

Fortinet offre à ses clients une sécurité sans compromis pour relever les défis de sécurité les plus critiques au sein des environnements réseaux, applicatifs, cloud ou mobiles.

92911 Paris-La Défense Cedex France
http://www.fortinet.fr

FULL IP SOLUTIONS

Représentant exclusif pour la France & autres pays francophones de éditeurs/constructeurs spécialisés sécurité & cybersécurité : Clavister, MobilityGuard, Cryptshare, Yubico, OnlyOffice, Feitian, etc.

78306 Poissy France
http://www.fullipsolutions.com

G DATA SOFTWARE

La solution multi-couche G DATA intègre tous les éléments nécessaires à la protection des entreprises. Antimalware, gestion des endpoints, filtrage Internet et email sont réunis dans une même console.

92120 MONTROUGE France

GATEWATCHER N H

Leader Européen de la détection d'intrusions et des cybermenaces avancées, Gatewatcher protège depuis 2015 les réseaux critiques des grandes entreprises comme des institutions publiques et des OIV.

92800 Puteaux France
http://www.gatewatcher.com

GEMALTO

La gamme de solutions SafeNet de Protection des Données et des Identités de Gemalto offre des solutions de chiffrement, de gestion de clés et d'authentification forte et gestion des accès.

92190 Meudon France

http://safenet.gemalto.com

GITGUARDIAN C L

GitGuardian est une plateforme de sécurité du code. Grâce à la détection automatique de secrets et autres vulnérabilités et à leur remédiation le cycle de développement logiciel est sécurisé.

75002 Paris France

https://www.gitguardian.com

GLIMPS

Nouvelles solutions de détection, notamment basées sur le DeepLearning, pour contrer les menaces avancées. C'est également une solution opérationnelle pour les SOC et les CERT. Glimps Malware, une plate-forme clé en main. Glimps Audit, pour accélérer l'ensemble des analyses logicielles.

35510-Cesson-Sévigné

https://www.glimps.fr

GLOBALSIGN

Prestataire de services d'identité aux solutions PKI évolutives sur le cloud pour les entreprises devant gérer la sécurité de leurs transactions commerciales, communications et offres de contenu.

75010 Paris

https://www.globalsign.com

GROUPE IMPRIMERIE NATIONALE C L N

Pass'IN est un service clé en main de gestion des identités professionnelles. Pass'IN protège le patrimoine, les systèmes, les applications et les données contre tout accès non autorisé.

75116 Paris France

http://www.imprimerienationale.fr

GS2I

i-Guard est le premier logiciel EDR (Endpoint Detection & Response) Européen et Français. Son intelligence artificielle agit seule et bloque menaces connues et inconnues directement sur les Endpoints

75010 PARIS France

https://www.gs2i.fr

GUARDICORE

Guardicore Centra assure la sécurité des Datacenters et du cloud de votre entreprise en contrôlant par de la micro segmentation et une visibilité en temps réel jusqu'au niveau des process applicatifs

78150 Rocquencourt France

http://www.guardicore.com

GUIDANCE SOFTWARE INC

Editeur d'EnCase, déployé sur 35 millions d'Endpoints à travers le monde, Guidance Software est le leader du marché de l'Endpoint Détection Response (EDR) et l'acteur de référence de l'investigation.

92400 Courbevoie France

HACKNOWLEDGE SA

Hacknowledge est une solution de monitoring sécurité de type MDR (managed detection response). Notre rôle est d'identifier les anomalies/problèmes sécurité et de vous conseiller pour leur résolution.

1028 Préverenges Suisse

http://www.hacknowledge.com

HACKUTY

RISK BASED VULNERABILITY MANAGEMENT COCKPIT

Hackuity's platform aggregates and normalizes all your security assessment practices, whether automated or handmade.

69009 Lyon France

https://www.hackuity.io

HAREL SYSTEMS

Protection des données de gestion commerciale.

75116 Paris France

https://www.helloharel.com

HARFANGLAB C L N

HarfangLab, le seul EDR français Full On Premise ou en Cloud qui préserve la souveraineté numérique de ses clients.

75008 Paris France

https://www.harfanglab.fr

HELPSYSTEMS

Protection des données : Digital Guardian, TITUS, Boldon James, VERA - Protection des email : Agari, Clearswift - Sensibilisation à la Cybersécurité : Terranova - Echanges sécurisés (MFT) : GoAnywhere.

MN 55344 Eden Prairie États-Unis

https://www.helpsystems.com

H-IAPPS

NBH est une solution SaaS de formation en continu sur le comportement des utilisateurs face aux risques informatiques qu'encourent les entreprises. Nous agissons en cybersécurité et RGPD.

80440 Boves France

https://neverbehacked.com

HID GLOBAL

Leader mondial des solutions d'identité sécurisée, HID Global délivre des solutions de contrôle d'accès et des transactions, d'impressions, de suivi (RFID…), d'authentification, de protection, etc.

92150 Suresnes France

https://www.hidglobal.fr

HP INC

HP Wolf Security est une approche disruptive de la sécurisation des postes de travail. Elle renforce votre sécurité tout en s'intégrant dans votre écosystème de sécurité en place.

92190 Meudon France

https://hp.com/fr/wolf

HYPERVISION TECHNOLOGY

Yuno, plate forme d'orchestration de réponse aux menaces ou attaques afin d'accélérer le traitement d'incident et de protéger la continuité d'exploitation. Pas de programmation requise, drag and drop.

75008 Paris France

http://www.hypervision-technology.com

IBM FRANCE C L N

Notre offre est développée autour de 3 axes, contrôler et améliorer la sécurité du SI. Le 1er, l'écosystème mondial d'IBM. Le 2e, les solutions de sécurité. Et, le 3e, notre offre de services.

92275 Bois-Colombes France

https://www-03.ibm.com/security/fr-fr/solutions

IDACTIS

La suite logicielle ID>Security permet de contrôler et sécuriser les accès aux postes de travail et aux applications en sécurisant la gestion des mots des mots de passe des utilisateurs.

14400 Maisons France

http://www.idactis.com

IDECSI C L C S N

IDECSI est une plateforme de détection spécialement conçue pour la sécurité de Microsoft Office 365 et des espaces collaboratifs Teams, OD, SP, Exchange et connectée aux utilisateurs.

75008 Paris France

https://www.idecsi.com

IDNOMIC N

IDnomic est le leader européen de la protection et la gestion des identités numériques. IDnomic fournit des services de PKI pour l'identification des personnes, des terminaux et des objets connectés.

92130 Issy-les-Moulineaux France

http://www.idnomic.com

I-GUARD

Fondée en 2014 à Paris, i-Guard est une société française innovante. Créateur du premier logiciel EDR européen et intelligent, idéal pour les TPE, PME et organismes désirant protection et simplicité.

75010 Paris France

https://www.i-guard.eu

ILEX INTERNATIONAL N C L H

Ilex Access (authentification multi-facteur&adaptative, SSO, fédération d'identité) / Ilex Identity (gestion des identités et des habilitations) / Ilex CIAM (IAM pour utilisateurs grand public).

92600 Asnières-sur-Seine France

https://www.ilex-international.com

ILLUMIO

Ilumio fournit une cartographie des flux réseaux afin de permettre la micro-segmentation Zero Trust de façon progressive, des systemes ou applications, quelle que soit la taille de l'infrastructure.

78000 Versailles France

https://www.illumio.com

IMPERVA

Les solutions d'Imperva permettent de détecter les risques et vulnérabilités, protéger l'information là où elle est utilisée (sur site et Cloud) et d'être en conformité avec les réglementations.

92800 Puteaux-La Défense France

http://www.imperva.com

IN GROUPE C L N

IN Groupe propose des solutions d'identité et des services numériques sécurisés à la pointe de la technologie.

75016 Paris France

https://www.ingroupe.com

INFOBLOX

Leader des services cloud-first de réseau et de sécurité, Infoblox transforme le parcours de vos clients en une expérience réseau cloud-first sécurisée offrant simplicité, évolutivité et fiabilité.

1019 GM Amsterdam Pays Bas

http://www.infoblox.com

INVENIS N

Invenis est un logiciel d'analyse Big Data, permettant l'exploration de données, la détection de signaux faibles et le reporting. Experts en Data Science, nous proposons également un accompagnement.

75011 Paris France

https://invenis.co

INWEBO TECHNOLOGIES N

inWebo propose une offre complète d'IAM incluant une l'authentification forte adaptative MFA & un orchestrateur CIAM qui permet de créer des parcours d'accès sans friction, personnalisés et sécurisés.

75009 Paris France

https://www.inwebo.com

ISIT

ISIT offre une stratégie cybersécurité globale (produits & services) pour les systèmes Temps Réel Critiques, couvrant aussi bien les logiciels développés en interne que les codes Open Source.

31830 Plaisance du Touch France

http://www.isit.fr

ISTORAGE

iStorage propose des solutions de stockage sécurisé avec chiffrement matériel et authentication par code PIN sous forme de clés USB, disques durs et SSD externes de 4Go jusqu'à 20 To.

UB6 8DH Perivale, Middlesex France

https://istorage-uk.com

ITRUST C L

ITrust propose des services et solutions en cybersécurité : IKare (scanner de vulnérabilités) ; Reveelium (SIEM, UEBA) ; ACSIA EDR (surveillance locale des événements) ; SOC souverain a la demande.

31100 Toulouse France

https://www.itrust.fr

IVANTI

Les solutions de sécurité Ivanti offrent une protection multiniveau : gestion des correctifs et vulnérabilités, whitelisting, contrôle des applications, gestion des privilèges, protection des données.

92979 Paris-La Défense France

http://www.ivanti.fr

IXIA

Ixia propose des solutions de test, de visibilité et de sécurité afin de valider, renforcer et optimiser vos produits, applications et réseaux physiques et virtuels.

91300 Massy France

http://www.ixiacom.com

JUNE-FACTORY

AUDITOOL, un logiciel d'audit pour piloter simplement la conformité SSI d'une organisation. MIOT, une solution d'IOT cybesécurisé (device et dashboard) pour gérer un parc d'engins de chantier.

31670 Labège France

http://www.june-factory.com

JUNIPER NETWORKS

SDSN est une plateforme réseau sécurisée, associée à des services cloud à la fois flexibles, évolutifs et sécurisés qui facilite la mise en place de politiques de sécurité axées sur le workflow métier.

92200 Neuilly-sur-Seine France

https://www.juniper.net

KASPERSKY LAB FRANCE

Kaspersky Lab propose des solutions de « Threat Intelligence » et de sécurité informatique pour protéger les entreprises, les infrastructures critiques, les gouvernements et les consommateurs.

92500 Rueil-Malmaison France

https://www.kaspersky.fr

KATANA DIGITAL SA C L

Destruction physique, sur site, sécurisée de supports informatiques (disques durs, tapes, SSD, mobiles) selon la norme ISO21964 et utilisation d'une application sur mobile pour tracer les n° de série.

75001 PARIS France

http://www.katanadigital.com

KAZEKO

Welcomr est la nouvelle solution de gestion des accès pour les smart buildings : accueil holistique des visiteurs, expérience utilisateur sans contrainte, 100 % dématérialisée et de haute sécurité !

37000 Tours France

https://welcomr.fr

KEMP-FLOWMON

Flowmon offre une solution innovante pour la sécurité et visibilité réseau. La solution Flowmon peut être deployée comme matériel, comme appliance virtuelle (VMware, KVM, Hyper-V) ou même en cloud.

61600 Brno République tchèque

http://www.flowmon.com

KEEEX N

KeeeX édite des solutions de confiance et sécurité numérique et ambitionne de devenir le standard du fichier et du processus vérifiable. Procédé sobre, universel, interopérable et multi-secteurs.

13013 Marseille France

https://keeex.me

KEEPER SECURITY

Facile à utiliser et à déployer, le gestionnaire de mots de passe Keeper permet de protéger une entreprise des cybermenaces et violations de données liées aux mots de passe.

IL 60607 Chicago États-Unis

https://www.keepersecurity.com/fr_FR/

KIUWAN

Solution d'analyse statique du code en mode SaaS ou On Premise pour détecter les failles de sécurité, les défauts de qualité et surveiller les composants externes embarqués.

78000 Versailles France

http://www.kiuwan.com

KIWI BACKUP N

Kiwi Backup propose deux solutions de sauvegarde de données externalisée : Kiwi Backup et Kiwi Santé (données de santé avec hébergement HDS). Disponible en marque blanche. Linux, Windows et Mac.

68200 Mulhouse France

http://www.kiwi-backup.com

KOBIL

Fondé en 1986, KOBIL est présent en France. KOBIL sécurise l'identité sur l'ensemble des plateformes, avec mAST, et supporte la directive DSP2. Parmi nos clients : Migros Bank, Société Générale, USB.

67547 Worms Allemagne

http://www.kobil.com

KONTROL SAS

Plateforme d'Encryption As A Service pour éditeurs SaaS qui souhaitent faire certifier Anssi leur service cloud en garantissant sécurité, confidentialité et intégrité des données à leurs utilisateurs.

75017 Paris France

https://www.tanker.io

KUB CLEANER

KUB-CLEANER appartient au Groupe RAS, il est leader sur le marché de la sécurisation des échanges de données entre vos périphériques USB et vos réseaux internes. En cours de qualif ANSSI.

92110 Clichy France

http://kub-cleaner.com

LACEWORK

Lacework est la plateforme d'automatisation de la sécurité du cloud basée sur le Machine Learning et l'analyse des données. La technologie permet de rationaliser le nombre d'alertes pertinentes.

CA 95002 San Jose États-Unis

https://fr.lacework.com

LASTPASS

LastPass fournit des solutions de gestion des identités et des accès qui sont faciles à gérer et sans effort à utiliser. Du gestionnaire de mots de passe, au SSO et MFA.

D02 R573 Dublin Irlande

https://www.lastpass.com/fr/

LINAGORA N

Des solutions clés en main pour : authentifier les personnes et les machines, assurer la confidentialité au sein de votre SI, dématérialiser vos documents grâce à la signature électronique sécurisée.

92800 Puteaux France

https://linagora.com

LMBA / GEDIX N

La solution GEDIX, conçue en France, permet la communication et l'acquisition de données sécurisées avec les moyens industriels dans les réseaux industriels. #DNC #MDC.

69003 Lyon France

https://www.gedix.fr

LOGMEIN

Profitez de la liberté de travailler de partout avec les outils logiciels de connexion à distance fiables de LogMeIn.

MA 02210 Street Boston USA

https://www.logmein.com/fr

LOGPOINT C L

Solution européenne de SIEM et Log Management, LogPoint permet d'assurer la mise en conformité réglementaire, de déployer une défense contre les menaces de sécurité et d'optimiser les opérations IT.

92500 Rueil Malmaison France

https://www.logpoint.com/fr

LOOKOUT

Lookout, alimentée par plus de 160 millions de mobiles, identifie les risques (Phishing, Malware, Sideloading, Conformité applicative...) et s'intègre parfaitement aux standards du marché.

75016 Paris France

https://www.lookout.com/fr

LUXTRUST

LuxTrust est une Autorité de Certification et un tiers de confiance européen qualifié, qui fournit des solutions de signature électronique de tout niveau eIDAS (simple, avancé, qualifié).

75008 Paris France

https://www.luxtrust.com/fr

LYBERO.NET

CryptnDrive, partage web de fichiers intégrant un séquestre numérique. Chiffrement de bout en bout, aucun logiciel client nécessaire; Lybcrypt SDK pour intégrer le chiffrement dans votre appli web.

54603 Villers-lès-Nancy Cedex France

https://lybero.net

MAILINBLACK H

Mailinblack est l'entreprise française qui rend la cybersécurité accessible à toutes les organisations. Ses solutions protègent les boîtes mails des cyberattaques et forment les collaborateurs.

13006 Marseille France

https://www.mailinblack.com

MAKE IT SAFE H

Make IT Safe est un logiciel français de conformité et de cybersécurité. Simple, complet et collaboratif, Make IT Safe est la solution pour réduire vos risques cyber et piloter votre conformité.

Rezé 44400 France

https://www.makeitsafe.fr

MALWAREBYTES

Malwarebytes, ENDPOINT PROTECTION et INCIDENT RESPONSE, technologie multicouche, protège les entreprises contre les attaques et répare les dommages non détectés par les autres solutions de sécurité.

75009 Paris France

https://fr.malwarebytes.com

MAPREUVE N

MaPreuve est le premier site de confiance permettant de protéger et certifier juridiquement et immédiatement un document numérique.

59650 Villeneuve d'Ascq France

https://www.mapreuve.com

MARKET ESPACE

TrackUp est une solution qui permet de surveiller des adresses emails pièges certifiées insérées dans une base de données. Le déclenchement d'alertes automatiques permet de détecter le vol des données.

59700 Marcq en Barœul France

https://www.track-up.com

MCAFEE C L

McAfee Security Connected sécurise les postes de travail (ENS), données (DLP), réseaux (IPS NSP); la gestion du SOC (SIEM ESM); Web filtering (MWG), Sandbox (ATD) interconnectés via OpenDXL.

92800 Puteaux France

https://www.mcafee.com/fr

MENAYA

Notre solution d'audit cybersécurité SaaS et clé en main permet aux chefs d'entreprises et aux DSI de surveiller et de prévenir simplement les risques Cyber avant qu'ils ne surviennent.

75016 Paris France

https://menaya.com

MEROX H

Plateforme SaaS française de cybersécurité. Protection noms de domaines et DNS contre l'usurpation d'identité et le phishing. Reporting et conformité (SPF, DKIM, DMARC, BIMI, DNSSEC, MTA-STS…).

34000 Montpellier France

https://www.merox.io

MICROSOFT C L N

L'offre Microsoft assure la sécurité globale du Système d'information sur les aspects détection, protection et réponse en s'appuyant sur la puissance du Cloud et de l'Intelligence artificielle.

92130 Issy-les-Moulineaux France

https://www.microsoft.com/fr-fr

MOABI SOLUTIONS H

MOABI Solutions , spécialisé en sécurité produit, propose une analyse automatique de la posture sécurité de logiciels basée sur une technologie de reverse engineering sans détenir le code source.

06560 Valbonne France

https://moabi.com

MOBILE PROCESS

Solutions pour l'ensemble des terminaux mobiles de l'entreprise : push mail sécurisé ; Mobile Device Management ; sécurisation des terminaux ; accès sécurisé aux données de l'entreprise.

57070 Metz France

http://www.mobile-process.com

MOSKITOS

Moskitos est l'éditeur de Crosscut®, plateforme d'intégration et d'APIs management pour connecter rapidement et en toute sécurité la data, les API, les applications et accélérer l'innovation numérique

92300 Levallois-Perret France

https://www.moskitos.fr

MYDPO

myDPO participe de manière active à la création du patrimoine informationnel des entreprises, en rendant accessible la gestion des données personnelles pour la mise en conformité RGPD des entreprises.

75009 Paris France

https://mydposolution.com

MYQ FRANCE

7 solutions en 1 : gestion de périphérique, gestion des systèmes, gestion d'impression, impression mobile (BYOD), gestion des scans, panneau de contrôle, et gestion de parcs.

75010 Paris France

https://www.myq-solution.com/fr/home

NAMESHIELD H CL

DNS Premium est une infrastructure robuste et fiable, basée en France, couplée à un réseau anycast, aux diverses fonctionnalités : DNSSEC - filtrage anti-DDoS - Failover - GeoIP - Statistiques fines.

75002 Paris France

https://www.nameshield.com

NANOCODE

Easylience® est une solution numérique dédiée aux métiers de la gestion de crise. Accompagnement sur l'évolution des pratiques opérationnelles (ISO 223xx) et dans la conduite d'exercices de crise.

35510 Cesson Sévigné France

https://www.nanocode-labs.com

NCIPHER SECURITY

Les modules de sécurité matériels (HSM) nShield sécurisent les processus de traitement cryptographique, de génération de clés, de protection, de chiffrement et autres.

CB1 2GA Cambridge Royaume-Uni

https://www.ncipher.fr

NEOWAVE H

NEOWAVE est spécialisée dans l'authentification forte et les transactions sécurisées. Nous proposons 3 gammes de produits : les solutions ID 2.0, la gamme FIDO et les Lecteurs de carte à puce.

13120 Gardanne France

http://www.neowave.fr

NETEXPLORER CL N

NetExplorer est la solution qui sécurise les données numériques de 1500 organisations publiques et privées. Au-delà de leur stockage, la plateforme permet de partager, collaborer et signer en ligne.

Issy-Les-Moulineaux 92130 France

https://www.netexplorer.fr

NETHEOS N

La solution SaaS de Netheos sécurise et automatise les parcours de souscription fortement réglementés des banques et des assurances, en conciliant notamment KYC et expérience utilisateur.

34000 Montpellier France

https://www.netheos.com

NETSCOUT

Défense anti DDoS automatique intelligente pour les réseaux d'opérateurs et d'entreprise, dans le Cloud ou sur site, virtualisée ou boitiers. Defense contre les APT rapide et automatisée. Forensic.

91300 Massy France

http://www.arbornetworks.com

NETSKOPE CL

Netskope Security Cloud: Les services informatiques peuvent localiser, comprendre et sécuriser leurs données sensibles présentes dans leurs environnements SaaS, IaaS et Web (Web Proxy).

EC1V 4JP London Royaume-Uni

https://www.netskope.com

NETWORK USERS INSTITUTE

Notre solution de Cybersécurité met en scène le DNS RPZ comme le premier rempart à la Cybercriminalité, soit 95 % de couvert en quelques minutes.

76100 Rouen France

https://nui.fr

NETWRIX

Une visibilité omniprésente sur le comportement des utilisateurs, les configurations système et la sensibilité des données sur les infrastructures informatiques hybrides afin de protéger les données.

75000 Paris France

https://www.netwrix.fr

NEXTDAY.VISION

Mieux sécuriser sans mot de passe- OtpOne API est la solution clé en main pour remplacer les mots de passe dans les applications d'entreprise par un login simple ou multi-facteur sans mot de passe.

2822 Courroux Suisse

https://www.otpone.com

NEXUS GROUP

Nexus est un groupe suédois, filiale de IN Groupe. Nos solutions Nexus Smart ID couvrent l'ensemble des besoins pour une gestion complète des identités numériques et des accès logiques et physiques.

75016 Paris France

http://www.nexusgroup.com

NIS

NIS offre le portefeuille de Gemalto/SafeNet de protection des identités et des données, permettant aux organisations d'être protégées, conformes et en contrôle, où que leurs activités les mènent.

13420 Gemenos France

http://www.nis-infor.com/fr

NORMASYS

NUMERISQUE est une solution cyber-sécurité hybride IDS/IPS qui applique les technologies de l'Intelligence Artificielle aux processus décisionnels.

75009 PARIS France

https://www.normasys.com

NORMATION

Solution de management des configurations systèmes : configuration automatique du socle système ; audit continu des configurations et des règles de sécurité ; correction automatique des écarts.

75003 Paris France

https://www.rudder.io/fr

NORMYA

Audit et externalisation du DPO.

44000 Nantes France

http://www.bellvision.fr

NOVALYS CL N

Visual Guard est une solution de sécurité applicative globale : gestion des utilisateurs, authentification, permissions fines, surveillance en temps réel, élévation de la sécurité en cas d'attaque.

92100 Boulogne Billancourt France

https://www.visual-guard.com

NOZOMI NETWORKS

Nozomi Networks est un spécialiste des solutions de Visibilité et de Sécurité en environnements Industriels (OT & IoT).

6850 Mendirisio Suisse

https://nozominetworks.com

NTX RESEARCH

Solutions : XCA (authentification forte des personnes et objets par tables de codage), PKI2.0 (certificats clients).
Logiciels : Win RGPD Manager (conformité RGPD), Win Security Manager, Smart City.

75116 Paris France

https://ntx-research.com/fr

NUCLEON SECURITY

Nucleon Security, spécialiste de la cybersécurité qui redéfinit la protection des endpoints et la gestion de vulnérabilité grâce à sa plateforme Nucleon Smart Endpoint.

921706 Vanves France

https://nucleon-security.com

NXO CL

Bénéficiez d'experts pour vous aider à définir une stratégie de sécurité de votre SI et vous accompagner de bout en bout sur les solutions de sécurité les plus pertinentes en phase avec vos objectifs.

92500 Rueil Malmaison France

https://www.nxo.eu

OLFEO

H N

Olfeo est le leader européen de la sécurité web. Ses solutions assurent le plus haut niveau de protection grâce à une technologie exclusive. Elles sont disponibles en modes on-premise et en mode SaaS.

75001 Paris France

https://www.olfeo.com

ONE IDENTITY

Gouvernance des identités et des accès, gestion des données non structurées, gouvernance et gestion des comptes à privilèges, sécurisation et administration de l'Active Directory, Log Management.

92200 Neuilly-sur-Seine France

https://www.oneidentity.com/fr-fr

ONELOGIN

OneLogin, leader de l'Unified Access Management, rend simple et sécurisé l'accès des entreprises à leurs applications et à leurs données, qu'elles soient dans le cloud ou sur site.

W1F 8BH London Royaume-Uni

https://www.onelogin.com

OODRIVE

N C L H

Oodrive est la première suite collaborative européenne de confiance. Oodrive édite et propose des outils pour collaborer, signer électroniquement, communiquer et sécuriser l'activité.

75010 Paris France

https://www.oodrive.com

OPENIP

N

Le SIP Trunk Touch permet aux entreprises de téléphoner sur Internet, en bénéficiant d'une gestion simplifiée, des sécurités anti-piratage dernières générations et de forfaits d'appels illimités.

92110 Clichy France

https://www.openip.fr

OPENTEXT SECURITY SOLUTIONS

L'offre comprend des solutions de sécurité s'appuyant sur sa plateforme d'intelligence contre les menaces BrighCloud, et des solutions de protections des données avec des sauvegardes cloud ou hybrides.

92400 Courbevoie France

https://www.carbonite.fr

OPSWAT

Créée en 2002 OPSWAT propose 2 solutions: MetaDefender pour la prévention des menaces et MetaAccess pour le contrôle d'accès au cloud et la conformité des terminaux.

75019 Paris France

http://www.opswat.com

ORACLE

N

Construire une infrastructure Cloud et une plateforme de services offrant à ses clients une sécurité opérationnelle et efficace pour stocker leurs données et héberger leurs applications critiques.

92715 Colombes Cedex France

https://www.oracle.com/fr/security

ORSEC TECHNOLOGIES SAS

OORIGIN Audit est une sonde passive de monitoring réseaux conçue pour le Cyber Threat Hunt que l'on développe à Bordeaux ; avec intégration de la technologie Deep Packet Inspection de « Rohde & Schwarz ».

33700 Mérignac France

https://www.oorigin.fr

OVELIANE

Solution française de prévention d'attaques par le contrôle en continu de l'hygiène de la sécurité du parc de serveurs (conformité et intégrité).

92300 Levallois-Perret France

http://www.oveliane.com

OXIBOX

C S

Oxibox est la première solution qui garantit la sécurité des sauvegardes. Enclaves sécurisées à immutabilité garantie, résistantes aux ransomwares. Sauvegarde 3-2-1 conforme aux préconisations ANSSI.

78280 Guyancourt France

https://www.oxibox.com/fr

PALO ALTO NETWORKS

C S

Spécialiste de la sécurité réseau de nouvelle génération, Palo Alto Networks joue un rôle moteur dans la sécurisation des applications et la prévention des cyberfailles.

92130 Issy les Moulineaux France

https://www.paloaltonetworks.com

PARSEC

Collaborez en confidentialité et intégrité dans le Cloud grâce à PARSEC, « solution sécurisée anti-ransomware et ergonomique certifiée ANSSI », disponible en Saas et On Premise.

33160 Saint-Médard-en-Jalles France

http://www.parsec.cloud

PATROWL

H

Patrowl is an Offensive Security as a Service solution which allows you to manage your External Security Posture.

92130 Issy les Moulineaux France

https://patrowl.io/patrowl

PHINASOFT

Solutions logicielles sur mesure pour la conduite et la supervision des analyses de risques et conformités aux politiques / normes : multi-méthodologies, workflows, suivi, reportings, historiques...

75013 Paris France

https://phinasoft.com

PHISHME

PhishMe : solution humaine de lutte contre le phishing. Collecter, analyser et intervenir, nos solutions : PhishMe Simulator, PhishMe Reporter, PhishMe Triage, PhishMe Intelligence.

VA 20175 Leesburg États-Unis

https://phishme.com

PHOENIX CONTACT FRANCE

La gamme de pare-feux industriels - mGuard - permet de protéger les machines / le réseau OT des cybermenaces et de faire de la télémaintenance en toute sécurité (via des tunnels VPN).

77436 Marne la Vallée France

https://www.phoenixcontact.com/online/portal/fr

PING IDENTITY CORPORATION

Plateforme Ping Identity : Offre de gestion des Accès (Authentification Forte, SSO, Fédération d'identité, WAM, API Security) et Offre de Gestion des Identités Clients CIAM. Solutions OnPrem et Cloud.

75116 PARIS France

https://www.pingidentity.com/fr.html

PRADEO

H

Leader européen dans le domaine la sécurité mobile, Pradeo propose des services innovants pour protéger les applications et les terminaux mobiles (smartphones, tablettes et objets connectés).

75116 Paris France

https://www.pradeo.com

PRIM'X

N H

Basés sur des technologies puissantes et avancées, les logiciels de chiffrement développés par Prim'X assurent une protection globale des données contre la perte, le vol et l'espionnage économique.

69444 Lyon France

https://www.primx.eu

PROMISEC

Promisec Endpoint Manager est une solution sans agent exclusive qui offre des fonctionnalités de visibilité intégrale, de détection, analyse et correction des anomalies.

75019 Paris France

http://www.promisec.com

PROOFPOINT

C L C S

Proofpoint, spécialisé dans la cybersécurité nouvelle génération, permet aux organisations de protéger leurs données contre les menaces avancées, et de se conformer aux réglementations en vigueur.

75009 Paris France

https://www.proofpoint.com/fr

PROVE & RUN CL

Prove & Run vend des briques logicielles de sécurité formellement prouvées pour protéger les systèmes connectés contre les cyberattaques à distance : ProvenCore, ProvenVisor et ProvenFilter.

75017 Paris France

http://www.provenrun.com

PYDIO N

Pydio est un logiciel de partage de fichiers pour les entreprises qui permet de gérer les accès à la donnée ainsi que ses autorisations d'accès et de partage. Pydio est conforme à la RGDP.

75003 Paris France

https://www.pydio.com

QONTROL H

Qontrol est une plateforme SAAS permettant aux PME et startups de structurer une politique de cybersécurité adaptée à leur environnement business.

75001 Paris France

https://www.qontrol.io

QUALYS

Qualys, Inc. (NASDAQ : QLYS) aide les entreprises à rationaliser et fédérer leurs opérations de sécurité et de conformité au sein d'une seule et même plateforme.

92400 Courbevoie

https://www.qualys.com

QUERY INFORMATIQUE CL

Nos solutions modulables protègent de façon optimale vos postes de travail, votre parc informatique et vos données numériques.

92700 Colombes France

https://www.query-informatique.com

QUEST SOFTWARE

L'ensemble du portefeuille de solutions logicielles Quest couvre la gestion de l'information, des terminaux, des identités et des accès, de la plateforme Microsoft, et la protection des données.

75116 Paris France

https://www.quest.com/fr-fr

RADWARE

Radware propose des solutions ADC (loadbalancing, reverse proxy, WAF) et des solutions anti-ddos on prem et cloud (detection et mitigation automatique & trafic legit garanti).

92400 Courbevoie France

http://www.radware.com

RAPID7

La plateforme Insight : sécurise les infrastructures Cloud, réduit les vulnérabilités; détection des menaces & réponse aux incidents; orchestration et automatisation des tâches.

75017 Paris France

https://www.rapid7.com

RCDEVS

OpenOTP Security Suite est une solution de sécurité MFA (Authentification Multi-Facteurs) et d'IAM tout-en-un pour les organisations, applicable à tous types d'accès notamment VPN, Wifi, Fédération.

4370 Esch-sur-Alzette Luxembourg

https://www.rcdevs.com

RSA SECURID

Cyber sécurité : détection et réponse aux attaques avancées. Gestion des identités et accès utilisateurs. Réduction des risques en termes de business, fraude et cybercriminalité. GRC.

95876 Bezons France

https://www.rsa.com/en-us

RUBYCAT

PROVE IT solution de contrôle d'accès et d'audit renforcé pour les connexions sensibles au SI (prestataires, utilisateurs à privilèges…) - PAM - avec enregistrement & visualisation des sessions.

35510 Cesson-Sévigné France

https://www.rubycat.eu

SAILPOINT TECHNOLOGIES CS

En tant que pionnier de l'industrie et leader sur le marché de la gouvernance des identités, SailPoint assure la sécurité, l'efficacité opérationnelle et la conformité des entreprises de tout secteur.

92931 Paris-La Défense France

https://www.sailpoint.com/fr

SCALE COMPUTING

Scale Computing propose des solutions de virtualisation clés-en-main pour les PMEs, combinant serveurs, stockage, virtualisation et haute-disponibilité dans un système simple et évolutif.

IN 46225 Indianapolis États-Unis

https://www.scalecomputing.com

SCASSI SOLUTIONS CL N

Scassi Solutions est l'éditeur des solutions HoneyNet, Auditool, Passed et de la plateforme RGPD.

31670 Labège France

http://www.scassi.com

SCHLEUPEN AG

Nos logiciels : R2C_GRC, pour la gestion des risques et GRC ; R2C_Security, pour la sécurité de l'information, aide à la mise en conformité et facilite le pilotage ISO 27001, 27005, GDPR…

76275 Ettlingen Allemagne

https://grc.schleupen.de/fr

SCPTIME N

SCPTime® met en œuvre un service de diffusion de l'heure légale (UTC) sécurisée, certifiée, précise et traçable pour « cybersécuriser » le temps (Adm, Finance, Digital, Transprt, Énergie, Ind4.0…).

38350 La Mure d'Isère France

https://www.scptime.com/fr/

SEALD

Solution de chiffrement d'emails et de documents simple et intégrée aux clients mails, utilisable même si le destinataire n'a pas la solution, et permet un contrôle a posteriori des données envoyées.

75014 Paris France

https://www.seald.io/

SEC'IT N

La solution de cyberdéfense des entreprises autonome et automatisée.

34000 Montpellier France

http://www.secit.fr

SECKIOT CL

Seckiot, éditeur de logiciel français, sécurise les systèmes industriels & IOT grâce à ses 3 modules : cartographie des équipements, scan des vulnérabilités et détection des intrusions.

75008 Paris France

https://www.seckiot.fr

SECLAB H

La gamme Secure Xchange permet de sécuriser les échanges de données sur les infratstructures critiques, via Réseau ou USB, et garantie une protection électronique sur les couches Transport.

34000 Montpellier France

http://www.seclab-security.com

SECLUDIT

Elastic Workload Protector protège vos applications (workloads) et données en continu avec une approche DevOps. Analysez automatiquement toutes vos failles de sécurité.

06560 Sophia Antipolis France

https://secludit.com

SECRET DOUBLE OCTOPUS

Secret Double Octopus est une solution d'authentification primée, qui remplace les Token, OTP et au final le mot de passe lui-même.

75009 Paris France

https://doubleoctopus.com

SECURE2BROWSE

Navigation Internet a distance. Laissez à vos utilisateurs un accès à distance vers un navigateur cloud ou on-premise dont seul le rendu graphique est envoyé. Supporte le filtrage URL et SSO.

CH-6312 Steinhausen Suisse

http://www.secure2browse.com

SECURE-IC

Secure-IC est spécialisée dans le domaine de la sécurité des systèmes embarqués. Notre offre tourne autour de 4 Business Lines : Threat Analysis, Threat Protection, Think Ahead et Content Protection.

35510 Cesson-Sévigné France

http://www.secure-ic.com

SECURITYSCORECARD

C L

Avec plus de 12 millions d'entreprises évaluées et plus de 100 milliards de vulnérabilités trouvées par semaine, SecurityScorecard aide à quantifier et remédier a vos cybermenaces digitales.

NY 10017 New York États-Unis

https://securityscorecard.com

SECUSERVE

N

Solution SaaS développée, hébergée en France depuis 2003, label France CyberSecurity. Bien plus qu'un antispam, e-securemail est une solution complète pour sécuriser votre messagerie et plus encore.

75004 PARIS France

https://www.secuserve.fr

SEKOIA

C L

Produits : SEKOIA.IO, solution XDR s'appuyant sur la Threat Intelligence.

Services : accompagnement et expertise (CERT, audit, Pentest, Threat Intel, Forensic, investigation).

75008 Paris France

https://sekoia.fr

SENTINELONE

C L C S

L'agent unique SentinelOne EPP, EDR, MDR combine prévention, détection et réponse afin d'assurer la protection des postes de travail et serveurs contre tous les vecteurs de menaces.

75008 Paris France

http://sentinelone.com

SENTRYO

C L

La solution Sentryo ICS CyberVision est une plateforme de surveillance réseau qui fournit visibilité, intégrité et sécurité pour les systèmes de contrôle industriel.

69100 Villeurbanne France

https://www.sentryo.net/fr

SERENICITY

Serenicity propose des solutions de sécurité performantes destinées aux petites, moyennes et grandes entreprises ainsi qu'aux collectivités pour lutter contre les cyberattaques et prévenir les risques.

42000 Saint-Étienne France

https://www.serenicity.fr

SESAME IT

Sesame it est un éditeur français de solutions de cybersécurité, leader sur les solutions d'Extended Network Detection & Response (NDR), qui assure une détection ultra-performante des cybermenaces.

75017 Paris France

http://www.sesame-it.com

SHADLINE

C L

Shadline est une plateforme d'échange et de stockage totalement immunisée contre les ransomwares, offrant des communications sécurisées et un accès aux données critiques même en cas de cyberattaque.

75003 Paris France

http://www.shadline.com

SIEMENS

Pionnier en cybersécurité industrielle, Siemens dispose entre autre des automates SIMATICS S7-1500, seule gamme au monde certifiée et qualifiée, dont l'Etat recommande l'achat, notamment pour les OIV.

93527 Saint-Denis France

http://www.siemens.fr/ingenuity-for-life

SILVER PEAK

Silver Peak, le leader mondial des réseaux SD-WAN, se positionne à la pointe de la transformation du cloud avec un modèle de réseau avant-gardiste.

92300 Levallois-Perret France

https://fr.silver-peak.com

SILVERFORT

Silverfort étend le MFA et la sécurisation moderne des identités de l'Active Directory à tous les utilisateurs, systèmes et environnements qui ne pouvaient pas être protégés avant.

93400 Saint Ouen France

https://www.silverfort.com

SITUATION

N

Situation est une infrastructure de collecte des données IT. Les équipes d'ingénieurs utilisent notre API pour requêter facilement les composants du SI, leurs métadonnées et leurs relations.

35510 Cesson-Sévigné France

https://www.situation.sh

SKYBOX SECURITY

Skybox est une suite logicielle dans le domaine de la cyber sécurité traitant à la fois la gestion de la politique de sécurité et de l'analyse les risques de manière innovante.

95110 San Jose États-Unis

http://www.skyboxsecurity.com

SKYHIGH NETWORKS

Cartographie des Services Cloud utilisés, monitoring et sécurisation d'applications Cloud critiques et/ou home made, protection des données et prévention des fuites d'informations vers le Cloud.

http://www.skyhighnetworks.com

SNOWPACK

H

Snowpack développe, opère et déploie son réseau d'invisibilité. Ce réseau permet d'utiliser les réseaux Internet publics pour envoyer des données de manière totalement anonyme et sécurisés.

91400 Orsay France

https://snowpack.eu

SONICWALL

Depuis 30 ans SonicWall propose des solutions de sécurité informatique : firewalls (physiques, virtuels, Cloud Azure/Aws), messagerie, terminaux, accès distants, wifi, protection Cloud O365, switchs.

75008 Paris France

https://www.sonicwall.com

SOPHOS

C L

Premier éditeur européen de solutions de sécurité professionnelles, Sophos propose une gamme complète de protections: NextGen Endpoint, serveurs, mobiles, chiffrement, Firewall, Email, Web et WiFi.

95870 Bezons France

https://www.sophos.com

SPIRENT COMMUNICATIONS

Notre offre de cybersécurité (logiciel, matériel & service) : validation sécurité & performance réseau en prod ; service de sécurité & tests d'intrusion ; test de sécurité & performance en lab.

78280 Guyancourt France

http://www.spirent.com

SPLUNK

N

Splunk permet de mettre en place une sécurité basée sur l'analyse. Notre mission est de rendre les données machine accessibles, exploitables et utiles à tous.

75009 Paris France

http://www.splunk.fr

STIMSHOP

Notre technologie exclusive Wi-Us de communication sans fil par ultrason permet l'échange de données sécurisé entre deux devices, sans onde radio. Pertinent pour une authentification forte en local.

75020 Paris France

http://www.wi-us.eu

STORMAGIC

StorMagic résout les problèmes de données périphériques. Les solutions StorMagic aident les entreprises à stocker, protéger et utiliser les données de et à partir de la périphérie(« edge computing »).

BS32 4AQ Bristol Royaume-Uni

https://stormagic.com

STORMSHIELD

N C L

Stormshield délivre des solutions de protection des réseaux, des postes de travail et des données certifiées au plus haut niveau de confiance européen, pour une sécurité de bout en bout.

59650 Villeneuve d'Ascq France

http://www.stormshield.eu

STRATON IT

Corrium découvre le réseau et ses composants, la cartographie générée est analysée par huits experts automatisés. Le diagnostic est complété par un plan d'action exhaustif, suivi hebdomadairement.

59000 Lille France

http://www.straton-it.fr

SYMANTEC

Symantec Corp., leader mondial de la cyber sécurité, aide les entreprises, les gouvernements et les particuliers à sécuriser leurs données les plus importantes, quelle que soit leur localisation.

92617 Courbevoie Cedex France
https://www.symantec.com/fr/fr

SYNOPSYS NORTHERN EUROPE LTD.

Synopsys propose aux organisations une offre complète de solutions et services permettant de détecter et de remédier à des défaillances, vulnérabilités et problèmes de conformité tout au long du SDLC.

RG7 4SA Reading Royaume-Uni
https://www.synopsys.com/software

SYSPERTEC N

L'offre JVL de SysperTec permet de renforcer la sécurité des systèmes informatiques Legacy (IBM z Systems et IBM i) et distribués depuis plus de 20 ans.

92210 Saint-Cloud France
https://www.jvl.fr

SYSTANCIA CL

Systancia propose des solutions de sécurité des accès externes au SI, de surveillance des utilisateurs à pouvoirs (PAM), d'authentification unifiée (SSO) et de gestion des identités (IAM).

68390 Sausheim France
http://www.systancia.com

TANIUM

Tanium propose une plateforme de visibilité et de contrôle des terminaux qui transforme la façon dont les entreprises gèrent et sécurisent leurs systèmes d'information.

92200 Neuilly sur Seine France
https://www.tanium.com/fr

TEAMVIEWER GMBH

Avec la combinaison de ITbrain Surveillance, Anti-Malware et Backup, vous obtenez une solution complète pour votre infrastructure informatique ! En plus c'est complètement intégré dans TeamViewer.

73037 Goeppingen Allemagne
https://www.itbrain.com

TEHTRIS N CL CS H

TEHTRIS XDR Platform & ses modules EDR, EPP, SIEM, MTD, NTA, ZTR, DNS FW & DR assurent une défense hyper automatisée en temps réel contre le cyber espionnage & le cyber sabotage 24/24 7/7.

75009 Paris France
https://tehtris.com

TENABLE N CL

Tenable est la société de Cyber Exposure. Plus de 30 000 entreprises dans le monde font confiance à Tenable pour comprendre et réduire les cyber-risques.

75008 Paris France
https://www.tenable.com

THALES N CL CS

Thales propose des services et solutions qui couvrent l'ensemble de la chaine de valeur cybersecurité, intègrant dans ses solutions des technologies innovantes comme AI, Analytics, IOT, Automation.

78141 Vélizy Cedex France
https://www.thalesgroup.com/en/activities/security/critical-information-systems-and-cybersecurity

THEGREENBOW N CL H

Le Client VPN TheGreenBow garantit la sécurité des connexions distantes au Système d'Information. C'est le seul logiciel VPN fiable, ergonomique et certifié pour postes fixes et terminaux mobiles.

75009 Paris France
http://www.thegreenbow.com

THREATQUOTIENT INC.

ThreatQ (TIP) permet de disposer du contexte, de la personnalisation et de la priorisation nécessaires pour prendre de meilleures décisions, accélérer la détection et la réponse aux incidents.

20191 Reston États-Unis
https://www.threatq.com

TIXEO H CL

La visioconférence sécurisée Tixeo (certifiée/qualifiée ANSSI) s'adapte à toutes les infrastructures avec les solutions TixeoCloud, TixeoServer (serveur en interne) et TixeoPrivateCloud (infogéré).

34080 Montpellier France
https://www.tixeo.com

TRANSFERTPRO

Société 100 % française: échange de fichiers volumineux ; stockage, partage, collaboration ; CFN ; HDS ; OP/Saas ANSSI ; CSPN ; qualification élémentaire ; SecNumCloud (wip).

75017 Paris France
https://www.transfertpro.com

TRANSMIT SECURITY

Fournisseur de solution innovante – 1er service d'authentification biométrique Passwordless Omni-Device et Omni-Canal – 0 Mot de passe – 0 Login – 0 Application – 0 Phishing – 0 Fraude – 100 % sécurisé.

75000 Paris, Nantes, Toulouse, Nice France
http://www.transmitsecurity.com

TRELLIX CL

Trellix est le fruit du rachat de FireEye et de McAfee enterprise. Evolutive l'entreprise fournit des solutions de cybersécurité adaptables et innovantes s'articulant autour de la technologie de détection et de réponse étendue XDR.

92800 Puteaux France
http://www.trellix.com

TREND MICRO CL

Notre offre protège les activités des utilisateurs, toutes les applications, tous les dispositifs, en tout lieu, les environnements virtuels, Cloud et hybrides, le réseau face aux attaques ciblées.

9250 Rueil-Malmaison France
http://www.trendmicro.fr

TRICENT

Tricent est une solution automatisée qui aide les entreprises à protéger leurs données en apportant des contrôles avancés sur le partage de fichiers Google Workspace et MS365.

1599 Copenhague Danemark
http://tricent.com

TRUSTINSOFT H N

TrustInSoft commercialise dans le monde entier des outils et services d'analyse exhaustive de code source C et C++ permettant de garantir mathématiquement la qualité des logiciels de ses clients.

75014 Paris France
https://trust-in-soft.com

TRUSTWAVE

Trustwave aide les entreprises à lutter contre la cybercriminalité avec ses offres de technologies sécurité réseau, application et données en mode licence ou SAAS également disponibles en mode gérés.

80807 Munich France
http://www.trustwave.com

TUFIN

Tufin permet aux entreprises d'automatiser la visibilité de leurs politiques de sécurité, la gestion des risques, la mise en œuvre et la conformité dans tout leur environnement hybride.

75017 Paris France
https://www.tufin.com/fr

UBIKA H

UBIKA est un fournisseur européen de cybersécurité. Notre technologie Web Application & API Protection se déploie sur site, dans le cloud, mode SaaS ou comme conteneur. 100% souverain et automatisé.

92360 Meudon France
https://www.ubikasec.com/fr

UNISYS N

Unisys a développé une solution 0 Trust (leader selon Forrester, Gartner) avec les fonctionnalités suivantes: invisibilité de l'infrastructure, accès distant, micro segmentation, isolation dynamique.

92250 La Garenne Colombes France
http://www.Unisys.com

USERCUBE

Usercube est une solution de gestion des identités et des habilitations de nouvelle génération, leader sur le marché du SaaS (certifié ISO27001) mais aussi disponible en mode On Premise.

13825 La Penne sur Huveaune France

http://www.usercube.com

VADE SECURE H

Notre solution de protection de l'email predictive utilise l'IA et les données du milliard de boîtes mail que nous protégeons, pour bloquer les attaques ciblées dès le premier email.

59510 Hem France

https://www.vadesecure.com

VARONIS

Varonis est une plate-forme innovante de sécurité des données qui permet aux entreprises de gérer, d'analyser et de sécuriser les données d'entreprise contre les menaces internes et les cyberattaques.

92400 Courbevoie France

VECTRA NETWORKS

Vectra est une société qui utilise l'intelligence artificielle pour détecter et traiter les cyber-attaques en temps réel.

8808 Pfaffikon Suisse

VEEAM

Fournisseur innovant de solutions de disponibilité assurant la continuité d'activité des entreprises (Availability for the Always-On Enterprise™).

92800 Puteaux France

https://www.veeam.com/fr

VENAFI

Venafi est le créateur et leader de la catégorie de marché Protection des Identités Machines. Nos solutions permettent d'obtenir Visibilité, Intelligence, Automatisation du cycle de vie des identités.

UT 84111 CARRY-LE-ROUET

Salt Lake City États-Unis

https://www.venafi.com/fr

VERACODE

Veracode est le précurseur de la sécurité applicative en mode DevSecOps. Offre 100 % Cloud, Veracode traite l'appSec sous toutes ses formes : statique, dynamique, composants Open Source, containers…

EC4 Londres Royaume-Uni

https://www.veracode.com

VERIZON

Fournisseur mondial de solutions de communications : plateformes sécurisées de mobilité, Cloud, réseau stratégique, Internet des objets, communications avancées, UCC, SOC, NOC, SIEM, SDN, SDP, Forensics, IAM.

92042 Courbevoie France

http://www.verizonenterprise.com/fr

VMWARE N

VMware, un leader mondial des infrastructures Cloud et de la mobilité d'entreprise, aide les organisations à accélérer leur transformation numérique.

92042 Paris La Défense France

https://www.vmware.com/fr.html

VULCAN CYBER

Vulcan propose la seule plateforme de Cyber Risk Management permettant:- d'avoir une vision à 360 degrés de son exposition aux risques- et d'orchestrer et d'automatiser la remédiation.

75000 Paris France

https://vulcan.io

WALLIX N H

Le Bastion WALLIX est une solution de gestion des accès à privilèges intègrant la gestion des mots de passe, un portail d'accès web, la gestion des accès et l'enregistrement des sessions.

75008 Paris France

WASACA

WaSaCa est le distributeur référent en France des solutions Endpoint Protector by CoSoSys by Invintia. Certificateur exclusif en France, il recrute, forme, certifie et anime un réseau de revendeurs.

75008 Paris France

htt://www.wasaca.fr

WATCHGUARD TECHNOLOGIES

WatchGuard est un acteur majeur dans le domaine de la sécurité et l'intelligence réseau, du Wi-Fi sécurisé, de l'authentification multifacteur et de la protection avancée des Endpoints.

92320 Châtillon France

https://www.watchguard.com

WITHSECURE

WithSecure™, anciennement F-Secure Corporation, est le partenaire européen de référence en matière de cybersécurité depuis plus de 30 ans.

92500 Rueil-Malmaison France

https://www.withsecure.com/fr/home

WOLEET

Woleet sécurise vos documents avec une preuve universelle horodatée d'existence ou de signature grâce à la Blockchain.

35577 Cesson-Sévigné France

https://www.woleet.io

WOOBE

Identité numérique & Signature électronique sans fichier central des données - Irrévocable - Supranational.

95300 Pontoise France

http://www.woobe.fr/w1

WOOXO N

Wooxo édite des solutions pour éliminer les risques d'interruption d'activité et la perte potentielle de données informatiques consécutifs à tout type de sinistre informatique.

13600 La Ciotat France

https://www.wooxo.fr

WRAPTOR N

Une protection antispam efficace à 100%, sans aucune perte de messages, grâce à une méthode de vérification de la relation entre vous et vos contacts de courrier électronique.

13400 Aubagne France

http://www.spamwars.fr

YAGAAN

YAGAAN développe et commercialise un scanner de code source de nouvelle génération. Grâce au machine learning, la YAG-Suite est une solution pertinente et abordable pour vos audits de code.

35 510 Rennes - Cesson Sévigné France

http://www.yagaan.com

YESWEHACK N C L C S H

YesWeHack est la 1re plateforme européenne de Bug Bounty et de VDP. La plateforme met en relation des organisations avec 18 000+ hackers éthiques pour sécuriser leurs périmètres exposés.

75004 Paris France

https://www.yeswehack.com

YOUZER N

Youzer est une plateforme de gestion des utilisateurs et de leurs idéntités.

75015 Paris France

https://www.youzer.net

ZERTIFICON SOLUTIONS GMBH

Solutions logiciels On-Premise et Cloud d'automatisation de la signature et du chiffrement des e-mails avec certificats de norme internationale S/MIME et PGP, ainsi que par mots de passe.

12347 Berlin Allemagne

https://www.zertificon.com/france

ZIWIT

Scanner de vulnérabilité web garanti zéro faux positif. Audits automatisés, rapports de failles, correctifs à appliquer et simulation d'attaques. Suivi technique personnalisé inclus.

34000 Montpellier France

https://httpcs.com

ZSCALER N

Zscaler apporte à chaque utilisateur une expérience Internet productive et sécurisée, quel que soit le terminal utilisé et l'endroit où il se trouve, en mode SaaS et 100 % Cloud.

92400 Courbevoie France

https://www.zscaler.fr

ZYXEL FRANCE

Zyxel propose une gamme de solutions de sécurité destinées aux entreprises, pour les aider à protéger et faciliter la gestion de leurs réseaux. Elle comprends les gammes Zywall USG, ATP et VPN.

69760 Limonest France

http://www.zyxel.fr

Prestataires de services

2SI CONSULTING N

2SI Consulting est un cabinet de conseils et de services spécialisé dans la cybersécurité et la protection des données personnelles qui vous accompagne dans votre transformation digitale.

97160 Le Moule France

https://www.2siconsulting.com

ABAKUS SÉCURITÉ N

Abakus Sécurité est un intégrateur de solutions de sécurité, expert des SIEM (QRadar), SIRP (Resilient), logiciels d'investigation (i2) et de la protection des appareils mobiles (MaaS360).

75008 Paris France

http://www.abakus-securite.fr

ABINGTON ADVISORY

Accompagnement (AMOA et expertise) au niveau : organisationnel ; technologique (architectures et hardening de composants) ; conformité (RGPD, NIS, LPM, ISO 27K...).

75800 Paris France

https://www.abingtonadvisory.com/fr/cybersecurite-confiance-numerique

ACCEIS

ACCEIS est une entreprise d'expertise en cybersécurité créée par deux experts techniques, proposant une offre transverse d'audits, de conseil et de formations sur le plan technique et organisationnel

35000 Rennes France

http://www.acceis.fr

ACCENTURE N

L'offre sécurité d'Accenture couvre 5 domaines : Cyberdefense, Identité Numérique, Stratégie & Risk, Sécurité Applicative et Services Managés. Accenture a acquis Arismore et Memority.

75636 Paris France

https://www.accenture.com/fr-fr

ACELYS SERVICES NUMÉRIQUES

Conseil et expertise. Analyse Risques. Gouvernance (RSSI/DPO, ISO 27001, PSSI). Audits (organisationnels et techniques), pentests. Ingénierie de la sécurité (architecture, solutions, configuration...).

34000 Montpellier France

https://www.acelys.fr

ACESI GROUPE N

Fournir à nos clients un accompagnement global, aussi bien sur des aspects organisationnels que techniques. Nos prestations vont du test d'intrusion jusqu'à la mise en œuvre d'un Système de Management

67960 Strasbourg - Entzheim France

http://www.ace-si.com

ACTIVANOS SAS

Spécialiste en architecture Microsoft Active Directory et Cloud.

34500 Béziers France

http://www.activanos.com

ACTIV'INFO

Nous accompagnons et mettons en oeuvre dans les TPE/PME (max 50 users) une informatique sécurisée, documentée, conforme RGPD. Des méthodes issues des grands comptes à la portée des plus petits.

33360 Camblanes et Meynac France

https://www.activinfo.fr

ACTUELBURO

Nos collaborateurs vous assistent dans l'optimisation et la gestion de vos systèmes d'information et votre mobilité de façon efficiente et concurrentielle. Audit de sécurité, pentest, maintenance, etc.

ORTHEZ 64300 France

https://www.actuelburo.fr

ADACIS

Qualifiée PASSI par l'ANSSI pour audits : test d'intrusion /configuration /architecture /organisationnel et physique. Solution d'Analyse de risque labélisée conforme à la méthode Ebios RM par l'ANSSI.

3150 CENON France

https://www.adacis.net

ADENIUM CL

Adenium est une société spécialisée dans la mise en œuvre de Plan de continuité d'activité (PCA) selon ISO 22301 et la résilience des organisations.

75020 Paris France

https://www.adenium.fr

ADIKTS

Adikts est un cabinet de conseil IT spécialisé sur la Sécurité Applicative (DevSec, DevSecOps), le cloud AWS (Architecture) et la conception d'applications autour de stacks techniques opensources.

78360 Paris France

https://www.adikts.io

ADVENS CL CS

Advens est le premier pure-player français de la cybersécurité. Nous avons développé une offre globale, proposant des réponses adaptées à chaque secteur, à chaque acteur, à chaque besoin.

75009 Paris France

https://www.advens.fr

ADVENTIUM TECHNOLOGIES N

Intervention sur l'audit, la gouvernance et la mise en oeuvre des politiques de sécurité.
Cellule de CyberSécurité en cours de création.»

75005 Paris France

http://www.adventium.fr

ADVISO

Adviso, expert en sensibilisation à la cybersécurité, vous accompagne de l'élaboration à la mise en œuvre de votre stratégie de sensibilisation. 2019 : 100 000 collaborateurs formés, dans 15 pays.

92048 Paris La Défense Cedex France

http://www.adviso.fr

AGENCEE

Audit, Conseils, Analyse, Implémentation, Controle pour PME PMI sur la sécurité informatique. Sensibilisation à la sécurité informatique.

31600 Eaunes France

http://www.agencee.fr

AKAMAI TECHNOLOGIES

En assurant une protection contre les attaques les plus sophistiquées, Akamai vous aide à protéger vos sites Web et applications en ligne des risques d'indisponibilité et de vol de données.

75008 Paris France

https://www.akamai.com/fr/fr

AKERVA

Société de conseil spécialisée en sécurité du SI et Cyberdéfense : Audits et Tests d'intrusion. Gouvernance & Sécurité du SI. Formation & E-Learning. SOC & Centre de cyberdéfense.

75008 Paris France

https://akerva.com

AKKA N

AKKA allie son expérience de l'électronique automobile, des réseaux, de l'architecture et des TI et son expertise en matière de cybersécurité pour lutter contre les risques.

92977 Paris-La Défense France

https://www.akka-technologies.com

ALASTAR

Sécurisez votre SI grâce à l'expertise Alastar, votre partenaire ExpertCyber. Cybersécurité. Gestion de l'infra. Sauvegarde. RGPD.

56800 Ploermel France

https://www.alastar.fr

ALEKSO

QUIVIV développe et opère des solutions de cybersécurité en SaaS reposant sur les principes de simplicité et d'efficacité, centré sur les usages et mis en œuvre dans une interface unique de pilotage.

92350 LE PLESSIS-ROBINSON France

http://www.alekso.fr

ALENATEC

Société de services et de conseils en informatique spécialisé en sécurité informatique : Audits techniques et organisationnels, Conseil, ingénieries, expertise technique, Intégration et développement.

75008 Paris France

https://www.alenatec.com

ALGOSECURE

AlgoSecure est un cabinet de conseil spécialisé en sécurité informatique. Nous réalisons des audits de sécurité et des tests d'intrusion pour vous aider à sécuriser votre système d'information.

69120 Vaulx-en-Velin France

ALLISTIC N

Allistic, pure player de la cybersécurité, accompagne ses clients dans leur stratégie cybersécurité, la gestion de la confiance numérique, la protection des menaces digitales et la sensibilisation.

59000 Lille France

https://www.allistic.fr

ALMOND C L C S

Nous sommes spécialisés en Cybersécurité et nos savoir-faire reposent sur 5 expertises : Offensive Security, Defensive Security, Infrastructure Security,Compliance et SOC-CERT CWATCH.

92310 Sèvres France

http://almond.consulting

ALTRAN TECHNOLOGIES N

Nos services couvrent l'IT, l'IOT, les syst. industriels, les systèmes embarqués et s'appuient sur nos labs, nos partenariats et nos centres d'expertises internes (Analytics, IOT, Industrie 4.0…).

92807 Puteaux France

http://www.altran.com

AMBICIO

Nous proposons d'auditer et-ou d'accompagner les entreprises dans l'évaluation et la sécurisation de leur SI. Nous bénéficions d'une solide expérience d'audit des SI adaptée au RGPD.

92100 Boulogne-Billancourt France

https://www.ambicio.fr

AMBIONICS SECURITY

Notre approche réaliste et offensive éprouve la sécurité de vos applications web en continu. Leurs vulnérabilités sont détectées et qualifiées, et l'efficacité des correctifs validée.

75009 Paris France

AMOSSYS

Société de conseil et d'expertise en cybersécurité, AMOSSYS propose une offre globale de services pour sécuriser ses SI : audit PASSI, conseil SSI, réponse à incident, évaluation CSPN ou CC, LID…

35000 Rennes France

https://www.amossys.fr

ANEXIS

Stratégie pour une meilleure cyber-résilience, conformité RGPD, organisation agile, transition numérique... nous accompagnons les TPE - PME dans leur démarche de développement et de sécurisation.

33000 Bordeaux France

https://www.anexis.fr

APIXIT N C L

APIXIT est expert dans la transformation numérique des entreprises en Cybersécurité, Infrastructures et Cloud : audit, conseil, intégration, MCO et services managés, assistance technique.

91940 Les Ulis France

https://www.apixit.fr

APSIDE N C L

Apside : Conseil, ingénierie SI, ingénierie industrielle, ingénierie infrastructure.

92100 Boulogne-Billancourt France

https://apside.com

ARMATURE TECHNOLOGIES N

Cabinet de conseil indépendant spécialisé en sécurité des systèmes d'informations : test d'intrusion, cybersécurité, cyberdéfense, risque, conformité et gouvernance, architecture orientée sécurité.

75008 Paris France

http://www.armaturetech.com

ASSYSTEM C L

Conseil en gouvernance de la sécurité, accompagnement à l'homologation, Intégration, MCS.

78180 Montigny le Bretonneux France

http://www.assystem.com

ATE

Expert français en hébergement et infogérance de systèmes d'information stratégiques. Solutions Cloud sur mesure ultra sécurisées. Hébergeur certifié de données de santé (HDS) et ISO 27001.

59650 Villeneuve d'Ascq France

https://www.ate.info

ATN GROUPE

ATN Groupe est une ESN fondée en 1997, spécialisée dans les infrastructures informatiques, les applications cloud ainsi que les réseaux et télécoms qui est reconnu dans le domaine de la cybersécurité.

38240 Meylan France

AUTICONSULT N

Auticonsult est la 1re ESN française à employer des consultants informaticiens autistes. Nous intervenons dans les domaines de la Cybersécurité, de la Data, du Développement et du Test.

92400 Courbevoie France

https://auticonsult.fr

AVITI

Aviti fournit des prestations de services autour de l'infrastructure systèmes et réseaux et des solutions d'infogérance. Aviti propose aussi du Cloud Computing à travers sa propre marque CloudDirect.

44300 Nantes France

https://www.aviti.fr

AXEL IT

Spécialiste de l'intégration IT des Entreprises, nous combinons 8 centres de compétences pour servir votre transformation digitale au travers des Infrastructures et de l'Outillage des processus IT.

92800 Puteaux France

https://www.axelit.fr

AXIANS C L N

Axians, marque de VINCI Energies dédiée à l'ICT, vous accompagne dans vos projets de cybersécurité, dans l'intégration et l'infogérance de votre système d'information.

69200 Vénissieux France

https://www.axians.fr

AXIANS C&C MARSEILLE-NICE-MONACO C L N

Axians accompagne ses clients et propose son savoir-faire pour couvrir l'ensemble des besoins de sécurité numérique des entreprises: conseil et conformité, audits, intégration, services managés.

13011 Marseille France

https://www.axians.fr/fr

AXICOM-SECURITE

Société d'intégrateur,d'audit et conseils solution orienté sécurité périmètre et terminaux ainsi qu'audit Rgpd et gestion de risque.

75002 Paris France

Https://axicom-security.com

AZERI BEGI CYBERSÉCURITÉ

Azeri begi est spécialisé en cybersécurité des entreprises dans les départements du pays basque et des landes. Nous effectuons des audits, formations, interventions (en cas d'attaques).

64240 Macaye France

https://www.azeri-begi.fr

BEA INFORMATIQUE

BEA est labellisées ExpertCyber et se distingue par une approche en Cybersécurité à 360°. Nous traitons le volet autant technique qu'organisationnel et couvrons de la Gouvernance jusqu'aux Pentests.

30100 Ales France

https://www.bea-informatique.fr

BEARINGPOINT

BearingPoint a développé ses activités de conseil en cyber sécurité autour de 3 grands axes : stratégie et sensibilisation, gestion des risques et gestion de crise, conformité règlementaire.

92907 Paris-La Défense Cedex France

http://www.bearingpoint.com

BLUESCREEN

BLUESCREEN est un MSP qui apporte à ses clients une offre d'infogérance sans engagement et illimitée sur poste utilisateur, serveur et CLOUD.

69760 Limonest France

https://bluescreen.fr

BOCK CONSEIL

Cybersécurité des SI industriels : formation, transfert de compétences, assistance à maîtrise d'ouvrage et maîtrise d'œuvre. Expérience de 8 ans à plein temps sur tous types de procédés.

69100 Villeurbanne France

https://www.bockconseil.fr

BRIGHTWAY C L

Brightway est un cabinet proposant une offre complète en cyber sécurité et gouvernance des données: audit, conseil, alerte et avertissement (SOC/CERT), réponse à incident et formation certifiante.

92310 Sèvres France

https://www.brightway.fr

BSI FRANCE CL

BSI France organisme de certification et de formation, vous propose des solutions de cyber sécurité, sécurité de l'information et de conformité au Règlement général sur la protection des données.

75017 Paris France

BSSI CONSEIL ET AUDIT CL

Conseil et audit en cybersécurité.

75009 Paris France

https://www.bssi.fr

BUG BOUNTY ZONE

Bug Bounty Zone est la première plateforme professionnelle de bug bounty proposant plusieurs niveaux d'expertise en cyberdéfense.

13014 Marseille France

https://www.bugbountyzone.com

BY THE WAY

By The Way assure des missions d'audit, d'étude, de définition & de mise en œuvre d'architectures systèmes et réseaux dans les domaines de la sécurité, de la mobilité et des infrastructures systèmes.

59175 Vendeville France

https://www.bytheway.fr

CALYPT CYBERSÉCURITÉ

Calypt est une société de cybersécurité basée à Lyon opérant sur tout le territoire français. Nous proposons audits, formations agréées, conseils, développement… pour entreprises de toute taille.

69003 Lyon France

https://www.calypt.com

CAPGEMINI - SOGETI N

Nous proposons des services de sécurité de bout en bout intégrant conseil, protection et surveillance pour protéger votre entreprise.

92130 Issy les Moulineaux France

https://www.sogeti.com/services/cybersecurity

CAPGEMINI TECHNOLOGIE SERVICES - SOGETI N CL

Notre offre inclut de l'audit/pentest (PASSI & PASSI LPM), du conseil stratégique et opérationnel, de l'intégration/run, de la surveillance (SOC PDIS) et de la réponse à incidents (CERT et SWAT).

92130 Issy les Moulineaux France

https://www.fr.sogeti.com/expertise/nos-activites/cybersecurite

CEGEDIM OUTSOURCING N

Cegedim Outsourcing, spécialiste dans les métiers de l'infrastructure IT, délivre aux entreprises de toutes tailles des services d'intégration, d'infogérance et des prestations en assistance technique.

78457 Vélizy Cedex France

http://www.cegedim-outsourcing.fr

CEIS CL

CEIS Cyberdéfense propose une offre complète et intégrée à 360 degrés à destination des entreprises ne disposant pas d'une organisation dédiée à la cybersécurité ou souhaitant la renforcer.

75015 Paris France

https://www.ceis.eu

CGI FRANCE N CL

Notre offre sécurité et gestion des risques s'étend aux métiers de CGI : conseil, intégration, services managés. Nos domaines d'interventions sont : gouvernance SSI, IAM, SOC, PCA, audit et tests…

92400 Courbevoie France

http://www.cgi.fr

CLARANET N

Expert en infogérance d'applications critiques et en sécurité. Hébergement sécurisé et conforme (PCI DSS & 27001). Offre sécurité : pentests/audits, Soc as a Service, Services managés.

75011 Paris France

http://www.claranet.fr

CNPP CYBERSECURITY CL

Audit, conseil et formation en sécurité des systèmes d'information.

Gouvernance, risques et conformité : ISO 27001, PCI DSS, ISO 22301... Technique et sécurité opérationnelle. Forensic.

75017 Paris France

http://www.cnpp-cybersecurity.com

CO-C

Expert en sécurité intrusive indépendant : tests d'intrusion (physique, externe, interne) ; Audit de sécurité (LAN, datacenter, cloud) ; Audit de configuration ; Formation sécurité et sensibilisation.

69160 Tassin France

http://www.co-c.net

COESSI CL N

Qualifiée PASSI RGS, reconnue pour ses travaux innovants en sécurité des systèmes industriels et de l'IoT, CoESSI intervient tant en Cybersecurité qu'en protection de la vie privée (RGPD) des SI.

92000 Nanterre France

https://www.coessi.com

COGITAL

Cogital est spécialisé en Cybersécurité. Nos activités portent sur l'Audit, le Conseil, l'intégration et les Services Managés. Nous sommes certifiés techniquement auprès de nos partenaires éditeurs.

75014 Paris France

https://www.cogital-it.com

CONIX CL

Expertise technique : audit / test d'intrusion, SOC managé, réponse à incident. Expertise conseil : référentiels SSI, analyses de risques, sensibilisation, tableaux de bord.

92130 Issy-les-Moulineaux France

http://www.conix.fr

CONSEILPREV CYBER

Christophe CERF, 26 years en conseil & expertise mutli-sectors Oil&Gas, Energy & Power, Renewables, Railway, Automotive, Buildings, Nuclear, Industry, Manufacturing, Pharmaceutical.

75014 PARIS France

https://conseilprevup.com

CONSORT N

Consort intervient sur l'ensemble du cycle de sécurisation et de protection des accès, des données, des tentatives d'intrusions, des tests de vulnérabilité.

75017 Paris France

http://www.consort-group.com

COREYE N

COREYE se positionne comme un MSSP (Managed Security Service Provider), accompagne ses clients avec son offre de sécurité CoreTrust (SOC externalisé, WAF, Anti-DDos, SIEM) et est certifié ISO27001.

59262 Sainghin-en-Mélantois France

http://www.coreye.fr

CORTEXERA

Avec plus de 25 ans d'expertise, nous proposons pour toutes les entreprises. Conseil, intégration, formation et RSSI à temps partiel. Certifié ISO27001, Label ExpertCyber, CISSP, CoBIT.

13008 Marseille France

https://www.cortexera.com

C-RISK CL

Expert en quantification des risques (CRQ), C-Risk aide les entreprises à comprendre les risques en termes financiers, prioriser les investissements et améliorer la cyber-résilience et la conformité.

92931 Paris La Défense France

https://www.c-risk.com

CS GROUP N

CS GROUP propose une offre globale : Conseil (PASSI LPM), Intégration, Services (CERT-CS/GIR, NOC/SOC), éditeur (Prelude SIEM, Vigilo NMS, Unity 360, Trusty - Confiance Numérique, SEDUCS - OS durci).

92350 Le Plessis Robinson France

http://www.csgroup.eu

CS NOVIDY'S

CS Novidy's propose une offre globale : Conseil (PASSI LPM), Intégration, Services (CERT-CS/GIR, NOC/SOC), éditeur (Prelude - SIEM, Vigilo - NMS, Trusty - IGC, horodatage, coffre-fort, SEDUCS - OS durci).

92350 Le Plessis Robinson France

http://www.c-s.fr

CYBER-EGIDE

Cyber-Egide propose un audit sur mesure de votre entreprise pour trouver et résoudre les vulnérabilités de votre réseau. Nous proposons aussi un logiciel qui protège tous vos pc, téléphones et réseau.

75005 Paris France

https://www.cyber-egide.fr

CYBERENS

Conseil en ingénierie de sécurité sur la base d'analyses de risque.

Édition de logiciels de protection des données : client sécurisé de messagerie (SET) pour Windows, bibliothèque cryptographique.

33000 Bordeaux France

https://www.cyberens.fr

CYBERGLOBAL

Cyber accompagnés (suivi) – Cyber formés (formation) – Cyber assurés (assurance).

1700 Miribel France

https://cyberglobal.fr

CYBERSEC&YOU

Cybersec&You est le distributeur à valeur ajoutée de l'ensemble des produits et services des membres d'Hexatrust. Nous proposons un guichet unique pour les organisations publiques et privées.

78750 Mareil-Marly France

https://www.cybersecandyou.com

CYBERSOLUTIONS N

Société de conseil et intégration en cybersécurité : sécurité des API & prévention de fraude ; SOAR & SIEM ; surveillance du Deep & Dark Web ; audit de sécurité, audit des API & formation.

75003 Paris France

https://cybersolutions.fr

CYBERZEN

Conseil stratégique, audit fonctionnel et organisationnel pour due dilligence ou accompagnement, prestation de conseil sur le moyen terme et offre de sensibilisation innovante.

75001 Paris France

https://www.cyberzen.com

DATA PRIVACY PROFESSIONALS N

Services de DPO externe et de mise en conformité RGPD à l'international (fr, eng, ger). Formations B2B (Datadock, OPCO) et B2C (Mon Compte Formation) : cybersécurité, RGPD, transformation numérique.

67114 Eschau France

https://www.dataprivacy.pro

DAVID INFORMATIQUE N

Offres de services proactives incluant direction de SI, infogérance niveau 1-2-3 physique / Cloud, sécurité (système de reprise d'activité, firewall…) avec engagement de temps de reprise d'activité.

21200 Beaune France

http://david-informatique.com

DBM PARTNERS

Cabinet de conseil à taille humaine, nous aidons nos clients à maîtriser leurs risques numériques sur les domaines Cybersécurité, Digital Workplace, Gouvernance de l'information et Projets.

75116 Paris France

http://www.dbm-partners.com

DEEPIT

DeepIT est une entreprise spécialisée en informatique médicale qui fournit à ses clients des services de maintenance allant du support au dépannage informatique, en passant par la prévention sécurité

1040 Etterbeek Belgique

https://www.deepit.be

DELOITTE C L

Deloitte est classé numéro 1 mondial des services de conseil en cyber sécurité par Gartner pour la 5e année consécutive. Une offre pluridisciplinaire au service de toutes les organisations.

92200 Neuilly-sur-Seine France

https://www2.deloitte.com/fr/fr.html

DEVELOPPEMENT CONSEIL COMMUNICATION

ESN spécialisée en cybersécurité, réseau et transformation digitale. prestations de conseil, d'intégration, infogérance dans le domaine de la sécurité. opérations de prévention et remédiation en cyber.

59710 Merignies France

https://www.dc-communication.eu

DEVENSYS CYBERSECURITY H

Pure player en cybersécurité. Créé il y 10 ans. 40 collaborateurs et experts. Red Team & Pentest - Sécurité Cloud & Infrastructure - Sécurité Managée (SOC 24/7 en 30 min) - Formation & Certification.

34000 Montpellier France

https://www.devensys.com

DEVOTEAM C L N

Transformer le risque en opportunité Business. Devoteam soutient les entreprises dans leur transformation digitale en intégrant la sécurité dans les projets, et veille au maintien de leur résilience.

92300 Levallois-Perret France

http://www.devoteam.fr

DIGITAL SECURITY C L C S

Digital.security est une société de services spécialisée en sécurité numérique. Premier CERT™ IoT, digital.security emploie 250 experts certifiés PASSI, ISO 27001, ISO 27005, CISSP, CMMI, ITIL.

75012 Paris France

https://www.digital.security/fr/

DIGITEMIS CYBERSECURITY & PRIVACY N C L H

Prestataire qualifié PASSI par l'ANSSI. 7 labels CNIL (audit & formation). Tests d'intrusion, audit architecture, gouvernance. Focus : Iot, sécurité des fournisseurs, systèmes industriels, Phishing.

44400 Nantes France

https://www.digitemis.com

DIGORA N C L

Analyse des mesures et évaluation des risques liés aux bases de données en 3 étapes : identifier des actifs SGBD, analyse des mesures en fonction d'un référentiel, cartographie des mesures de sécurité.

67000 Strasbourg France

https://www.digora.com/fr/expertises/securite/analyse-risques

DILITRUST N

DiliTrust offre une gamme de solutions et services dédiés à la Gouvernance : Gestion des Conseils et Comités, des Data rooms, transfert sécurisé de données sensibles ou volumineuses.

92059 La Défense France

http://ww.dilitrust.com

DPO CONSULTING N

DPO Consulting est une société de conseil spécialisée en protection des données personnelles qui a pour objet d'accompagner les entreprises dans la mise en conformité au RGPD.

75009 Paris France

https://dpo-consulting.fr

DYNAMIT

Cap Antigone est en mesure de vous accompagner depuis la création d'une infrastructure à partir d'une feuille blanche.

92000 NANTERRE France

https://www.dynamitservices.fr

EBRC H

Cyber-Resilience services : conseil en gestion des risques ICT, Business Continuity, ISO27001-22301, PCI DSS, Pentests, DC Tier IV ; SOC, Gestion des vulnérabilités, Cyber-Securité & Forensics.

2453 Luxembourg Luxembourg

http://www.ebrc.com

E-CATALYST N

Formation en cybersécurité, audit en cybersécurité, création de sites web, campagne de communication digitale, appui à la mise en conformité au RGPD, maintenance informatique.

59600 Maubeuge France

https://e-catalyst.fr

ECO HARDWARE SAS

Contrat de maintenance, infogérance informatique. Solutions Cloud. Société spécialiste en sécurité informatique. Entreprise de cybersécurité. Récupération de données disque dur NAS.

75015 Paris France

https://www.eco-hardware.fr

EIFFAGE ENERGIE SYSTÈMES - CLEMESSY C L

Clemessy, la marque dédiée à l'industrie du groupe Eiffage répond aux besoins des industries les plus exigeantes dans le domaine de la cybersécurité, pour exploiter en toute sécurité les installations.

68100 Mulhouse France

https://www.clemessy.com

EIGHT TECH

Infogérance des systèmes informatiques professionnels. Sécurisation, optimisation et performance des systèmes et des réseaux. Conseil, déploiement et accompagnement.

34170 Castelnau le Lez France

https://8tech.fr

EITA CONSULTING N

Conseil, ingénierie SI, ingénierie industrielle, ingénierie infrastructure, Installation Fibre Optique (D1, D2, D3), Antenne G5, IoT, IA.

78360 Montesson France

https://www.eitaconsulting.fr

ELIT-CYBER

Elit-Cyber propose une offre de cybersécurité globale : SOC & CSIRT, PAS & PSSI, audits, scans de vulnérabilité, campagnes de phishing, tests d'intrusion, sensibilisation, analyse forensique, etc.

92400 COURBEVOIE France

https://elit-cyber.com

ENGIT N

engIT conseil et accompagne ses clients dans les aspects liés à la sécurisation de leur SI. Gouvernance GRC, Audit, Ethical Hacking (Pentest), Analyse de Risques, Firewalling, Conformité...

06250 Mougins France

https://engit.fr

ETELCOM S.A.S.

Société de services d'ingénierie informatique spécialisée dans la sécurité informatique. Audit, conseil, surveillance, installation, maintenance et infogérance informatique et Télécom.

56400 Auray France

https://www.etelcom.fr

EXAPROBE - GROUPE ECONOCOM N

Exaprobe est un opérateur souverain de sécurité augmentée, intervenant autour de quatre axes: le conseil, l'intégration, les services managés & l'infogérance et les offres packagées en mode SAAS.

92350 Le Plessis-Robinson France

http://www.exaprobe.com

EXCELLIUM SERVICES

With its headquarter in Luxembourg and more than 90 security professionals, Excellium is the leader of Cybersecurity services regarding Application Security and Security Incident management.

L-5326 Contern Luxembourg

https://www.excellium-services.com

EXODATA N

Exodata est un MSP qui place la sécurité au cœur de son offre. Elle accompagne ses clients dans leur transformation digitale, avec un support 24/5 sans surcoût grâce à un positionnement Follow the Sun.

Paris 75001 France

https://www.exodata.fr

EXPONENS

Audit et conseil en gouvernance et sécurité des SI.

75107 Paris France

http://www.exponens.com

EXTERN IT N

Service informatique externalisé pour PME et assos, nous avons développé une offre de services cybersécurité adaptée à ces structures pour leur permettre de se protéger et se relever d'un incident.

59118 Wambrechies France

https://www.extern-it.fr

EXTIA

92370 Sèvres France

https://extia.fr

EXTREMIT CS

extremIT est une Entreprise de Services du Numérique qui accompagne les PME des Hauts-de-France dans leur politique de cybersécurité (audit préalable, résolution d'incidents, prévention et formation).

59650 Villeneuve d'Ascq France

http://www.extremit.fr

FIDENS CL

FIDENS à la pointe de l'expertise de la cybersécurité depuis plus de 15 ans, nos équipes réunissent des professionnels aguerris et certifiés, experts des techniques, méthodes et standards du domaine.

75009 Paris France

https://www.fidens.fr

FORMIND N CL H

Formind est un leader français indépendant expert en cybersécurité, qualifié PASSI. Avec 250 consultants, Formind accompagne ses clients sur toute problématique avec une approche risque.

92130 Issy-les-Moulineaux France

http://www.formind.fr

G-ECHO N

Diagnostic, conseil, audit, expertise, Accompagnement (formation, recrutement), Solutions (gestion des risques et vulnérabilités, tests de sécurité, DLP…).

31380 Garidech France

http://www.g-echo.fr

GPLEXPERT

Conseils & Services en Ingénierie Informatique spécialiste du Système d'Information Sécurisé. Système, Réseaux, Open source, Hébergement, Supervision, Cybersécurité, Gestion de crise. ISO27001 & HDS.

91290 Arpajon France

https://gplexpert.com

GRAND E NOV N

Accompagnement suite Diagnostic Compétitivité Région Grand Est

67100 Strasbourg France

http://www.grandenov.fr

GROUPE INFODIS

La stratégie du groupe INFODIS et de ses actionnaires (dirigeants, LBO France et BPI France) est de placer INFODIS en leader des services d'intégration, d'infogérance et de support aux infrastructures.

95100 Roissy En France France

https://www.infodis.com

GROUPE SII N CL

Le Groupe SII apporte une expertise sur la confiance numérique dans les domaines de l'informatique industrielle, du système d'information et de l'IoT à travers son offre SECURE DIGITAL FACTORY.

35510 Cesson-Sévigné France

http://www.groupe-sii.com

HARMONIE TECHNOLOGIE N

Partenaire des Grands Comptes, nous couvrons l'ensemble de la cybersécurité : la stratégie SSI, le management des identités et des accès, et la gouvernance et la protection des données.

75008 Paris France

https://www.harmonie-technologie.com

HEADMIND PARTNERS

HeadMind Partners est un acteur majeur du Conseil au sein de l'écosystème Cybersécurité, apportant une expertise sur l'ensemble de la chaîne de confiance auprès de +100 entreprises Grands Comptes.

75016 Paris France

https://www.headmind.com

HELIX SECURITY SAS

Conseils, formations et accompagnement dans la sécurité. Prestataire de Service proposant SOC et une gamme étendue de services.

97460 Saint Paul France

https://www.helixsecurity.cloud

HEXANET CS

Opérateur télécom, hébergeur et fournisseur de services managés certifié ISO27001 et HDS. Hexanet-Soluceo vous conseille et vous accompagne sur tous vos projets de modernisation et de sécurisation SI.

51100 Reims France

https://www.hexanet.fr

HIRMES

Hirmes est une entreprise qui œuvre pour la confiance numérique. Nous proposons des services de conseil et d'audit dans le domaine de la sécurisation des systèmes d'information.

63122 Ceyrat France

https://www.hirmes.fr

HIUMA

Nous Sécurisons votre système d'information Partenaire cybersécurité de grands comptes depuis 2011, nous nous positionnons en experts sur la cybersécurité, les réseaux, le cloud et les infrastructures.

69330 Meyzieu France

https://www.hiuma.fr

HOLISEUM CL H

Holiseum vous aide à mieux appréhender vos risques cyber en adoptant une approche globale, dite holistique. Nous pouvons ainsi intervenir sur l'ensemble de la chaîne de valeur cybersécurité.

92088 Paris-La Défense

https://www.holiseum.com

HUB ONE CL N

Hub One propose une offre globale de sécurité : Audit, Conseil, Formation, Cyber-entraînement, Intégration, Edition, SOC.

93290 Tremblay en France France

https://www.hubone.fr

I.S. MANAGEMENT

MA-SAUVEGARDE spécialisée dans la sauvegarde externalisée depuis plus de 10 ans, propose une solution fiable et robuste personnalisable en marque blanche. ISO27001 et HDS.

69360 Sérézin-du-Rhône France

https://ma-sauvegarde.com

IBC DIALOG

Ibc Dialog réalise des mises en place de réseaux et la sécurisation des postes. IBC propose aussi l'hébergement de données avec des prestations d'infogérance globale ou partielle.

14120 Mondeville France

https://www.ibc-dialog.fr

IDAXIO

Nous assurons la connectivité des données grâce aux meilleures solutions API, pour partager en toute sécurité vos informations avec vos clients, partenaires et fournisseurs.

78230 Le Pecq France

https://www.idaxio.com

IDENTO

Idento est le cabinet de conseil et d'intégration, leader de la gestion de l'identité et des accès (IAM, IAG, PAM, CIAM, DAG, Fédération, Authentification forte, MFA…).

92600 Asnieres sur Seine France

https://idento.fr

ID-LOGISM

Cabinet de conseil sécurité/protection données strat & perso. Analyse de risques ISO27005. Gouvernance sécurité ISO27001 PSSI RSSI CLOUD. Conformité RGPD DPO externe. IAM. Classification données. DLP.

75005 Paris France

http://www.id-logism.fr

IDNA C L

iDNA, conseil expert en Cybersécurité, Réseaux, Datacenter et Cloud, vous accompagne dans vos projets de sécurisation et de transformation IT. #Gouvernance #Expertise #Opérations #Expert-Cyber.

75003 Paris France

https://www.idna.fr

IMS NETWORKS N

IMS Networks aide les organisations à optimiser la performance et la sécurité de leurs infrastructures IT en leur proposant des services RÉSEAU & CYBERSÉCURITÉ certifiés ISO 27001.

81100 Castres France

http://www.imsnetworks.com

INDATABLE

Indatable est une société de conseil spécialisée dans l'accompagnement à la mise en conformité numérique et réglementaire. Nous proposons des prestations de sécurité informatique, RGPD et SAPIN II.

13014 Marseille France

https://indatable.com

INET SYSTEM N

Spécialiste de la sécurité sur les plates-formes Apple (postes de travail et terminaux mobiles).

92310 Sèvres France

http://www.inet-system.com

INETUM N

Inetum est une ESN agile, une société de services et de solutions digitales, et un groupe international qui aide les entreprises et institutions à tirer le meilleur du digital flow.

93400 Saint Ouen France

https://www.inetum.com

INFOCLIP N

Le Groupe Infoclip propose d'accompagner ses entreprises clientes dans l'exécution de leurs projets de transformation digitale. Infoclip met en place et infogère les systèmes de sécurité.

75002 PARIS France

http://www.infoclip.com

INFORSUD TECHNOLOGIES N

INFORSUD Technologies accompagne les entreprises/collectivités dans l'optimisation, la performance de leur système d'information et en assure la cybersécurité - audits/pentests/sensibilisation.

31500 Toulouse France

https://inforsud-technologies.com

INFOSYS N

Nous aidons à gouverner, à opérer, à surveiller, à détecter et à réagir aux attaques, avec une suite de cybersécurité evolutive, pour transformer, automatiser et orchestrer, On-Prem ou sur Cloud.

92914 Paris-La Défense Cedex 9 France

https://www.infosys.com/services/cyber-security.html

INOPS N

Société spécialisée dans la prestations intellectuelles d'experts du digital et conseil métiers.

75017 Paris France

http://www.inops.fr

INQUEST

INQUEST propose une offre complète de réponse à incident de cybersécurité ainsi qu'une offre d'audit (organisationnel et technique) et conseil SSI.

92800 Puteaux France

http://www.inquest-risk.com

INTEGRALE IP C L

ESN spécialisée en Infrastructure Réseau & Sécurité Informatique : audit, conseil, expertise technique, intégration de solutions LAN / WLAN / MAN / WAN / SDWAN.

93400 Saint-Ouen France

https://integraleip.fr

INTEGRASYS

Intégrateur.

20100 Casablanca Maroc

http://www.integrasys.ma

INTERDATA C S

Interdata a l'expérience et l'expertise certifiée pour vous apporter des services intégrés ou managés afin de sécuriser vos réseaux, vos applications et vos identités.

91940 Les Ulis France

https://interdata.fr

INTRINSEC N

Intrinsec propose un portfolio d'expertises & services en cybersécurité pour accompagner de la définition de la stratégie à la fourniture de services managés pour en maintenir le niveau.

92000 Nanterre France

http://www.intrinsec.com

ISATECH N

Notre offre consiste en l'identification des processus métiers critiques, l'audit, la cartographie des systèmes d'information et l'accompagnement dans la sécurisation des données d'entreprise.

56000 Vannes France

https://www.isatech.fr

ISE SYSTEMS H

Audits d'infrastructures, d'applications, du SMSI, de conformité (ISO 27001), analyse de risques. Mise en place SOC/SIEM, Veille CERT, PRA/PCA, PSSI. Gouvernance, contrôle de la conformité, risque.

92300 Levallois Perret France

http://ise-systems.fr

IT&M REGIONS N

Assistance dans le domaine de la cybersécurité : Antivirus / Firewall / Sauvegarde / Gestion poste de travail, RGPD/DPO (volet sécurité).

45000 Orléans France

http://www.it-m.fr

IT3 INFORMATIQUE

Audit de cybersécurité. Certification infrastructure. Tests d'intrusion. Infogérance. Accompagnement RGPD. Matériel. Logiciels.

67201 Eckbolsheim France

https://it3.fr

I-TRACING C S

I-TRACING est un leader français du conseil & de l'ingénierie en cybersécurité : audit, forensic, intégration, développements sécurisés, conformité, SOC, services managés, formation...

92800 Puteaux France

https://www.i-tracing.com/fr

ITS GROUP

ITS Group est une ESN qui accompagne les entreprises dans les domaines de la sécurité, aussi bien sur du conseil que dans l'intégration et l'infogérance de solutions.

92100 Boulogne Billancourt France

http://www.itsgroup.com

ITS INTEGRA C L

Nos activités sont l'automatisation, la sécurisation et les services managés autour des infrastructures Cloud privées, publiques ou hybrides. Certifiées ISO 27001, ISO 9001, HDS et Label ExpertCyber.

92100 Boulogne-Billancourt France

https://www.itsintegra.com

IVISION

Sensibilisation utilisateurs, outils de protection, audits de sécurité, PCA / PRA, décontamination, RGPD / DPO, sauvegarde hébergée, messagerie hébergée, infogérance, ingénierie…

92600 Asnières-sur-Seine France

https://www.ivision.fr

JANUA N

Consulting, implémentations, déploiement et support de solutions de gestion des identités open source (annuaires LDAP, SSO, Provisioning).

06650 Le Rouret France

http://www.janua.fr

JLLNET

Vous accompagner sur les domaines d'infrastructure (réseau/ système/ stockage/ virtualisation/ sécurité/ supervision) mais aussi sur le MCO, l'évolution de votre SI et sur vos projets métiers.

13127 Vitrolles France
https://www.jllnet.fr

K SECURITY

Audit de sécurité informatique, mise en place firewall infogéré, mise en conformité RGPD.

85500 Les Herbiers France
https://www.k-security.fr

KEYSIGHT

The value of connectivity, digital transformation, and security has never been so clear.

91940 LES ULIS France
https://www.keysight.com

KPMG

Maitriser les risques cyber en dialoguant avec toutes les fonctions, en intégrant les problématiques business/conformité/risques tout en s'appuyant sur des expertises techno et investissements majeurs.

92066 Paris-La Défense France
https://home.kpmg.com/fr/fr/home.html

KUDELSKI SECURITY CL

Fournisseur indépendant de solutions et services innovants de cybersécurité pour les entreprises privées et le secteur public : conseils, technologies, services managés, innovation personnalisée.

1033 Cheseaux sur Lausanne Suisse
https://kudelskisecurity.com

KYRON SI CL N

Kyron propose des solutions de cybersécurité IT/ OT en s'appuyant sur l'expertise reconnue de ses collaborateurs à travers de multiples certifications (ISA62443, CISSP, CCSP, CEH, ISO27001, ISO27005...).

31100 Toulouse France
http://www.kyron.fr

LECPAC CONSULTING

Nous sommes une société de conseil dans les domaines du cloud (Partenaire OVH) et en cybersécurité. Nous proposons des accompagnements sur la démarche ISO 27001 et des audits d'infrastructure cloud.

91170 Viry Chatillon France
https://lecpac-consulting.com

LEXFO

LEXFO est un cabinet indépendant d'expertises techniques en sécurité des SI. L'activité de LEXFO se décline en 5 offres de service : Audit de sécurité, Réponse à incidents, Surveillance des SI, R&D.

75009 Paris France
https://www.lexfo.fr

LISIS CONSEIL CL

Lisis Conseil est un cabinet de conseil indépendant spécialisé dans la gouvernance de la sécurité des systèmes d'information, la gestion des risques, la continuité des activités et la conformité.

78170 La Celle Saint Cloud France
http://www.lisis-conseil.com

LOGIFORM CONSEIL N

L'informatique, plus simplement : intégration d'ERP, CRM Mobile et logiciels de gestion pour PME ; Divalto ; Gestimum ; administration de réseaux et serveurs.

69300 Caluire et Cuire France
http://logiform-conseil.com

LOGIN SECURITE N CL

Login Sécurité accompagne les DSI dans la définition et la mise en œuvre de leur stratégie de Confiance Numérique en s'appuyant sur deux leviers : la Cybersécurité et le Réseau.

92210 Saint-Cloud France
https://www.login-securite.com

MANIKA N CL

MANIKA est un cabinet indépendant de conseil, d'audit et de formation spécialisé dans la protection et le renforcement du système d'information.

92200 Neuilly-sur-Seine France
https://www.manika-consulting.com

MASTER SECURITY CONSEIL

MASTER SECURITY CONSEIL société de spécialistes, à fort potentiel, travaillant sur de la sécurité, cybersécurité, RGPD, intelligence artificielle & machine learning,big data & science de la donnée.

92100 Boulogne France
http://www.mastersecurityconseil.fr

MATILAN

Matilan est une ESN spécialisée dans les services informatiques destinés aux PME, ETI et grands comptes. Notre expertise s'appuie sur des compétences en sécurité, services Cloud et infogérance.

75008 Paris France
https://www.matilan.com

MCA

Conseil et ingénierie et SI dont la Cyber

92300 Levallois Perret France
https://mca-groupe.com

MEDIANE SYSTEME N CL

R&D externalisée. Systèmes embarqués sécuritaires. Temps réel. Objets connectés. IIoT. LINUX Secure. OPC UA…

78230 Le Pecq France
https://medianesysteme.com

METANEXT N

Conseil en Gouvernance, Risque et Conformité, et en Conception et Intégration de solutions de sécurité des réseaux, sécurité périmétrique, firewalling, PRA/PCA, solutions SIEM et solutions Idaas.

92100 Boulogne-Billancourt France
http://www.metanext.com

METSYS N H

Acteur incontournable des services du numérique, Metsys vous offre un accompagnement sur mesure tout au long de vos projets de transformation numérique.

92100 Boulogne Billancourt France
https://www.metsys.fr

MHCONSEIL

Conseil, accompagnement et mise en service de solutions IT (matériels, logiciels, mise en production et assistances).

75017 Paris France
https://www.mhconseil.fr

MICROPOLE

Go Cloud & Security est la structure au sein du Groupe Micropole spécialisée dans le Conseil et l'assistance technique dans les domaines du Cloud Public et de la Cybersécurité.

92300 Levallois France
https://www.micropole.com

MIXCOM N

Diagnostic rapide de problèmes informatiques grâce à notre service innovant OptimIS d'analyse comportementale simultanée de l'ensemble des composants d'une architecture informatique complexe.

35760 Saint-Grégoire France
http://www.mixcom.fr

MODIS N

Modis, acteur mondial du conseil en ingénierie, services numériques et sciences de la vie, déploie une offre dédiée à la sécurité avec un focus réglementaire (RGPD).

92800 Puteaux France
http://www.modisfrance.fr

MPTCONSEIL

Je vous accompagne dans votre digitalisation de confiance.

37000 Tours France
http://www.mptconseil.fr

NAXIOS

Infogérance globale de PME. Conseil et Installation de pare-feu. Équipe de réponse aux incidents cybersécurité.

92100 Boulogne-Billancourt France
https://www.naxios.fr

NBS SYSTEM

NBS System est créateur et infogérant de l'offre Cerberhost, un système de très haute sécurité, disposant de plusieurs dizaines de couches de sécurité, disponible sur AWS et sur nos Clouds privés.

75017 Paris France
http://www.nbs-system.com

NDA-SECURITY

NDA-Security réunit EXPERTISES SSI indépendantes(FR)et SOLUTIONS LOGICIELLES européennes uniques sélectionnées pour répondre aux enjeux techniques, assurantiels, organisationnels et réglementaires.

91230 Montgeron France
https://www.nda-security.fr

NET FREED
N

Net Freed est un cabinet de conseil en cybersécurité. Nous accompagnons nos clients dans le choix et la mise en œuvre de réponses adaptées aux enjeux de leurs métiers, avec agilité et pragmatisme.

13340 Rognac France

http://www.netfreed.com

NETFORMATIC

Prestataire spécialisé dans les services informatiques destinés aux PME : conseil, sécurité, intégration, infogérance. Accompagnement RGPD, audit fonctionnel, analyse de risques. Labellisé ExpertCyber.

69340 Francheville France

https://www.netformatic.com

NEWLODE

Newlode est un fédérateur de sociétés de service expertes sur les grandes thématiques qui composent les Systèmes d'Informations actuels : Sécurité, Cloud, Big Data, Virtualisation, Containerisation.

92038 La Défense France

http://www.newlode.io

NOMIOS

Nomios agit pour la sécurisation des réseaux informatiques d'entreprise par sa présence constante auprès des entreprises clientes.

92100 Boulogne-Billancourt France

https://www.nomios.fr

NOVENCI

Nous préconisons et mettons en place des solutions pour renforcer la sécurité informatique des entreprises et contrer les cyberattaques (rançongiciel ou ransomware).

1340 L'Îsle d'Espagnac France

https://www.novenci.fr

NOVIDY'S

Intégrateur Sécurité & Réseaux, Novidy's offre à ses clients des solutions, prestations et services basés sur l'écoute, la personnalisation et l'excellence technique.

78140 Vélizy Villacoublay France

https://www.novidys.com

NTT FRANCE
C L

Leader mondial des services technologiques. NTT Ltd aider les entreprises à mieux performer grâce à des solutions technologiques intelligentes - orientées données, connectées, numériques et sécurisées.

94618 Runfis France

https://hello.global.ntt

NXO FRANCE
C L N

Leader indépendant de l'intégration pour les entreprises et les administrations, NXO conçoit, déploie et exploite des solutions de Communication & Collaboration, Infrastructures digitales et Sécurité.

92500 Rueil Malmaison France

https://www.nxo.eu

OFISS

Nous sommes consultés pour auditer et préconiser des solutions cyber.

75008 Paris France

OÏKIALOG

Conseil, intégration et maintient en condition opérationnelle de solutions de sécurité des systèmes d'information, avec une très forte expertise sur les SIEM.

92300 Levallois-Perret France

http://www.oikialog.com

OKTA

Plus de 13 000 clients nous font confiance pour sécuriser leurs interactions numériques et accélérer l'innovation.

75008 PARIS France

https://www.okta.com/fr

ONPOINT AFRICA GROUP

Conseil en strategie.

28230 EPERNON France

https://www.onpointafrica.net

ON-X
C L N H

ON-X, cabinet français indépendant de conseil et d'expertise, spécialisé en CyberSécurité : gouvernance, Risques et Conformité ; SecOps et Managed Detection & Response ; audits de sécurité PASSI.

92800 Puteaux France

https://www.on-x.com

OPEN GROUPE
C L N

Éditeur de solutions digitales en mode SaaS.

92300 Levallois-Perret France

http://open.global

OPENMINDED PART OF ACCENTURE
N

Pure player français en cybersécurité, nous réalisons des prestations de conseil, de vente et d'intégration de solutions, d'audit, de contrôle et de mise à l'épreuve de la sécurité du SI.

75009 Paris France

http://www.opmd.fr

OPENSPHERE
N

Cabinet de conseil international crée en 2005. OpenSphere est l'expert indépendant en cyber sécurité des DOM-TOM : Conseil, Audit de sécurité, Forensic, RSSI délégué, SOC, ISO 2700x et Formation.

97490 Sainte-Clotilde La Réunion

https://www.opensphere.fr

OPTRIUM

Créée en 2004, la société Optrium est Distributeur-Conseil-Intégrateur de solutions logicielles axées sur Gouvernance des SI (Systèmes/Données/Utilisateurs).

92000 Nanterre France

http://www.optrium.fr

OPTYMA SARL

Conseillers à la protection des données, on-demand CSO, GAP analysis, Finma, CH LPD, GDPR.

1204 Genève Suisse

https://www.optyma.ch

ORANGE CYBERDEFENSE
C L N

Fort de son expérience d'opérateur télécoms, Orange Cyberdefense propose une approche complète de la sécurisation des actifs numériques : audit, pilotage quotidien de la sécurité, gestion de crise.

92983 Paris-La Défense France

https://www.cyberdefense.orange.com

OROL SOLUTIONS
C L

Entreprise française, spécialisée dans la transformation numérique et la cybersécurité offensive et défensive, OROL Solutions vous accompagne dans la sécurisation de votre S.I et sa conformité.

18000 Bourges France

https://www.orol.solutions

OSINX - GROUPE ACTIMAC

osinx est un ESN qui propose des solutions et des services spécialisés dans la cybersécurité pour les PME, ETI et collectivités : sensibilisation, audit, mise en conformité, protection et remédiation.

14200 Hérouville Saint Clait France

https://osinx.fr

PA CONSEIL

Accompagnement des dirigeants d'entreprises.

7320 ST AGREVE France

http://www.armandtourisme.fr

PCL ASSISTANCE INFORMATIQUE

Créée depuis 1994 dans les Alpes Maritimes, PCL Assistance Informatique s'est développée à partir d'une idée simple. Apporter une qualité de service adaptée aux nouvelles exigences des PME-PMI.

06800 Cagnes sur Mer France

https://www.pcl-assistance.com

PHŒBE
N

PHŒBE propose un "Pré-Diagnostic", une rapide analyse de risque déclinée à partir de la méthode EBIOS et dont le résultat est un rapport commenté abordant objectivement vos risques Cyber.

83200 La Valette du Var France

https://www.phoebe.fr

PICTIME GROUPE
N

PICTIME GROUPE propose des services managés de sécurité pour les acteurs du retail, sous la marque PICTIME, et les acteurs de la santé sous la marque COREYE.

59262 Sainghin-en-Mélantois France

https://www.pictime-groupe.com

PINSENT MASONS FRANCE LLP

Cabinet d'avocat disposant d'une expertise en droit des nouvelles technologies et tout particulièrement sur les questions de cybersécurité et de réglementation applicables aux données.

75008 Paris France

http://www.pinsentmasons.com

POST LUXEMBOURG

POST Luxembourg propose des forfaits mobiles, abonnements Internet, télé, services postaux et financiers pour les particuliers.

L-2417 Luxembourg Luxembourg

https://www.post.lu

PPP-CONSEIL

Consultant sécurité. Architecte réseau. Conduite de projets. Étudier la fiabilité de votre système d'information (certifier ISO 27001 27005). Audit de lignes industrielles (certification Sentryo).

56370 Le Tour du Parc France

http://www.ppp-conseil.fr

PRIAMOS

Le cabinet Priamos accompagne ses clients en proposant 4 offres différentes : Conseil, Audit et Formation en interventions courtes, et son offre Ingenierie pour un renfort au quotidien.

Toulouse 31000 France

https://www.priamos.fr

PRIVACY IMPACT

Privacy Impact - audit conseil formation - intègre les enjeux techniques et juridiques pour proposer des solutions concrètes et efficaces dans la protection des données et le respect de la vie privée.

75017 Paris France

http://www.privacyimpact.fr

PROBE I.T

Conseil en gouvernance, analyse de risque, architecture sécurisée, pentesting. Assistance MOA, pilotage de projet. Audit, conformité. Impact GDPR/RGPD.

30900 Nîmes France

PROCESS-IT

Process-IT est une ESN à taille humaine qui est spécialisée dans le service sécurité informatique. Nos offres de service disponibles « SOC - Cyberdéfense » - « Sécurité opérationnelles » - « Intégration ».

13100 Aix-En-Provence France

https://www.process-it.fr

PRODWARE

Une expertise au service des clients

Créé en 1989, Prodware est un Groupe international spécialisé dans l'édition-intégration et l'hébergement de solutions de gestion pour les entreprises.

75019 Paris France

https://www.prodware.fr

PRODWARE BIS

CS EC

Conseil, intégrateur, hébergeur, éditeur et mainteneur de solutions informatiques, Prodware procure un large catalogue de solutions et de services de Cybersécurité auprès des PME et ETI.

75019 Paris France

https://www.prodwaregroup.com

QUIETIC

N

L'entreprise est spécialisée en services managés et cybersécurité, avec des solutions et méthodes pour lutter contre les risques, et intervention en cas d'attaques, sinistres ou erreurs humaines.

44300 Nantes France

https://www.quietic.fr

QUODAGIS

N

Experts des services aux infrastructures, QUODAGIS vous accompagne dans votre transformation digitale dans le respect des bonnes pratiques et des contraintes de sécurité (modes projet, AT, MSP).

75008 PARIS France

http://www.quodagis.fr

QUODAGIS INTEGRATION

N

QUODAGIS Integration est intégrateur spécialisé dans les solutions ITSM, ITAM et ITOA. Nous accompagnons les DSI de moyennes et grandes entreprises dans le choix des outils et leur mise en œuvre.

75008 Paris France

https://integration.quodagis.fr

QUONEX

Partout où l'Information et la Communication sont des enjeux décisifs, Quonex déploie avec précision et engagement toute son expertise.

93300 Aubervilliers France

http://www.quonex.fr

RAMPAR

Rampar se positionne comme un acteur majeur français sur les métiers de l'intégration, du Cloud et des services managés dans les domaines de la cybersécurité et des infrastructures.

92310 Sèvres France

https://www.rampar.com

REALSOFT INFORMATIQUE

Société de Service lié aux developpements de solutions spécifiques (du cahier des charges à la mise en place formation du personnel), specialiste réseaux, solutions de location serveurs.

06250 Mougins France

http://www.realsoft.fr

RECOVEO

Recoveo Forensics comprend 2 catégories :
Vente d'outils et logiciels de forensics ; Service de récupération de données sur téléphone, disque dur et tous autres supports numériques.

42300 Roanne France

http://recoveoforensics.com

RHSOLUTION

Consultant Linux/Cybersécurité.

69005 Lyon France

https://www.linkedin.com/in/laurent-jouannic-a7933337/

RISK&CO

Notre groupe déploie une offre globale de sécurisation des systèmes informatiques complexes et industriels.

92300 Levallois Perret France

https://www.riskeco.com

RLG INFORMATIQUE

N

Sécurisation des comptes utilisateurs et comptes Office 365. Sécurisation des PC et serveurs. Mise en place de coffre-forts de mots de passe. Sensibilisation des utilisateurs à la sécurité.

44100 Nantes France

https://www.rlginformatique.com

SASETY

SASETY conseille, déploie, surveille et opère des solutions de transport sécurisé, de protection des infrastructures et des terminaux et de validation continue de la cyberdéfense des organisations.

92100 Boulogne Billancourt France

https://www.sasety.com

SAVANE CONSULTING

N

Savane-Consulting intervient de l'étude de faisabilité au délivery sur les problématiques de : Sécurité des systèmes et infrastructures informatiques ; Gouvernance sécurité du SI ; Cybersécurité.

75008 Paris France

http://www.savane-consulting.com/

SCASSI

N CL

SCASSI, ingéniérie - conseil en cybersécurité des SI Métiers et Systèmes Critiques est basée en France et en Espagne. L'offre se compléte par le e-learning de Phosforea et les produits June-Factory.

31670 Labège France

https://www.scassi.com

SCC FRANCE

CL N

SCC accompagne ses clients dans leur transformation IT(conseil, intégration, maintenance, financement). Nos offres : Réseau et Sécurité, Workspace, Software Asset Management, Infogérance et Maintenance.

92000 Nanterre France

http://france.scc.com/

SCHNEIDER ELECTRIC

CL

Prestataire d'intégration et de maintenance spécialisé en Cyber industrielle. Conforme au référentiel d'exigences PIMSEC de l'ANSSI. Intégrateur certifié Stormshield, Wallix, Sentryo. Formateur Cyber agréé.

69792 Saint-Priest France

http://www.schneider-electric.com

SCIURUS CONSEIL

CL

SCIURUS Conseil est un cabinet de conseil français spécialisé en Cyber Sécurité.

34770 Gigean France

http://www.sciurusconseil.com

SEC-IT SOLUTIONS

Audit organisationnel et technique, tests d'intrusion, conseil, sécurité opérationnelle, formation - SEC-IT est qualifiée PASSI et accréditée CIR - Agences : Aix, Lyon, Rennes.

13290 Aix-en-Provence France

https://www.sec-it-solutions.fr

SECTOR

Accompagnement dans la mise en place de process en conformité avec les normes sectoriels.

38230 Tignieu France

http://www.sectorgroup.net

SECUREWARE

C S

SecureWare est composée d'ingénieurs expérimentés, pluri-compétences capables d'accompagner nos clients dans toutes les phases d'un projet. Intégration, Conseils, Formation. Missions à l'étranger.

21600 Fenay France

https://www.secureware.fr

SECUREWORKS

SecureWorks propose des services de gestion et de surveillance sécurité (SOC), threat intelligence, réponse aux incidents au travers d'une plateforme propriétaire (CTP) ainsi que du conseil.

95870 Bezon France

SECURIVIEW SAS

Securiview offre des services SOC - Log Management- Détection d'intrusion-Réponses à incidents - Vulnerability Management - Forensic - Tests d'intrusion.

93400 Saint-Ouen France

http://www.securiview.net

SERMA SAFETY & SECURITY

SERMA Safety & Security est un interlocuteur unique pour la sécurité et la sureté de fonctionnement des systèmes d'information, embarqués et industriels.

75008 Paris France

https://www.serma-safety-security.com

SERVAL-CONCEPT

La société Serval-Concept est spécialisée dans les tests d'intrusions ainsi que les audits des systèmes d'information (architectures systèmes et réseaux, application, systèmes industriels, etc).

59250 Halluin France

http://serval-concept.com

SFR BUSINESS

N

Opérateur/Intégrateur de solutions et services en cybersécurité pour grands comptes, ETI & PME : conseil, audit, Pentest, Scan Vuln / protection sur mesure & packagées / exploit, services managés, SOC.

75015 Paris France

http://www.sfrbusiness.fr

SII

C L N

Assistance aux entreprisex en mode régie ou forfait.

75016 Paris France

http://www.groupe-sii.com

SILICOM

N

Silicom propose un accompagnement de ses clients dans l'architecture et l'intégration de produits Cyber. Innover, Silicom se charge de sécuriser vos infrastructures, vos applications et vos produits.

78280 Guyancourt France

http://www.silicom.fr

SMARTPOINT

Dans un monde en constant changement, en embrassant constamment la nouveauté, Smartpoint se positionne en tant que conseiller sur la protection de vos technologies, vos données, et vos collaborateurs.

75013 Paris France

http://www.smartpoint.fr

SNS SECURITY

SNS SECURITY est une société de services indépendante, spécialisée dans la sécurité informatique défensive et offensive (pentest). Expert partner FORTINET, Gold SENTINELONE et partenaire SEKOIA.IO.

34070 Montpellier France

https://www.sns-security.fr

SOCOA SÀRL

Gérez votre entreprise, nous gérons votre (cyber) sécurité !

1025 Saint Sulpice Suisse

http://www.socoa.ch

SODIFRANCE

N

Offre de conseil et d'intégration en Cybersécurité incluant un SOC, une activité d'infogérance et de formation. Réalisation d'audits (Pentest, Bug Bounty…). Expertise certifiée ISO 27001 et PASSI.

44000 Nantes France

http://www.sodifrance.fr

SO-IT

Intégrateur Cybersécurité. Solution de sécurité : Palo Alto Firewall et Endpoint (Cortex), SIEM LogPoint, Forescout (NAC et 802.1x), Vade (AntiSpam). Service : Managed Detection And Response.

31100 Toulouse France

https://www.so-it.fr

SOLUCEO DGPF

Partenaire intégrateur national reconnu pour notre expertise et nos réalisations. Focus sur les projets de transformation et de modernisation des Réseaux et de la Sécurité.

38170 Seyssinet-Pariset France

https://www.soluceo.fr

SOPRA STERIA

N C L

Acteur majeur de la cybersécurité, reconnu par l'ANSSI, Sopra Steria s'appuie sur 750 experts en Europe et propose une offre globale de services (GRC, sécurité applicative et du Cloud, SOC).

92360 Meudon la Forêt France

https://www.soprasteria.com/fr

SOSATOUTPC

L'ingénierie des systèmes : audit de l'existant ; étude de l'architecture des systèmes ; analyse des besoins réels et des pôles d'évolution ; préconisation des matériels et des logiciels.

22160 Callac France

http://www.sosatoutpc.com

SPIE ICS

N C L

Au travers de son centre d'expertise dédié et de son partenariat avec Airbus Cybersécurity, SPIE ICS délivre un accompagnement global sur l'ensemble sujets de Cybersécurité

92240 Malakoff France

http://www.spie-ics.com

SQUAD

C L

Protéger le patrimoine informationnel. Surveiller le cycle de vie de l'information dans et en dehors de l'entreprise. Réagir à un incident de sécurité sur les plans technique et légal.

75001 Paris France

https://www.squad.fr

STEEL PC

Un besoin de maintenance, de matériel, d'hébergement ou de solutions de sauvegarde? L'expérience acquise par Steel PC vous assure expertise, performance et réactivé dans vos projets IT !

57140 Norroy-le-Veneur France

https://steel-pc.fr

STRATEGY & GOVERNANCE

Strategy & Governance offre des services autour de la cyber sécurité depuis plus de 10 ans, nous intégrons la sécurité dans les organisations en vue de les aider à préserver leur patrimoine.

41170 Baillou France

http://www.strategy-and-governance.eu

SYNACKTIV

Synacktiv est une société d'expertise en sécurité des systèmes d'information fondée en 2012 par des consultants ayant plus de 12 ans d'expérience dans le conseil et l'audit de systèmes informatiques.

75015 Paris France

http://www.synacktiv.com

SYNCHRONE

N C L

Synchrone certifié ISO27001 dispose d'une communauté d'expertise constituée de plus de 160 consultants susceptibles d'intervenir sur l'ensemble du territoire national.

75002 Paris France

http://www.synchrone.fr

SYNETIS

N C L H

Synetis, leader français des cabinets de conseil spécialisés en Sécurité des Systèmes d'Information, propose une démarche complète à ses clients : conseil, intégration et opération des solutions.

75008 Paris France

https://www.synetis.com

SYNEXIE

Synexie expert en cybersécurité accompagne ses clients dans l'évolution et le maintien en condition opérationnelle des infrastructures systèmes et réseaux sécurisés.

83000 Toulon France

https://www.synexie.fr

SYSDREAM

C L

Sysdream division Cybersécurité de Hub One propose une gamme de solutions axées sur l'audit, la formation et le cyber-entrainement.

92300 Levallois-Perret France

https://www.sysdream.com

SYSTEMIS N

Maîtrisez en toute autonomie vos risques cyber grâce aux talents de SYSTEMIS et aux solutions de cybersécurité souveraines françaises (Gouvernance, Audit, Identité, Intrusion, DevSecOps, Formation).

94270 Le Kremlin-Bicêtre France
https://www.systemis.eu

TALC SI

Talc SI est une société de service spécialisée dans la gestion, l'optimisation et la sécurisation des systèmes d'information (serveur, stockage, sauvegarde/restauration, virtualisation,cybersécurité).

95130 Franconville France
https://www.talcsi.com

TECODATA

Créée en 2003, nous sommes spécialisés dans le déploiement de matériel ainsi que dans la mise à disposition de ressources techniques (de Technicien Itinérant à Consultant Big Data & Cybersécurité).

79270 Frontenay Rohan Rohan France
http://www.tecodata.fr

TEOS CYBERSECURITY

Gouvernance (RSSI de transition / à temps partiel, sous-traitance RSSI, politiques SSI, analyses de risques…). Audit & conformité (TI, audits, conformité RGPD). Sécurité IoT & industrielle.

17000 La Rochelle France
http://www.teos-cybersecurity.com

TGS FRANCE INFORMATIQUE

Une offre complète de solutions et de conseils : logiciels de gestion, ERP, Paie & RH, BI & DATA, infrastructure, maintenance, infogérance, conseil en systèmes d'information et en cybersécurité.

49070 Beaucouze France
https://www.tgs-france.fr

TIBCO

Chez Tibco, nous mettons l'humain au cœur de la sécurité de l'information: Des hommes, des process, des outils et de la gouvernance pour vous aider à agir au plus près des métiers et des utilisateurs.

44860 Saint-Aignan de Grand Lieu France
http://www.tibco.fr

TNP CONSULTANTS N C L

Stratégie & Gouvernance SSI, Protection des données, Audit de sécurité, Tests d'intrusion Analyses de risque, Privacy & Security by design, Certification Privacy & Security, Forensics, SOC, Formation.

92200 Neuilly-sur-Seine France
https://www.tnpconsultants.com/fr

TRAX N C L

Trax est une agence de conformité digitale, qui accompagne les entreprises à la certification ISO 27001 (sécurité des systèmes d'information), via des prestations d'audit, de formation et de conseil.

92300 Levallois-Perret France
http://www.trax.solutions

TRÈFLE SOLUTION

Nous sommes spécialisés dans la protection de l'information et la sécurité des systèmes d'information. Nous intervenons sur des problématiques en cybersécurité de type technique et organisationnel.

92100 Boulogne-Billancourt France
http://www.groupetrefle.com/solution

TRSB N

L'offre TRSb s'articule autour de quatre expertises métiers : le conseil, la stratégie & l'innovation, le développement & l'intégration de solutions, les services managés et l'expérience utilisateurs.

75008 Paris France
http://www.trsb.net

T-SYSTEMS N

T-Systems propose les compétences des 1 400 experts de sa Division Magenta Security, des opérations de solutions périmétriques et SIEM/SOC au Consulting sur le protection et les réponses.

92500 Rueil-Malmaison France
http://www.t-systems.com

UBCOM SA

Préparer et organiser nos clients à la cybersécurité avec une gouvernance, des outils, du comportement, du juridique, de l'innovation et de l'intelligence. Analyse du risque cyber.

1920 Martigny Suisse
http://www.ubcom.ch

UBG. CYBER

UBG. Cyber est un cabinet indépendant spécialisé dans l'audit, le conseil et la formation en Cyber Threat Intelligence, Cyber-défense, cybersécurité et cybercriminalité.

69002 Lyon France
https://cyber.ubg-interactive.com

UNUMKEY

Labellisée France Cybersecurity, UnumKey propose des prestations de conseil, d'audit et de formation à destination des entreprises privées et publiques.

51100 Reims France
https://www.unumkey.fr

UPPER LINK

Upper-Link, ESN (ex SSII) Paris accompagne les entreprises dans leurs projets IT. Infogérance - Solution Cloud - Programmation - Microsoft Gold Partner.

77185 Lognes France
https://www.upper-link.com/

UPSAIL

Nous accompagnons les entreprises dans la définition, la mise en oeuvre, le suivi et la sécurisation de leurs systèmes d'information reposant sur l'usage des meilleurs technologies au monde.

10000 Kinshasa République démocratique du Congo
http://www.upsail.co

URAEUS CONSULT N

Spécialisée en Cybersécurité : Audit de SI, Évaluation du risque, Accompagnement à la certification ISO27001, Conformité RGPD et ISO27002. Risk Managers certifiés ISO27005 LSTI Grade.

06560 Sophia-Antopolis France
http://www.uraeus.fr

UTIKXO

UTIKXO est un cabinet de conseil en organisation et processus spécialisé dans la sécurité de l'information, cybersécurité, intelligence économique, protection des données et de la vie privée.

75017 Paris France
https://www.utikxo.com

VAADATA

Vaadata est une entreprise spécialisée en tests d'intrusion. 3 types d'audits: black box, grey box, ingénierie sociale. Périmètre des tests: plateformes web/mobile, objets connectés, facteur humain.

69009 Lyon France
https://www.vaadata.com

VEYAN N

VEYAN est une société de conseil, organisationnel et politique, en cybersécurité. Notre gamme d'accompagnement porte sur la gouvernance de la sécurité de l'information et sur la conformité au RGPD.

56520 Guidel France
https://www.veyan.fr

VNEXT

vNext est une société de conseil. Nous intervenons dans trois domaines d'activités : Business Consulting, IT Consulting et Managed Services.

75014 Paris France
http://www.vnext-group.com

WALLACK

Wallack intervient comme Responsable de la Cybersécurité de ses clients. De la construction d'une feuille de route jusqu'à la conformité terrain, nous intégrons la cybersécurité à votre organisation.

35135 Chantepie France
https://www.wallack.fr

WANCORE

Nous délivrons notre expertise en ingénierie Réseaux (architectures LAN/WAN) et CyberSécurité selon 3 modes d'intervention : Conseil, Intégration et MCO N3. Clientèle CAC 40 à ce jour.

75008 Paris France
http://www.wancore.fr

WANNATH

WANNATH est un cabinet de conseil spécialisé dans l'efficience des Systèmes d'Information et plus particulièrement dans le domaine de la cybersécurité : Conseil, audit et accompagnement.

75008 Paris France
https://www.wannath.com

WAPLI INFORMATIQUE

Accompagnement des PME pour l'ensemble de leurs besoins informatiques/numériques : audit, conseil, intégration, réseaux, infogérance, sauvegardes et cybersécurité. Certifié ZyXEL Security Specialist.

82000 Montauban France
https://www.wapli-informatique.fr

WAPSI

Accompagnement de clients dans le choix de solutions outillées et de solutions à la régie et au contrat d'assistance, sur les éléments vecteurs de failles de sécurité (utilisateur, application, Cloud).

75008 Paris France

https://www.aerow.group

WAVESTONE

N C L

Wavestone est le leader du conseil en cybersécurité et confiance numérique en France avec plus de 500 consultants dédiés et la capacité à adresser des grands projets internationaux.

92042 Paris-La Défense Cedex France

http://www.wavestone.com

WEODEO

Notre approche est ou peut être globale au regard du parcours du dirigeant. notre offre est donc sur mesure… en fonction de votre contexte, de vos besoins.

75013 Paris France

http://www.weodeo.com

WISE PARTNERS

WISE Partners est un Cabinet de conseil indépendant, spécialisé en cyber-sécurité et confiance numérique.

75116 Paris France

http://www.wise-partners.fr

XEFI

N C S

XEFI - Leader des services informatiques auprès des TPE / PME.

63170 Aubière France

http://www.xefi.fr

XMCO

C L

XMCO est un cabinet de conseil spécialisé en cybersécurité (audit techniques/tests d'intrusion, certifications PCI DSS, cybersurveillance/veille vulnérabilité/analyses inforensiques).

75002 Paris France

http://www.xmco.fr

XPERIZ

Analyse de risques (EBIOS, ISO 27005). Posture permanente de sécurité : intégration de la sécurité dans les projets, et comportements. Pilotage des plans d'actions issus des audits. Gestion de crise.

75004 Paris France

http://www.stratops.fr

YEC'HED MAT CONSEIL

Yec'Hed Mat est un cabinet de conseil et de formation dans la mise en conformité avec le RGPD et appliqué spécifiquement à la santé auprès des cliniques, start-up, CRO et industrie pharmaceutique.

33800 Bordeaux France

https://yeched-mat.com

YOGOSHA SAS

N C L

Yogosha est une plateforme de Bug Bounty qui permet à ses clients de mettre en œuvre une recherche de vulnérabilités en rémunérant les chercheurs à la faille découverte.

92514 Boulogne Billancourt France

https://www.yogosha.com

YOURAX (GROUPE ACESI)

H

Fort d'une expertise depuis 25 ans, Yourax vous conseille et soutient vos projets informatiques pour sécuriser, optimiser et gérer votre système d'informations : Cybersécurité, Cloud, Infrastructure.

59223 RONCQ France

https://www.yourax.fr

ZENIKA

N

Zenika s'inscrit dans une démarche d'amélioration continue et de mise en place de la sécurité chez ses clients en leur apportant conseil et expertise dans les grands domaines.

75009 Paris France

http://www.zenika.com

ZERO TRUST SAS

Spécialiste des environnements Cloud, pure player sur le conseil en sécurité Cloud 2.0, avec une réelle indépendance. Conseil de solution et intégration, Conseil et audit, SOC de nouvelle génération

93200 Saint Denis France

https://zerotrust.fr

ENTREPRISES SPÉCIALISÉES, RÉFÉRENCEZ-VOUS SUR L'ANNUAIRE EN LIGNE

**Les informations de ce guide sont issues de l'annuaire en ligne.
Les sociétés spécialisées en cybersécurité doivent se référencer
et mettre à jour régulièrement leur fiche.**

***Attention, l'annuaire est réservé aux entreprises réellement spécialisées en cybersécurité.
La rédaction valide la création des fiches.***

Inscription et mise à jour :

https://www.solutionsnumeriques.com/securite/ annuaire-cybersecurite/

E C Label ExpertCyber
C L CLUSIF
C S CESIN
N Adhérents Numeum
H Adhérents Hexatrust

Consultants (1 à 5 personnes)

ADVISECURITY

Gouvernance, organisation cybersécurité ; Identity et Access Management ; Data Protection et management ; Security Analytics.

75017 PARIS France

https://www.advisecurity.com

AGENCE RGPD N

L'Agences RGPD met et maintient toutes les entreprises, collectivités et associations dans leur mise en conformité avec le Règlement Général de la Protection des Données (RGPD).

86000 POITIERS France

https://www.agencergpd.eu

BLASCOM IT E C

Expertise en Reseaux et Cybersecurité.

69002 LYON France

http://www.blascom.com

CYBERWORKS

Conseil et audit autour des normes ISO 27001/27701/HDS et des référentiels de l'ANSSI : PASSI, SecNumCloud, PDIS, PRIS, PAMS.

44100 Nantes France

https://www.cyberworks.fr

FEUILLE À FEUILLE

Conseil pour audit cybersécurité sur la base des techniques de hacking (White) Cible ETI-PME.

46090 BELLEFONT LA RAUZE France

http://www.feuilleafeuille.fr

INTUITEM C L

Après avoir développé Agile Security Framework pour aider les entreprises à concilier agilité et cybersécurité, intuitem lance Mira, la solution d'analyse de risques la plus simple du marché !

92360 Meudon France

https://intuitem.com

LE NET EXPERT

Expert informatique formé par la CNIL- Spécialisé en Cybercriminalité et en Protection des Données personnelles- Audits / Accompagnements / Formations / Forensic.

84300 CAVAILLON France

https://www.lenetexpert.fr

LEXAURA C L

Lexaura est un cabinet de conseil spécialisé dans la gestion, la transformation et la sécurisation des SI (Systèmes d'Information) des entreprises de taille moyenne (PME)

75008 Paris France

https://www.lexaura.com

LOIC CAROLI SAS C L

Nous accompagnons les RSSI dans la définition de leur roadmap de cybersécurité annuelle et la mise en œuvre de cette roadmap en mode agile.

84110 VAISON LA ROMAINE France

https://www.linkedin.com/company/loiccaroli/

MEDERI C S

Cartographie, audits infrastructure et sécurité, déploiement solutions sécurité (FW, NBH, SOC...), PCA et PRA, élaboration de SDI et scénarii évolution du SI, pilotage projets et conduite changement.

60100 Creil France

http://mederi-consulting.fr

MINE

Apport de l'IA à la Sécurité Informatique

75014 Paris France

https://www.linkedin.com/in/philippe-mercier-69647a9

PRONETIS C S

Conseil, Audit et Formation en Cyber Sécurité : audits, tests instrusifs, forensique ; sécurisation du S.I., plan de secours informatique ; formation et sensibilisation ; RSSI et DPO externalisés.

84120 PERTUIS France

https://www.pronetis.fr

RESILIENT SHIELD CONSULTING

Conseil et formation resilience, continuité, risques et crises.

75008 Paris France

https://www.resilient-shield.com

SYC CONSULTANTS

Audit informatique, gouvernance informatique, assistance MOA projet ERP GED BI, commissaire aux comptes et expert comptable.

75017 Paris France

https://www.sycconsultants.fr

TANCO & CO

Agence technologique consulting sureté & sécurité informatique - Expert cybersécurité - esign & intégration de solutions sur mesure - Alarme, contrôle d'accès & vidéoprotection - Éditeur de logiciel.

06250 MOUGINS France

https://www.tanco.fr

TC CONSEIL C L

Conseil au forfait, Coaching, Part Time Cisco. Exemples de travaux : évaluer (audit flash, risque) ; se conformer (ISO, RGPD) ; gouverner (PSSI, dashboards) ;- se renforcer (SOC, continuité).

92170 Vanves France

https://www.linkedin.com/company/tchiofalo-conseil

WILLIAM BOURGEOIS CONSULTING

Diagnostic de maturité SSI Auditeur ISO27001, 27701, HDS et RGPD. Accompagnement à la mise en œuvre ou le suivi de SMSI/PIMS. Analyse de risques (ISO27005, EBIOS2010) Sensibilisation.

69380 CHESSY France

https://kyneo.fr

Formation

2600

L'École 2600 est un organisme de formation spécialisé dans la cybersécurité; notre but est de remédier à la pénurie d'experts opérationnels en cybersécurité. Nous recrutons à Bac+3 pour 3 ans d'études.

78180 Montigny le Bretonneux France

https://ecole2600.com

4CYSEC

4CYSEC vous accompagne dans vos projets liés à Cybersécurité et à la protection des données : FORMATION - AUDIT - FORENSIC - COMPLIANCE (RISK MANAGEMENT, ISO, EBIOS, PENTEST, ISO2700x, GDPR, DPO...).

75012 Paris France

https://4cysec.io

AASTERIA

Face aux menaces de vol de données en entreprise Aasteria forme vos salariés à identifier les risques et postures à adopter. Dotez vous des capacités de confiance indispensables à votre développement.

92400 Paris-La Défense France

http://aasteria.com

APPSECFR

Formation en Sécurité des Applications. Nous formons dans les cadres réglementaires PCI-DSS chapitre 6. Ainsi qu'autour des référentiels de type OWASP.

79000 Niort France

https://www.appsec.fr

BLUECYFORCE

Premier centre d'entraînement opérationnel à la cyberdéfense en France, BLUECYFORCE propose des parcours immersifs, individuels ou collectifs, afin d'intensifier l'apprentissage « par la pratique ».

75015 Paris France

https://www.bluecyforce.com

CLÉON CONSEIL

Conseil et formation : RGPD sensibilisation, formation des DPO/DPD, CODIR ; assistance à maitrise d'ouvrage DSI ; conseil DSI ; diagnostic numérique EHPAD.

31700 Cornebarrieu France

http://www.cleon.cc

CONSCIO TECHNOLOGIES

N C L

Conscio Technologies est le spécialiste des solutions de sensibilisation des utilisateurs. Son offre est constitué de contenus de sensibilisation et des solutions logicielles de gestion de campagnes.

75002 Paris France

http://www.conscio-technologies.com

DMR

N

DMR (Développement Multimédia et Réseaux), centre de formation, forme au niveau régional, national et international les RSSI, DPO, Experts Cyber sécurité, Analyste SOC, Architectes sécurité, Administrateurs et Développeurs, etc.

13170 Les Pennes-Mirabeau France

http://www.dmr-formation.fr

ÉCOLE DE GUERRE ÉCONOMIQUE

L'École de guerre économique (EGE) propose des formations en intelligence économique, cyber et sûreté. Elle est l'organisme certifiant pour l'obtention du Titre « Expert(e) en intelligence économique ».

75007 Paris France

http://www.ege.fr

ÉCOLE EUROPÉENNE DE CYBERSÉCURITÉ (EECS) DE VERSAILLES

L'EECS forme des techniciens systèmes et réseaux et des opérateur en cybersécurité à qui elle délivre le titre RNCP 34975. Ses étudiants proposent leurs compétences en alternance pour 2 ans.

78000 Versailles France

EDUGROUPE

C L

EduGroupe accompagne les entreprises dans leurs projets de formations liées à la Sécurité informatique, Cybersécurité, Management des risques, ISO, EBIOS, Développement sécurisé, Sécurité cloud, IOT.

75016 Paris France

https://www.edugroupe.com

EXPERNET

Expernet est un centre de formation Informatique, une école informatique et formation e-learning. Domaines : Bureautique, Système et Infrastructure réseaux, Infographie, Gestion de projet, CAO, PAO.

97420 Le PORT France

http://www.expernet.fr

GLOBAL KNOWLEDGE

Notre offre de formations et de certification couvre les solutions techniques éditeurs et les référentiels métiers de la cybersécurité (Normes ISO, CISSP, CRISC, CISM, CCSP, sans oublier le RGPD).

92500 Rueil-Malmaison France

https://www.globalknowledge.fr/securite

HS2

N C L

HS2 (Hervé Schauer Sécurité) propose un programme complet de formations inter-entreprises en cybersécurité technique et organisationelle, droit de la cybersécurité, protection des donnéesl (DPO/RGPD) et continuité d'activité.

92200 Neuilly-sur-Seine France

http://www.hs2.fr

HSC BY DELOITTE

Leader français de la formation en SSI, HSC by Deloitte propose le plus large programme du marché :cyber sécurité (pentest, ISO2700x), vie privée (GDPR, DPO) et continuité d'activité (RPCA, ISO22301).

92200 Neuilly-Sur-Seine France

IPSSI

L'IPSSI, grande école d'informatique, Web et Digital Marketing implantée à Paris, Marne-la-Vallée, Brest et Nice forme les étudiants du Bac au Bac+5 en alternance, aux métiers des technologies.

75012 Paris France

https://www.ecole-ipssi.com

NETAO

N

Notre centre de formation, installé à Quimper, forme les salariés et dirigeants des entreprises et collectivités dans leur transition digitale, en particulier dans le domaine de la cybersécurité.

29000 Quimper France

ŒIL POUR ŒIL CRÉATIONS

Formations à distance, elearnings et serious games pour acculturer les collaborateurs d'une entreprise à la la protection des données ou GDPR - RGPD, la cybersécurité.

59000 Lille France

https://www.oeilpouroeilcreations.fr

PHOSFOREA

Expert en sensibilisation-formation à la cybersécurité en e-learning et présentiel. Editeur SaaS : LMS, plateforme de faux phishing, application mobile. Contenus SCORM à façon et chefferie de projet.

31670 Labège France

PÔLE FORMATION UIMM BRETAGNE

L'École supérieure du numérique appliqué propose, en intra ou inter entreprise, des formations continues selon les 7 modules de l'ANSSI (3 en tronc commun et 4 spécialisés).

35170 BRUZ France

https://www.esna.bzh/esna/cyberdefense

SANS INSTITUTE

N

SANS, référence mondiale en matière de formation dans le domaine de la cybersécurité, propose plus de 70 cours, qui s'alignent sur les rôles, responsabilités et disciplines des équipes de sécurité.

20852 North Bethesda, MD États-Unis

https://www.sans.org

SECURESPHERE BY EPITA

SECURESPHERE by EPITA propose des formations professionnelles à la cybersécurité pour tous les collaborateurs. Ces modules couvrent aussi bien la sensibilisation que l'approfondissement technique.

94270 Le Kremlin Bicêtre France

https://www.securesphere.fr/index.php

SEELA

Accréditée organisme de formation, certifiée Qualiopi, Seela (groupe pr0ph3cy) est une plateforme SaaS pro-posant des formations en cybersécurité. La gamme de produits Seela conçue par des experts de

13290 Aix-en-Provence France

TERRANOVA SECURITY

C L

Chef de file mondial en sensibilisation à la sécurité, nous aidons les RSSI à mettre en place des programmes de simulation de phishing, de sensibilisation à la cybersécurité et de formation RGPD.

H7S 2N5 Laval Canada

https://terranovasecurity.com/fr

EC Label ExpertCyber
CL CLUSIF
CS CESIN
N Adhérents Numeum
H Adhérents Hexatrust

Hébergeurs - Data Center

3DS OUTSCALE N CS H

Fournisseur européen de Cloud d'hyper-confiance, proposant des services d'infrastructure hautement sécurisés (calcul, stockage, réseau et sécurité) qualifiés SecNumCloud, ISO 27001-27017-27018 et HDS.

92210 Saint-Cloud France

https://fr.outscale.com

ANTEMETA N

Découvrez les solutions AntemetA autour de nos expertises Réseau, Infrastructure, Cyber-Sécurité, Data Management et Plateformes & Solutions type SAP.

78280 GUYANCOURT France

https://www.antemeta.fr/

BRETAGNE TÉLÉCOM

Bretagne Télécom, labelisé Cloud Verified VMware, vous propose plusieurs solutions cloud privé et hybride, avec un hébergement sécurisé dans son Data Center certifié ISO 27001 et HDS.

35220 Châteaubourg France

https://www.bretagnetelecom.com

CELESTE

Baies 15 kVA, Suites 100 kVA
Fibre optique 1 à 10 Gb/s
6 opérateurs
Taux de disponibilité 100 %
Double chaîne électrique jusqu'à la baie
Surveillance 24/7
P.U.E. 1,3"

77420 Champs-sur-Marne France

https://www.celeste.fr

COREYE

Avec CoreTrust, COREYE (MSP et MSSP) propose des services managés de sécurité (Anti-DDoS, Waf, SIEM, Scan de vulnérabilité, SOC externalisé) pour sécuriser vos données. COREYE est ISO 27001 et HADS.

59262 Sainghin-en-Mélantois France

https://www.coreye.fr

DATA4 GROUP

DATA4, opérateur de data centers en Europe, dispose de réserves foncière et électrique (121 ha et 146 MW disponibles) uniques sur le marché européen pour accompagner la croissance de ses clients.

91460 Marcoussis France

https://www.data4group.com

FCNET CS N

Opérateur télécoms dédié aux professionnels, fcnet propose également des services d'hébergement en data center, anti-virus, firewall, infrastructure, poste.
Labellisé ExpertCyber.

25000 BESANCON France

https://www.fcnet.fr

FULLSAVE N

Opérateur indépendant qui fournit des services de connectivité, d'infrastructures cloud et d'hébergement mutualisé.
Certifié ISO 27001 sur le périmètre « Housing » de son propre datacenter TLS00.

31670 Labège France

http://www.fullsave.com

GROUPE CYLLENE N

Cyllene.Cyber planifie, organise, déploie, pilote et mesure tout en satisfaisant aux obligations réglementaires et aux exigences juridiques et assurantielles.

92000 Nanterre France

https://www.groupe-cyllene.com

GROUPE PSIH N

Hébergeur certifié de données de santé (1,2,3,4,6) proposant un ensemble de services permettant de déployer facilement des solutions tout en sécurisant les données des patients.

69003 Lyon France

https://ids.host

HELIANTIS

Opérateur Télécoms (FAI, MPLS, BGP…). Hébergement datacenter (sauvegardes, PRA&PCA…). Prestations de services : audit, conseil, intégration, cybersécurité, Réponse à incident.

64000 PAU France

https://www.heliantis.fr

IBO

Les services d'hébergement, les services d'infogérance, les services liés à la sécurité informatique, IBO est agréé depuis 2013 par le Ministère de la Santé en tant qu'Hébergeur de Données de Santé.

63014 Clermont-Ferrand Cedex 2 France

http://www.ibo.fr

IKOULA

Ikoula spécialiste, des serveurs dédiés et du Cloud depuis 1998. Propriétaire de 2 DataCenters en France et présent à l'international (filiale aux Pays-Bas), Cloud disponible sur 3 continents.

92100 Boulogne-Billancourt France

https://www.ikoula.com/fr

IRON MOUNTAIN

Iron Mountain votre partenaire de confiance : solutions digitales, Cloud, restauration de données archivées, externalisation des bandes de sauvegarde, destruction sécurisée de matériel informatique.

91420 Morangis France

https://www.ironmountain.fr

JAGUAR NETWORK CL

Jaguar Network est un opérateur cloud souverain qui accompagne plus de 1.000 clients pour valoriser leurs données grâce à 15 ans d'expertise en Cloud, Telecom, Big Data, IoT et services nanagés.

13321 Marseille France

https://www.jaguar-network.com

KABIA N

Services d'hébergement, Kabia est un opérateur Cloud souverain français fournissant des services managés à haute valeurs ajoutées tout en respectant les contraintes et processus métier des nos clients.

06100 Nice France

https://www.kabia.eu

LEVEL 3 COMMUNICATIONS

Level 3 dispose d'un portefeuille complet de services de sécurité basés sur son réseau international qui permet d'avoir une vision complète de la cartographie des menaces au niveau mondial.

92000 Nanterre France

http://www.level3.com/en

NEOJEDI

Clood le cloud à la française est une solution de stockage, de sauvegarde et de partage en ligne pour tous types & formats de documents, ultra sécurisée et entièrement localisée en France.

31500 Toulouse France

https://clood.co

OT GROUP

OT Group fait de la protection des données de ses clients son enjeu n°1 et propose : architecture Cloud, infogérance SI ; SaaS ; Web, interconnexion réseaux, SecOps, DevOps et sécurité informatique.

44800 Saint Herblain France

https://www.ot-group.com

RÉSEAU CONCEPT N

Pionnier de l'Internet, fondée en 1995, Réseau Concept dispose de ses propres data center. Nous infogérons plusieurs centaines de PME/PMI et ETI.

21000 Dijon France

https://www.reseau-concept.com

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction. Consultez le site web, qui peut comporter des mises à jour : www.solutions-numeriques.com/securite/annuaire-cybersecurite/. L'éditeur ne peut pas garantir l'exactitude des informations et décline toute responsabilité.

ROVERBA CGS CS

Depuis plus de 10 ans nous protégeons, les données de nos clients au sein d'un Data Center français ,avec une infinie précaution. L'accès est chiffré via VPN pour un niveau de sécurité optimal.

38230 CHAVANOZ France

https://www.roverba.com/

SYNAAPS

SynAApS fournit des services d'hébergement Cloud souverain (PaaS-IaaS, PRA-PCA, infogérance et Housing) haute qualité, doublement certifiés sécurité (ISO 27001:2013) et agréés Santé (HADS).

69603 Villeurbanne Cedex France

https://www.synaaps.com

TDF

TDF propose des services d'infrastructures sur l'ensemble du territoire : Datacenter, connectivité haut débit (fibre optique, faisceau hertzien), transit IP, liaison sécurisée vers les Clouds publics.

92120 Montrouge France

http://www.tdf-telecom.fr

THESEE DATACENTER

Thésée DataCenter est un opérateur français garantissant la souveraineté des données clients. Le très haut niveau de sécurité, la disponibilité et la performance énergétique exceptionnelle.

78410 Aubergenville France

https://thesee-datacenter.fr

TITAN-INFORMATIQUE

Solution de sauvegarde Cloud Souverain. Système complet et automatisé de sauvegarde et de restauration basé sur un prestataire physique.

83260 la crau France

https://ecura.fr

T-SYSTEMS FRANCE N

T-Systems opère des solutions de « Security as a Service » pour les protections, analyses et réponses aux risques et attaques. Ses 1 200 experts ont intégré et opèrent le Best-of-Breed des solutions.

93200 Saint-Denis France

VENDOME SOLUTIONS

Vendôme propose à ses clients la conception de data center sur-mesure et un hébergement dans ses locaux, en plein cœur de Paris.

25000 Besançon France

https://www.groupetenor.com

YULPA

YULPA propose des services d'hébergements et vous accompagne sur la sécurisation et l'audit de vos infrastructures hébergées chez YULPA ou en interne. Infrastructure intégralement en France.

75008 Paris France

https://yulpa.io

Avocats spécialisés

CABINET SFEZ AVOCATS

Domaines d'expertise : droit des Data et des technologies avancées, et Propriété intellectuelle. Prestations : rédaction et négociation de contrat, audit juridique, étude de faisabilité et formation.

75009 Paris France

https://www.avocats-sfez.fr

CHRISTIANE FERAL-SCHUHL SAINTE-MARIE AVOCATS

Depuis près de 30 ans, Christiane Feral-Schuhl éxerce dans le secteur du droit de l'informatique, des nouvelles technologies, des données personnelles et de la propriété intellectuelle, dont elle est un acteur reconnu.

75016 Paris France

www.feral-avocats.com

ITEANU AVOCATS

Société d'Avocats composée de 13 professionnels à l'activité quotidienne dédiée droit du numérique, conseil et défense de ses clients, depuis 28 ans. La cybersécurité est au coeur de sa pratique.

75008 Paris France

http://www.iteanu.com

LE NINIVIN AVOCAT

Le cabinet dispose d'une solide expérience dans la prévention des risques, la rédaction des contrats, la gestion des litiges associés, y compris les expertises techniques et la défense pénale.

75008 Paris France

LEXING ALAIN BENSOUSSAN AVOCATS

Le cabinet a été fondée 1978 par Aain Bensoussan, avocat à la Cour d'Appel de Paris et est spécialisé dans le droit de l'informatique.

75017 Paris France

https://wwww.alain-bensoussan.com

MATHIAS AVOCATS

MATHIAS Avocats vous accompagne tant en conseil qu'en contentieux de manière dédiée dans votre conformité juridique (contrats, conformité RGDP, droit des affaires).

75017 Paris France

http://www.avocats-mathias.com

PINSENT MASONS FRANCE LLP

Cabinet d'avocat disposant d'une expertise en droit des nouvelles technologies et tout particulièrement sur les questions de cybersécurité et de réglementation applicables aux données.

75008 Paris France

http://www.pinsentmasons.com

Cyber-assurances

ADD VALUE ASSURANCES

Assurance Cyber risques : 1. assistance informatique 24/7 ; 2. pertes d'exploitation ; 3. réclamations de tiers en cas de données perdues ; 4. enquêtes & sanctions assurables ; 5. négociations & rançon.

92800 PUTEAUX France

https://www.add-value.fr

AU SERVICE DU RISK

Management des risques - assurances des risques cyber - formation.

13390 AURIOL France

http://www.auservicedurisk.fr

BESSÉ

Bessé est conseil en assurances des entreprises. Le transfert à l'assurance du risque cyber renforce la chaîne de valeur de la cybersécurité. Nos experts vous accompagnent dans vos démarches.

44000 Nantes France

https://www.besse.fr/fr

CNC-EXPERTISE

CnC Expertise est un cabinet d'expertise en assurance spécialisé dans les réponses à incident cyber et les sinistres liés aux technologies de l'information.

78600 Maisons-Laffitte France

https://www.cnc-expertise.com

CYBEX ASSISTANCE N EC

CYBEX ASSISTANCE accompagne les organisations dans leurs besoins en matière de prévention et de résolution des problématiques liées à la cybercriminalité.

33300 BORDEAUX France

http://cybex-assistance.com

INPHB

RAS

00225 ABIDJAN Côte d'Ivoire

http://www.vne-ci.com

NEOTECH ASSURANCES H

Conseil en gestion de risque. Placement et gestion des sinistres Cyber. Audit des polices Cyber. Cartographie des risques cyber.

75017 PARIS France

https://www.neotech-assurances.fr

STOÏK

Stoïk, la première cyber-insurtech qui associe logiciel de sécurité et assurance pour protéger les TPE/PME des cyberattaques.

75008 Paris France

https://www.stoik.io

Distributeurs

ABBAKAN

Distributeur à valeur ajoutée spécialisé dans la commercialisation de solutions de cybersécurité à destination des intégrateurs, revendeurs et Telecoms du secteur des technologies de l'information.

92400 Courbevoie France

http://www.abbakan.com

ARROW ECS FRANCE

Spécialiste de la distribution de solutions d'infrastructure et de services dans les domaines des serveurs d'entreprise, stockage, logiciels et virtualisation pour les professionnels de l'informatique.

92600 Asnières sur Seine france

http://www.arrowecs.fr

CERBERIS

Forte de son expérience, la société Cerberis a su nouer des partenariats forts avec les plus grands acteurs du marché, lui permettant aujourd'hui de proposer à ses clients et partenaires des solutions.

38100 Grenoble France

https://www.cerberis.com

CONFIG

CONFIG propose des solutions par le biais de partenariats avec des acteurs reconnues de l'IT. Ceux-ci dispensent des formations et des compléments de compétences pour assurer leur savoir-faire.

75019 Paris France

https://www.config.fr

D2B INFORMATIQUE

Distributeur de solutions d'infrastructure, spécialisé dans les domaines de la protection des données, du Data Management et de la sécurité informatique.

93100 Montreuil France

http://www.d2b.com

DYNAMIT

Société de services et de distribution informatique nous fournissons, en plus du matériel et des logiciels, de l'assistance, de la maintenance, des services de protection et de cybersécurité.

92000 Nanterre France

https://www.dynamitservices.fr

EXCLUSIVE NETWORKS

Spécialiste mondial de la cybersécurité de confiance pour les infrastructures numériques, dispose de bureaux dans 40 pays, propose « Solution Zone » et le PowerLab pour une démonstration technique des intégrations en temps réel.

92100 Boulogne Billancourt France

https://www.exclusive-networks.com/fr

FEEDER

Offre vidéosurveillance, écosystème et les acteurs du marché de la vidéosurviellance.

13127 Vitrolles France

http://www.feeder.fr

GROUPE DFM

Groupe DFM accompagne les entreprises avec ses 4 expertises : informatique (infogérance & réseaux), télécoms, impression & solutions documentaires, et sécurité électronique.

94000 Créteil France

https://groupe-dfm.fr

HERMITAGE SOLUTIONS

Hermitage Solutions est un distributeur à valeur ajoutée spécialisé dans les solutions d'infrastructure, de réseau et de sécurité informatiques.

LYON 69001 France

https://www.hermitagesolutions.com

IGNITION TECHNOLOGY

Ignition, filiale du distributeur Exclusive Networks, est un incubateur de technologies de cybersécurité en mode SaaS, alliant souplesse d'un spécialiste local et robustesse d'un groupe mondiale.

92100 Boulogne-Billancourt France

https://www.ignition-technology.com

INFINIGATE

Infinigate est un distributeur spécialisé dans la fourniture de solutions de sécurité informatique. Pare-feu, Endpoints, authentification forte, audit… notre catalogue répond à tous les besoins.

92100 Boulogne-Billancourt France

http://www.infinigate.fr

INGRAM MICRO

Grossiste en produits technologiques, Ingram Micro offre aux partenaires un accès aux dernières technologies et solutions gérées, notamment le cloud, la configuration, la chaîne d'approvisionnement et le cycle de vie des actifs.

59810 Lesquin France

https://fr.ingrammicro.eu

MIEL

MIEL propose un éventail complet et complémentaire de technologies pour sécuriser l'informatique d'entreprise à l'ère du Cloud, protégeant endpoints, IoT, accès SaaS, réseaux, e-mails, identités…

91570 Bièvres France

https://www.miel.fr

NEOVAD

NeoVAD est distributeur de solutions innovantes autour du (DEM) Digital Experience Monitoring, du SASE (Secure Access Service Edge), et de la sécurité.

92100 Boulogne-Billancourt France

http://www.neovad.fr

TECH DATA FRANCE

Tech Data est un leader européen de la distribution de produits et services technologiques pour les réseaux de revendeurs.

776111 Bussy St Georges Marne-La-Vallée

https://fr.techdata.com

WATSOFT DISTRIBUTION

Watsoft propose une gamme complète de solutions de cyber-sécurité qui permet de minimiser et d'anticiper sensiblement les menaces, les cyber-attaques, les ransomwares, etc.

33600 Pessac France

https://www.watsoft.com

WESTCON-COMSTOR FRANCE

Distributeur à valeur ajoutée de solutions de pointe dans les domaines de la sécurité, la collaboration, les réseaux et les Data Centers, disposant d'un réseau mondial de revendeurs spécialisés.

92600 Asnières sur Seine France

https://www.westconcomstor.com/fr/fr.html

Recrutement

UVU GROUP CL

Cabinet de recrutement et management de transition spécialisé dans la gestion des risques d'entreprise et Cybersécurité pour le compte des grandes PME, ETI et groupes internationaux.

92000 Nanterre France

https://www.uvu-group.com

Les acteurs du marché

Panorama

Solutions et Services

Tableaux Comparatifs



- **Solutions - Tableaux comparatifs p190**
- **Services - Tableaux des prestataires p204**

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction.
L'éditeur ne peut pas garantir l'exactitude des informations et décline toute responsabilité.

Consultez le site web, qui peut comporter des mises à jour :
www.solutions-numeriques.com/securite/annuaire-cybersecurite/.

Les éditeurs et sociétés de services peuvent se référencer ou mettre à jour leur fiche existante sur la même page.

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction.

Éditeurs de

Société	Domaines couverts par l'offre									Etat des lieux					
	Données	Applications	Réseaux	Mobilité	Systèmes de contrôle industriels	Identité	Objets connectés	Blockchain	Poste de travail	Classification des données	Cartographie	Analyse de risques	Analyse de vulnérabilité	Log Management	Audit de code source
3D-OXIDES						●	●	●							
3M FRANCE	●			●											
42CRUNCH	●	●			●		●	●					●		●
6CURE	●		●									●			
8MAN	●					●					●				
A10 NETWORKS		●	●	●		●									
ACG CYBERSECURITY	●	●	●	●		●	●		●						
ACRONIS	●							●							
ADVANCED TRACK & TRACE	●			●	●	●									
AF SOFTWARE		●	●												
AFFINION INTERNATIONAL	●	●		●		●			●			●			
AIRBUS CYBERSECURITY	●		●		●				●			●	●		
ALGOSEC											●	●	●		
ALHAMBRA SYSTEMS SA	●	●	●		●	●	●	●				●	●	●	●
ALINTO	●	●	●	●										●	
ALL4TEC		●										●			
APICEM	●	●		●					●						
AQUA SECURITY		●										●	●		
ARCAD SOFTWARE	●										●				
ARCSERVE	●	●							●	●					
ARMIS (ARMIS.COM)			●		●		●		●		●	●	●		
ARS NOVA SYSTEMS	●	●		●											
ARSEN	●								●				●		
ARUBA A HEWLETT PACKARD ENTERPRISE COMPANY		●	●	●			●					●	●	●	
ARX ONE	●														
ATEMPO	●								●						
ATOS	●	●	●	●		●	●	●	●	●	●	●	●	●	●
AVANT DE CLIQUER									●			●	●		
AVAST BUSINESS									●				●		
AVAST SOFTWARE		●	●			●	●		●				●		
AVIRA	●	●	●	●		●	●		●			●	●		
AXONIUS		●	●										●		
AXWAY SOFWARE	●	●													
B<>COM	●		●	●		●	●	●							
BALABIT	●		●			●									
BARRACUDA NETWORKS	●	●	●				●						●		
BEEMO TECHNOLOGIE	●														
BERTIN IT	●		●	●	●				●			●	●		
BETA SYSTEMS	●	●				●	●				●	●		●	
BEWARE CYBERLABS			●		●	●	●		●		●		●		
BEYONDTRUST	●	●		●	●	●	●		●		●		●		
BE-YS SOFTWARE	●	●				●		●							
BITDEFENDER	●	●	●	●	●		●		●			●	●		
BKUBE	●	●	●						●	●		●	●		
BLOCKPROOF	●														
BMC SOFTWARE		●	●						●			●	●	●	●

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction.

Entreprises spécialisées en cybersécurité : référencement et mise à jour sur
https://www.solutions-numeriques.com/securite/annuaire-cybersecurite/

Solutions

Protection							Exploitation							Saas	Adhérent			
Threat Intelligence	Contrôle d'accès et gestion des identités	Protection de la donnée	Protection applicative	Protection des postes de travail	Protection réseau & infrastructure	Protection des terminaux mobiles	Sécurité & DevOps	SIEM	SOC	Dashboards sécurité	Réponse à incident	Analyses forensiques	Contrôles continus	Solutions délivrées en mode SaaS	NUMEUM	CLUSIF	CESIN	HEXATRUST
	●	●					●		●									
		●		●														
		●	●			●	●			●			●	●				
			●		●						●			●				●
	●	●					●	●		●	●	●	●					
			●		●		●			●	●	●	●	●				
		●																
	●											●	●					
	●	●	●	●	●	●	●											
		●		●		●												
●		●		●	●				●		●							
			●		●		●		●	●	●							
●	●	●	●	●	●		●	●	●		●	●		●				
●		●	●		●		●		●	●	●			●				
																●		
	●	●					●							●	●			
			●				●											
		●					●											●
		●		●	●		●							●				
											●		●	●		●		
		●				●								●				
										●			●	●		●		
●	●	●			●													
		●												●				
		●	●	●	●													●
●	●	●	●	●	●		●	●	●	●	●	●	●	●	●			
		●		●						●				●	●			
				●	●		●							●				
●	●	●	●	●	●	●									●			
●		●		●		●	●			●	●		●					
●			●	●	●	●	●	●	●	●	●		●	●				
	●	●								●				●				
	●	●			●									●	●			
	●				●			●	●	●								
●	●	●	●		●					●			●					
		●													●			
●		●			●													
	●	●					●			●		●	●			●		
●					●					●		●	●					
	●	●	●	●	●	●	●			●	●	●	●	●				
	●																	
●		●	●	●	●	●	●		●	●	●	●	●	●				
	●	●		●	●		●	●	●									
●			●	●	●		●	●		●	●	●	●	●	●			

Consultez le site web, qui peut comporter des mises à jour : www.solutions-numeriques.com/securite/annuaire-cybersecurite/. L'éditeur ne peut pas garantir l'exactitude des informations et décline toute responsabilité.

Éditeurs de

Société	Domaines couverts par l'offre									Etat des lieux					
	Données	Applications	Réseaux	Mobilité	Systèmes de contrôle industriels	Identité	Objets connectés	Blockchain	Poste de travail	Classification des données	Cartographie	Analyse de risques	Analyse de vulnérabilité	Log Management	Audit de code source
BOARD OF CYBER	●	●	●								●	●	●		
BOLDON JAMES	●			●					●	●					
BOX	●	●		●					●	●					
BRAINWAVE GRC	●	●				●				●	●	●			
CA TECHNOLOGIES	●	●	●	●		●	●			●		●			●
CAILABS			●												
CECURITY.COM	●	●		●		●								●	
CERTIGNA	●	●		●		●									
CERTINOMIS						●									
CHAMBERSIGN FRANCE						●									
CHECK POINT SOFTWARE TECHNOLOGIES	●	●	●	●	●	●	●		●	●	●	●	●	●	
CHECKMARX	●	●											●		
CISCO SYSTEMS FRANCE			●				●					●	●	●	
CITALID	●	●	●	●	●	●			●		●	●	●		
CLOUD ECO	●		●	●					●						
COFENSE	●		●												
COHESITY	●	●								●		●	●		
CONPAL	●								●	●					
CROWDSEC	●	●	●												
CROWDSTRIKE			●	●		●			●		●	●	●	●	
CRYPTONEXT SECURITY	●	●	●	●	●	●	●	●							
CYBELIUS					●						●				
CYBERARK	●	●				●	●		●		●	●	●		
CYBERNETECH SAS	●	●	●						●						
CYBEREASON															
CYBERRES MICRO FOCUS	●	●				●			●	●	●	●	●	●	●
CYBERVADIS	●											●			
CYBERWATCH		●	●		●				●		●	●	●		
CYBONET	●		●				●		●			●	●	●	
CYNET - HOLISTIC SECURITY SIMPLIFIED									●			●	●		
DANTOOIN	●	●				●				●		●	●		
DARKTRACE		●	●		●		●		●				●	●	
DATALOCKER	●					●								●	
DATAXIUM	●	●	●	●		●			●					●	
DATTO	●	●								●					
DHIMYOTIS	●	●				●	●		●						
DIGITAL GUARDIAN	●	●	●	●						●					
DIGITALBERRY	●	●	●			●	●	●	●		●	●			
DIGITEMIS (SOFTWARE)	●	●	●	●	●		●		●		●	●			
DISKYVER		●	●	●					●			●	●		
DMARC EXPERT		●				●									
DOCAPOSTE ARKHINEO	●	●													
DOCTOR WEB FRANCE	●	●	●	●					●						
DROPCLOUD	●	●							●						
ECHOWORX	●	●							●						
EDSI	●	●		●			●								

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction.

Solutions

Entreprises spécialisées en cybersécurité : référencement et mise à jour sur https://www.solutions-numeriques.com/securite/annuaire-cybersecurite/

Protection							Exploitation							Saas	Adhérent			
Threat Intelligence	Contrôle d'accès et gestion des identités	Protection de la donnée	Protection applicative	Protection des postes de travail	Protection réseau & infrastructure	Protection des terminaux mobiles	Sécurité & DevOps	SIEM	SOC	Dashboards sécurité	Réponse à incident	Analyses forensiques	Contrôles continus	Solutions délivrées en mode SaaS	NUMEUM	CLUSIF	CESIN	HEXATRUST
										●				●				
		●					●			●			●					
		●				●								●	●			
										●		●	●		●			●
	●	●	●			●	●			●				●				
		●			●													
		●												●	●			
	●	●												●				
	●													●	●			
●	●	●	●	●	●	●	●	●	●	●	●	●	●					
			●				●			●				●				
●	●	●	●	●	●	●	●	●	●	●	●	●	●	●		●		
●							●		●	●				●			●	
		●		●	●	●												
●											●			●				
●	●	●	●					●	●		●		●	●				
		●					●											
●		●	●	●	●	●	●			●	●			●				●
●	●	●		●		●	●		●	●	●	●	●	●			●	
		●	●		●	●								●				●
														●				
	●	●	●	●	●	●	●						●	●				
	●	●	●	●	●	●		●						●				
●	●	●	●	●	●		●	●	●	●	●	●		●		●		
										●				●		●		●
				●	●				●	●						●		●
●				●	●					●	●	●	●					
		●		●	●				●		●	●						
●		●	●										●	●				
●					●					●	●	●	●	●		●		
	●	●					●											
●		●	●	●	●	●		●	●	●	●			●		●		
															●			
		●		●							●			●				
	●	●	●	●	●	●	●			●			●					
		●												●	●	●		●
●			●	●	●		●		●	●				●				
		●		●										●				
		●												●	●	●		●
		●		●	●	●							●	●				
		●																
		●												●				
		●				●								●	●			

Consultez le site web, qui peut comporter des mises à jour : www.solutions-numeriques.com/securite/annuaire-cybersecurite/. L'éditeur ne peut pas garantir l'exactitude des informations et décline toute responsabilité.

Éditeurs de

Société	Domaines couverts par l'offre									Etat des lieux					
	Données	Applications	Réseaux	Mobilité	Systèmes de contrôle industriels	Identité	Objets connectés	Blockchain	Poste de travail	Classification des données	Cartographie	Analyse de risques	Analyse de vulnérabilité	Log Management	Audit de code source
EFFICIENTIP	●		●						●			●	●		
EGERIE	●	●	●	●	●	●	●	●	●		●	●			
EM2B	●														
ENTRUST	●					●	●	●							
EQUISIGN	●	●							●	●					
ERCOM (THALES)	●	●	●	●		●	●		●						
ESET FRANCE	●	●	●	●	●		●		●			●	●		
ETAS SAS		●	●		●		●					●	●		●
EURAFIBRE			●												
EUROEDI	●														
EVERTRUST		●				●					●				
EVINA		●											●		
F5 NETWORKS		●	●	●		●	●						●	●	
FACTORYTHINGS		●							●						
FEITIAN TECHNOLOGIES	●	●		●		●	●	●	●						
FLASHPOINT	●		●			●	●		●			●			
FLEXERA		●							●			●	●		●
FORECOMM	●	●	●	●		●			●						
FORGEROCK						●									
FORTINET	●	●	●	●	●	●	●		●			●	●		
FULL IP SOLUTIONS	●	●	●			●				●	●	●	●	●	
G DATA SOFTWARE	●	●	●	●											
GATEWATCHER	●	●	●		●								●		
GEMALTO	●	●		●		●	●	●							
GITGUARDIAN		●											●		●
GLIMPS	●	●	●	●			●		●				●		●
GLOBALSIGN	●		●	●		●	●								
GS2I	●	●	●		●		●		●						
GUARDICORE		●	●		●										
GUIDANCE SOFTWARE INC	●	●		●	●		●				●	●	●		
HACKNOWLEDGE SA	●	●			●	●	●		●						
HACKUITY	●	●											●		
HAREL SYSTEMS	●	●					●								
HARFANGLAB									●						
HELPSYSTEMS	●		●						●	●			●		
H-IAPPS	●		●									●	●		
HID GLOBAL						●						●	●	●	
HP INC		●							●						
HYPERVISION TECHNOLOGY	●	●	●		●	●	●		●			●	●	●	
IBM FRANCE	●	●		●		●			●	●		●	●	●	●
IDACTIS						●			●						
IDECSI	●	●											●	●	
IDNOMIC	●			●	●	●	●		●						
I-GUARD	●	●	●	●					●					●	
ILEX - GROUPE INETUM		●		●		●			●						
ILLUMIO		●	●								●				
IMPERVA	●	●								●		●	●	●	

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction.

Solutions

Entreprises spécialisées en cybersécurité : référencement et mise à jour sur https://www.solutions-numeriques.com/securite/annuaire-cybersecurite/

Protection							Exploitation							Saas	Adhérent			
Threat Intelligence	Contrôle d'accès et gestion des identités	Protection de la donnée	Protection applicative	Protection des postes de travail	Protection réseau & infrastructure	Protection des terminaux mobiles	Sécurité & DevOps	SIEM	SOC	Dashboards sécurité	Réponse à incident	Analyses forensiques	Contrôles continus	Solutions délivrées en mode SaaS	NUMEUM	CLUSIF	CESIN	HEXATRUST
		●			●		●	●	●				●	●	●	●	●	
									●	●	●			●			●	●
		●			●									●				
	●	●			●	●								●				
		●												●	●			●
	●	●	●	●	●	●												●
●	●	●	●	●	●	●		●	●		●	●	●	●		●		
	●	●	●		●		●	●						●				
					●													
		●												●				
	●	●	●							●				●				●
●			●			●				●		●		●				
●	●	●	●		●		●	●	●	●	●			●				
	●			●	●		●											
	●	●	●	●		●												
●										●	●	●						
			●	●														
	●	●	●											●				
●										●				●				
●		●	●	●	●		●	●	●		●	●		●				
●		●	●	●	●	●	●			●	●	●	●	●				
●		●	●	●						●	●	●		●				
●							●		●	●				●				
				●							●	●			●	●		
		●		●	●					●	●			●				
													●	●				
				●		●						●						
●	●	●					●			●				●				
●								●	●		●		●	●				
●	●	●	●	●	●		●	●	●	●	●	●		●	●	●		
	●			●		●												
●		●	●						●	●		●	●	●		●	●	
	●	●		●	●	●	●							●	●			
●		●	●	●	●													
	●														●	●		●
					●		●				●							
	●	●	●				●		●		●			●				

Consultez le site web, qui peut comporter des mises à jour : www.solutions-numeriques.com/securite/annuaire-cybersecurite/. L'éditeur ne peut pas garantir l'exactitude des informations et décline toute responsabilité.

Éditeurs de

Société	Domaines couverts par l'offre									Etat des lieux					
	Données	Applications	Réseaux	Mobilité	Systèmes de contrôle industriels	Identité	Objets connectés	Blockchain	Poste de travail	Classification des données	Cartographie	Analyse de risques	Analyse de vulnérabilité	Log Management	Audit de code source
IN GROUPE	●			●		●	●		●						
INFOBLOX	●		●	●	●		●		●		●				
INVENIS	●		●				●			●	●				
INWEBO TECHNOLOGIES		●	●	●		●	●	●	●						
ISIT	●	●	●	●	●		●		●	●		●	●	●	●
ISTORAGE	●					●								●	
ITRUST	●	●	●								●	●	●	●	●
IVANTI	●	●		●		●	●		●			●	●		
IXIA	●	●	●				●			●	●				
JUNE-FACTORY	●				●		●					●	●		
JUNIPER NETWORKS			●							●			●	●	
KASPERSKY LAB FRANCE	●	●	●		●				●				●		
KATANA DIGITAL SA	●			●			●		●						
KAZEKO		●		●			●								
KEMP-FLOWMON		●	●		●				●						
KEEEX	●	●		●		●	●	●	●	●				●	
KEEPER SECURITY	●					●			●					●	
KEYSIGHT			●		●		●		●		●	●	●		
KIUWAN		●											●		●
KIWI BACKUP	●	●		●					●						
KOBIL	●	●		●		●									
KONTROL SAS	●	●		●			●								
KUB CLEANER	●				●		●		●						
LACEWORK		●	●			●					●	●	●	●	
LASTPASS						●									
LINAGORA	●	●	●	●		●									
LMBA / GEDIX	●	●	●	●	●		●		●						
LOGPOINT	●	●	●	●	●				●					●	
LOOKOUT				●					●			●	●		
LUXTRUST	●			●		●									
LYBERO.NET	●														
MAKE IT SAFE	●	●	●		●						●	●	●		
MALWAREBYTES				●					●			●	●		
MAPREUVE	●														
MARKET ESPACE	●					●									
MCAFEE			●				●		●			●	●	●	
MENAYA	●	●	●	●					●		●	●	●		
MEROX		●				●					●		●		
MICROSOFT	●	●	●	●		●	●	●	●	●			●	●	
MOABI SOLUTIONS		●		●			●						●		●
MOBILE PROCESS				●											
MOSKITOS	●	●					●							●	
MYDPO	●														
MYQ FRANCE	●					●	●		●						
NAMESHIELD	●		●				●							●	
NANOCODE		●		●							●	●			
NCIPHER SECURITY	●						●								

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction.

Solutions

Entreprises spécialisées en cybersécurité : référencement et mise à jour sur https://www.solutions-numeriques.com/securite/annuaire-cybersecurite/

Protection							Exploitation							Saas	Adhérent			
Threat Intelligence	Contrôle d'accès et gestion des identités	Protection de la donnée	Protection applicative	Protection des postes de travail	Protection réseau & infrastructure	Protection des terminaux mobiles	Sécurité & DevOps	SIEM	SOC	Dashboards sécurité	Réponse à incident	Analyses forensiques	Contrôles continus	Solutions délivrées en mode SaaS	NUMEUM	CLUSIF	CESIN	HEXATRUST
	●	●												●	●	●		
●		●		●	●	●			●	●	●	●		●				
										●		●		●	●			
	●			●	●		●							●				
	●	●	●	●	●		●	●										●
	●						●											
●	●	●	●	●	●		●	●	●	●	●	●		●				
		●	●	●	●	●	●			●	●			●				
					●		●		●				●					
													●	●				
●	●	●	●		●		●	●	●	●	●	●						
●		●	●	●	●	●				●	●	●		●				
		●														●		
	●									●				●				
●					●		●	●	●	●	●	●	●	●				
	●	●		●				●						●	●			
	●	●					●							●				
●							●		●	●			●	●				
							●			●			●	●				
		●	●	●		●								●	●			
	●	●	●											●				
		●	●		●									●				
		●	●	●	●									●				
●			●		●		●		●	●	●	●	●	●				
	●									●				●				
	●	●			●										●			
						●								●				●
		●											●	●				
		●																
		●																
		●

Éditeurs de

Société	Domaines couverts par l'offre									Etat des lieux					
	Données	Applications	Réseaux	Mobilité	Systèmes de contrôle industriels	Identité	Objets connectés	Blockchain	Poste de travail	Classification des données	Cartographie	Analyse de risques	Analyse de vulnérabilité	Log Management	Audit de code source
NEOWAVE	●					●									
NETEXPLORER	●	●		●		●			●	●					
NETHEOS						●				●					
NETSCOUT								●				●	●		
NETSKOPE	●	●	●	●	●	●			●		●	●	●	●	●
NETWORK USERS INSTITUTE	●	●	●	●			●		●	●		●	●		
NETWRIX	●	●				●				●	●	●	●	●	
NEXTDAY.VISION		●			●	●			●						
NEXUS GROUP						●	●								
NIS	●	●	●	●		●	●		●						
NORMASYS	●	●	●						●	●			●		
NORMATION					●		●		●		●	●	●	●	●
NORMYA	●										●				
NOVALYS		●				●									
NOZOMI NETWORKS					●		●				●	●	●		
NTX RESEARCH	●					●	●			●	●				
NUCLEON SECURITY	●			●		●			●						
NXO		●	●	●		●			●			●			
OLFEO	●		●	●					●						
ONE IDENTITY						●						●	●	●	
ONELOGIN	●	●				●			●						
OODRIVE	●	●		●		●			●						
OPENIP		●	●	●					●						
OPENTEXT SECURITY SOLUTIONS	●		●						●						
OPSWAT	●			●					●				●		
ORACLE	●	●	●	●		●	●	●		●			●	●	
ORSEC TECHNOLOGIES SAS			●							●					
OVELIANE	●	●	●	●								●	●		
OVERSOC	●	●	●				●		●		●		●	●	
OXIBOX	●	●	●	●	●	●	●	●	●						
PALO ALTO NETWORKS	●	●	●	●	●	●	●		●	●	●	●	●	●	
PARSEC															
PATROWL	●		●							●	●	●	●		
PHINASOFT	●	●								●	●	●			
PHISHME	●	●							●	●	●	●	●		
PHOENIX CONTACT FRANCE	●	●	●	●	●				●						
PING IDENTITY CORPORATION						●									
PRADEO		●		●			●						●		
PRIM'X	●		●	●					●						
PROGENIA	●	●									●	●	●		
PROMISEC		●							●				●		
PROOFPOINT															
PROVE & RUN				●	●		●								
PYDIO	●			●					●						
QONTROL	●	●	●	●		●			●		●	●			
QUALYS	●	●	●	●	●		●		●		●		●		

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction.

Solutions

Entreprises spécialisées en cybersécurité : référencement et mise à jour sur
https://www.solutions-numeriques.com/securite/annuaire-cybersecurite/

Protection							Exploitation							Saas	Adhérent			
Threat Intelligence	Contrôle d'accès et gestion des identités	Protection de la donnée	Protection applicative	Protection des postes de travail	Protection réseau & infrastructure	Protection des terminaux mobiles	Sécurité & DevOps	SIEM	SOC	Dashboards sécurité	Réponse à incident	Analyses forensiques	Contrôles continus	Solutions délivrées en mode SaaS	NUMEUM	CLUSIF	CESIN	HEXATRUST
	●	●		●	●	●												●
	●	●												●	●	●		
	●													●	●			
●		●	●		●	●	●		●	●	●	●		●				
●	●	●	●	●	●	●	●	●	●	●	●	●	●	●		●		
●	●	●	●	●	●	●			●	●		●		●				
●	●	●								●								
	●						●							●				
	●				●	●												
	●	●												●				
		●	●	●	●		●	●		●								
●	●			●	●	●	●			●	●		●					
		●					●											
	●		●												●	●		
●								●	●	●		●	●	●				
	●	●																
	●		●	●	●	●			●							●		
	●			●	●									●	●			●
	●	●						●		●			●	●				
	●	●	●	●										●				
	●	●	●		●		●						●	●	●	●		●
	●			●	●									●	●			
●		●		●	●		●	●		●			●	●				
		●		●		●							●					
●	●	●	●		●	●	●	●		●				●	●			
●					●		●	●	●	●		●	●					
		●			●				●									
			●	●	●					●	●	●						●
		●		●							●			●				
●	●	●	●	●	●	●	●	●	●	●	●			●			●	
●	●	●	●				●		●	●			●	●				●
●		●		●	●			●	●	●	●		●	●				
		●	●		●													
	●		●											●				
●		●	●			●	●	●	●	●				●				●
		●		●	●	●									●			●
				●							●			●				
●				●					●	●	●	●	●	●				
																●	●	
		●	●		●													
		●													●			
	●	●	●	●	●	●				●				●				●
		●	●	●	●	●	●			●			●	●				

Consultez le site web, qui peut comporter des mises à jour : www.solutions-numeriques.com/securite/annuaire-cybersecurite/. L'éditeur ne peut pas garantir l'exactitude des informations et décline toute responsabilité.

Éditeurs de

Société	Domaines couverts par l'offre									Etat des lieux					
	Données	Applications	Réseaux	Mobilité	Systèmes de contrôle industriels	Identité	Objets connectés	Blockchain	Poste de travail	Classification des données	Cartographie	Analyse de risques	Analyse de vulnérabilité	Log Management	Audit de code source
QUERY INFORMATIQUE	●								●						
QUEST SOFTWARE	●	●	●	●		●	●		●		●	●	●	●	
RADWARE	●	●	●				●								
RAPID7	●	●	●			●			●			●	●	●	
RCDEVS			●	●		●			●						
RSA SECURID	●	●	●	●	●	●			●			●	●		
RUBYCAT	●	●	●		●	●									
SAILPOINT TECHNOLOGIES						●									
SCALE COMPUTING															
SCASSI SOLUTIONS	●	●	●		●		●				●	●	●		
SCHLEUPEN AG	●	●	●						●	●	●	●	●		
SCPTIME	●	●	●		●		●	●							
SEALD	●	●				●									
SEC'IT	●	●	●	●	●		●		●				●		
SECKIOT			●		●		●				●		●		
SECLAB	●		●		●				●						
SECLUDIT	●	●	●		●							●	●		
SECRET DOUBLE OCTOPUS				●		●									
SECURE2BROWSE		●							●						
SECURE-IC	●						●					●	●		
SECURITYSCORECARD	●	●	●				●				●	●	●		
SECUSERVE	●	●	●	●						●					
SEKOIA	●	●	●						●					●	
SENTINELONE									●						
SENTRYO			●		●		●				●		●		
SERENICITY	●		●						●			●			
SESAME IT	●	●	●		●	●			●		●	●	●	●	
SHADLINE	●				●		●								
SIEMENS					●										
SILVER PEAK		●	●												
SILVERFORT		●	●		●	●			●						
SITUATION	●	●	●				●			●	●				
SKYBOX SECURITY	●	●	●	●	●		●	●	●		●	●	●		
SKYHIGH NETWORKS	●	●	●	●							●	●		●	
SNOWPACK	●		●	●			●		●						
SOFT EXPANSION	●								●						
SONICWALL	●	●	●	●					●	●	●	●	●	●	
SOPHOS	●	●	●	●											
SPIRENT COMMUNICATIONS	●	●	●	●			●						●		
SPLUNK	●	●	●	●	●		●					●		●	
STIMSHOP			●	●	●		●		●						
STORMAGIC	●														
STORMSHIELD	●		●	●	●								●	●	
STRATON IT	●	●	●		●				●	●	●	●	●		
SYMANTEC	●	●	●	●	●	●	●		●	●	●	●	●		
SYNOPSYS NORTHERN EUROPE LTD		●										●			●

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction.

Solutions

Entreprises spécialisées en cybersécurité : référencement et mise à jour sur https://www.solutions-numeriques.com/securite/annuaire-cybersecurite/

Protection							Exploitation							Saas	Adhérent			
Threat Intelligence	Contrôle d'accès et gestion des identités	Protection de la donnée	Protection applicative	Protection des postes de travail	Protection réseau & infrastructure	Protection des terminaux mobiles	Sécurité & DevOps	SIEM	SOC	Dashboards sécurité	Réponse à incident	Analyses forensiques	Contrôles continus	Solutions délivrées en mode SaaS	NUMEUM	CLUSIF	CESIN	HEXATRUST
																●		
●	●	●	●	●	●	●	●			●	●	●	●	●				
			●		●		●		●	●								
●							●	●	●	●	●	●	●	●				
	●			●	●	●												
●	●			●	●	●		●	●		●		●	●				
	●				●		●			●	●		●					
	●	●												●			●	
					●		●											
			●		●		●						●		●	●		
		●								●	●		●					
		●			●		●	●	●	●				●	●			
	●	●												●				
					●								●					
●					●	●				●	●	●	●			●		
		●	●	●	●													●
					●		●			●			●	●				
	●		●			●	●	●						●				
		●		●														
●		●	●															
●		●	●	●	●		●	●	●	●	●	●	●	●		●		
		●	●	●	●									●	●			
●							●	●	●	●	●	●	●	●		●		
				●							●	●					●	
●					●					●	●	●	●	●				
		●		●	●					●	●		●					
●		●	●	●	●		●											
					●									●				
					●		●						●					
	●						●								●			
●	●	●	●	●	●	●	●		●	●	●	●	●	●				
●	●	●	●							●				●				
●		●			●		●		●		●	●						●
		●		●														
●	●	●	●	●	●	●	●			●			●	●				
	●	●	●	●	●											●		
					●					●			●					
							●	●	●	●	●	●	●	●	●			
	●			●	●	●												
		●					●											
●	●	●		●	●		●							●	●	●		
										●			●	●				
●	●	●	●	●	●	●			●	●	●	●	●					
		●	●				●						●					

Consultez le site web, qui peut comporter des mises à jour : www.solutions-numeriques.com/securite/annuaire-cybersecurite/. L'éditeur ne peut pas garantir l'exactitude des informations et décline toute responsabilité.

Éditeurs de

Société	Domaines couverts par l'offre									Etat des lieux					
	Données	Applications	Réseaux	Mobilité	Systèmes de contrôle industriels	Identité	Objets connectés	Blockchain	Poste de travail	Classification des données	Cartographie	Analyse de risques	Analyse de vulnérabilité	Log Management	Audit de code source
SYSPERTEC		●				●			●				●		
SYSTANCIA	●	●		●		●			●						
TANIUM		●	●		●				●		●	●	●		
TEAMVIEWER GMBH	●	●							●				●	●	
TEHTRIS	●	●	●	●	●	●	●		●			●	●	●	
TENABLE		●	●		●	●					●	●	●		
THALES	●	●	●	●	●	●	●	●		●	●	●	●	●	●
THEGREENBOW	●		●	●											
THREATQUOTIENT INC	●	●	●												
TIXEO		●	●												
TRANSFERTPRO	●	●		●						●					
TRANSMIT SECURITY						●									
TRELLIX	●	●	●	●	●		●		●					●	
TREND MICRO			●	●	●		●		●			●	●		
TRICENT	●	●													
TRUSTINSOFT	●	●	●	●	●	●	●	●				●	●		●
TRUSTWAVE	●	●	●	●		●	●		●			●	●	●	●
TUFIN		●	●			●						●	●	●	
UBIKA	●	●	●	●		●			●				●		
UNISYS											●	●			
USERCUBE						●									
VADE	●		●			●				●		●			
VARONIS	●						●			●		●			
VECTRA NETWORKS	●	●	●		●										
VEEAM	●	●							●			●			
VENAFI						●					●				
VERIZON	●		●	●	●	●	●	●		●	●	●	●	●	●
VMWARE	●	●	●	●	●							●			
VULCAN CYBER		●	●		●		●		●			●	●		●
WALLIX	●				●	●	●								
WASACA	●	●								●	●	●	●	●	
WATCHGUARD TECHNOLOGIES		●	●	●		●			●						
WHALLER	●	●		●											
WITHSECURE		●	●	●			●		●			●	●		
WOLEET	●					●		●							
WOOBE						●									
WOOXO	●	●							●						
WRAPTOR	●	●		●					●				●		
YAGAAN	●	●										●	●		●
YESWEHACK	●	●	●			●	●					●	●		
YOUZER		●				●					●				
ZERTIFICON SOLUTIONS GMBH	●					●									
ZIWIT	●	●									●		●		
ZSCALER	●	●	●	●											
ZYXEL FRANCE			●												

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction.

Solutions

Entreprises spécialisées en cybersécurité : référencement et mise à jour sur
https://www.solutions-numeriques.com/securite/annuaire-cybersecurite/

Protection							Exploitation							Saas	Adhérent			
Threat Intelligence	Contrôle d'accès et gestion des identités	Protection de la donnée	Protection applicative	Protection des postes de travail	Protection réseau & infrastructure	Protection des terminaux mobiles	Sécurité & DevOps	SIEM	SOC	Dashboards sécurité	Réponse à incident	Analyses forensiques	Contrôles continus	Solutions délivrées en mode SaaS	NUMEUM	CLUSIF	CESIN	HEXATRUST
	●				●			●							●			
	●	●	●	●	●	●								●		●		
				●			●		●	●	●	●	●					
			●	●	●						●		●	●				
●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
			●		●			●	●	●	●		●	●	●	●		
●	●	●	●	●	●	●	●	●	●	●	●	●	●		●	●	●	
		●			●	●									●	●		●
●									●	●	●							
		●														●		●
	●	●												●				
	●													●				
●		●	●	●	●	●	●	●	●	●	●	●	●	●		●		
●		●	●	●	●	●								●		●		
	●	●												●				
		●	●		●		●							●	●			●
●		●	●	●	●	●	●	●	●	●	●	●	●	●				
●					●		●	●			●		●	●				
●	●	●	●		●		●			●				●				●
	●	●	●	●	●	●								●	●			
	●													●				
●				●									●					●
		●					●			●	●	●	●					
		●	●	●	●				●	●			●					
		●		●	●													
●	●						●											
●	●	●	●	●	●	●	●	●	●	●	●	●	●	●				
		●	●	●	●	●	●	●		●	●				●			
●										●			●	●				
	●	●									●		●	●	●			●
	●	●	●	●	●	●	●	●		●		●	●	●				
●	●		●	●	●					●		●		●				
		●									●				●			
●		●		●	●	●								●				
	●	●																
		●		●														
		●	●	●		●									●			
				●			●							●	●			
		●	●				●			●								
	●	●	●		●		●		●	●			●	●	●	●	●	●
	●													●	●			
	●	●																
		●	●							●			●	●				
●		●	●		●	●	●			●				●		●		
					●													

Consultez le site web, qui peut comporter des mises à jour : www.solutions-numeriques.com/securite/annuaire-cybersecurite/. L'éditeur ne peut pas garantir l'exactitude des informations et décline toute responsabilité.

Prestataires

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction.

	Domaines couverts par l'offre									Organisation			Etat des lieux					
SOCIÉTÉ	Données	Applications	Réseaux	Mobilité	Systèmes de contrôle industriels	Identité	Objets connectés	Blockchain	Poste de travail	Conformité	Politiques de sécurité & gouvernance	Formation, sensibilisation	Classification des données	Cartographie	Analyse de risques	Analyse de vulnérabilité	Log Management	Audit de code source
2SI CONSULTING	●	●	●	●		●	●		●	◆	◆					◆▮▲	◆▮▲	
ABAKUS SÉCURITÉ	●		●	●						◆▮	◆▮	◆▮▲✖			◆	◆▮▲	◆▮▲	
ABINGTON ADVISORY	●	●	●	●					●	◆	◆	◆	◆	◆	◆	◆	◆	◆
ACCEIS	●	●	●	●			●		●	◆	◆	◆	◆	◆	◆	◆		◆
ACCENTURE	●	●	●	●	●	●	●	●	●	◆	◆	◆	◆▮	◆▮	◆▮▲	◆▮▲✖	◆▮▲	◆▮
ACELYS SERVICES NUMÉRIQUES	●	●	●	●					●	◆▮▲	◆▮▲	◆▮	◆	◆▮▲	◆▮▲	◆▮▲		
Groupe ACESI	●	●	●	●		●			●	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮	◆▮▲	◆▮▲	◆▮	◆▮
ACTIVANOS SAS	●		●			●				◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲	◆▮▲	
ACTIV'INFO			●							◆	◆	◆				◆		
ACTUELBURO	●	●	●	●	●	●	●		●	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲
ADACIS	●	●	●						●	◆	◆	◆			◆✖	◆		
ADENIUM	●	●	●	●	●	●	●	●	●	◆	◆	◆	◆	◆	◆	◆		
ADIKTS	●	●									◆	◆				◆		
ADVENS	●	●	●	●	●	●	●		●	◆▮▲	◆▮	◆▮	◆▮	◆▮▲	◆▮	◆▮▲	◆▮▲	◆▮
ADVENTIUM TECHNOLOGIES	●	●								◆	◆	◆	◆	◆	◆		◆	
ADVISO												◆▮▲✖						
AGENCEE	●		●	●					●	◆	◆	◆		◆	◆	◆		
AKAMAI TECHNOLOGIES	●	●		●		●										◆▮▲	◆▮▲	
AKERVA	●	●	●		●	●	●			◆▲	◆▲	◆	◆▲	◆▲	◆▲	◆▲	◆▲	◆▲
AKKA	●	●	●	●	●					◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮
ALASTAR	●		●						●	◆▮	◆▮	◆▮	◆▮	◆▮		◆▮		
ALEKSO	●	●	●	●		●			●	◆▮▲✖	◆					▲✖	▲✖	
ALENATEC	●		●	●	●	●		●	●	◆	◆	◆		◆▮	◆	◆	◆▮	
ALGOSECURE	●	●	●							◆	◆	◆	◆	◆	◆	◆	◆	◆
ALLISTIC	●	●	●	●		●	●		●	◆	◆	◆	◆	◆	◆	◆▲	◆▮▲	◆▮▲
ALMOND	●	●	●	●		●	●		●	◆	◆	◆✖	◆	◆	◆	◆▲	◆▲	◆
ALTRAN TECHNOLOGIES	●	●	●	●	●	●	●	●	●	◆	◆	◆▮	◆	◆	◆	◆	◆	◆
AMBICIO	●	●		●		●	●		●	◆✖	◆	◆	◆	◆	◆		◆	
AMBIONICS SECURITY	●	●	●															
AMOSSYS	●	●	●	●	●	●	●		●	◆	◆	◆	◆	◆	◆	◆	◆	◆
ANEXIS	●	●							●	◆		◆	◆	◆	◆			
APIXIT	●		●	●		●			●	◆▮▲	◆▮▲	◆▮	◆	◆▮▲	◆▮▲	◆▮▲	◆▮▲	
APSIDE	●	●	●							◆▮				▮		▮		
ARMATURE TECHNOLOGIES	●	●	●			●		●	●									
ASSYSTEM					●					◆	◆	◆	◆	◆	◆	◆		
ATE	●	●	●							▲	▲	▲	▲	▲	▲	▲	▲	▲
ATN GROUPE	●			●		●				◆		◆		◆		◆▮▲	◆▮▲	
AUTICONSULT	●	●	●	●	●	●	●	●	●	◆	◆		◆	◆	◆	◆	◆	◆
AVITI	●		●			●			●	◆	◆	◆	◆	◆▮▲			▮	
AXEL IT			●	●		●	●		●	◆	◆▮			◆▮	◆▮	◆▮	◆▮	
AXIANS	●		●		●					◆	◆	◆	◆	◆▮	◆	◆▮▲	◆▮▲	
AXIANS C&C MARSEILLE-NICE-MONACO	●	●	●	●	●	●			●	◆▮	◆▮	◆▮	◆	◆	◆	◆▮▲	▮▲	
AXICOM-SECURITE	●	●	●	●		●			●		◆▮				◆▮			
AZERI BEGI CYBERSÉCURITÉ	●	●			●	●			●			◆			◆			
BEA INFORMATIQUE	●	●	●	●					●	◆▮▲	◆▮▲	◆▮▲	◆	◆▮▲	◆▮▲	◆▮▲		
BEARINGPOINT	●	●	●	●	●	●	●	●	●	◆▮	◆	◆	◆	◆	◆	◆	◆	◆
BLUESCREEN			●						●									
BOCK CONSEIL			●		●					◆	◆	◆		◆	◆			

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction.

Entreprises spécialisées en cybersécurité : référencement et mise à jour sur
https://www.solutions-numeriques.com/securite/annuaire-cybersecurite/

de Services

◆ Conseil ▮ Intégration ▲ Infogérance ✖ Edition

Protection							Exploitation							Contrôles			CERT	FORM	Adhésion				
Threat Intelligence	Contrôle d'accès et gestion des données	Protection de la donnée	Protection applicative	Protection des postes de travail	Protection réseau & infrastructure	Protection des terminaux mobiles	Sécurité & DevOps	SIEM	SOC	Dashboards sécurité	Réponse à incident	Analyses forensiques	Contrôles continus	Tests d'intrusion	Audit d'architecture	Audit organisationnel	CERT	Organisme de Formation	NUMEUM	CLUSIF	CESIN	Hexatrust	Label ExpertCyber
◆▮▲	◆▮▲	◆▮▲	◆▮	◆▮	◆▮			◆		◆			◆▮▲	◆	◆	◆			●				
◆▮▲✖		◆▮		◆▮	◆▮	◆▮▲		◆▮	◆▲	◆▮	◆▮	◆▮✖	◆	◆▮▲	◆				●				
◆	◆	◆	◆	◆	◆	◆		◆	◆	◆	◆			◆	◆	◆							
	◆	◆	◆	◆	◆	◆	◆	◆			◆			◆	◆	◆		●					
◆▮▲✖	◆▮▲✖	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮	◆	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆	◆	◆		●	●				
	◆▮	◆▮▲	◆▮▲	◆▮▲	◆▮▲			◆▮▲		◆▮▲	◆	◆	◆▮▲	◆▮	◆▮	◆▮							
◆▮	◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮	◆▮▲				◆▮	◆▮▲	◆▮▲			●				
◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲			◆▮▲		◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲		●					
		◆▮		◆▮	◆▮			◆			◆▮		◆▮	◆▮	◆	◆		●					
◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲							
					▮▲			◆						◆	◆	◆							
◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆				●			
			◆		◆▮		◆							◆	◆								
◆▮▲	◆▮	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮	◆▮	◆▮▲	◆▮	◆▮	◆▮		●			●		
◆▮	◆	◆	◆	◆	◆		◆	◆	◆	◆	◆	◆	◆	◆	◆	◆			●				
				◆▮▲	◆▮▲			◆▮▲	◆▮▲	◆▲	◆▲	◆▲	◆▲	◆▲	◆▲								
		◆▮	◆▮				◆▮	◆▮			◆▮								●				
																			●				
	◆	◆			◆			◆								◆				●			
▲	▲	▲	▲		▲		▲	▲	▲	▲	▲	▲	▲	▲	▲	▲							
	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲			◆					◆▮▲	◆	◆								
◆	◆	◆	◆	◆	◆		◆	◆	◆	◆	◆	◆	◆	◆	◆	◆			●				
	◆▮▲			◆▮▲	◆▮▲			◆			▮▲				◆▮▲								
◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮		◆										●					
◆	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆	◆▮▲	◆	◆▮▲	◆▮	◆	◆	◆▮▲	◆	◆	◆			●	●			
▮▲	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	▮▲✖	◆▮	▮▲	◆▮▲	◆▮	◆▮	◆▮▲	◆▮	◆▮	◆▮			●				
	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮																	
	◆			◆								◆		◆									
		◆▮	◆▮	◆▮▲	◆▮▲			◆▮▲						◆▮▲	◆▮▲	◆▮▲							
◆	◆	◆	◆	◆	◆	◆	◆	◆▮	◆	◆▮	◆	◆			◆	◆▮							
	▲	▲		▲	▲	▲					▲												
								◆							◆								

Consultez le site web, qui peut comporter des mises à jour : www.solutions-numeriques.com/securite/annuaire-cybersecurite/. L'éditeur ne peut pas garantir l'exactitude des informations et décline toute responsabilité.

Prestataires

SOCIÉTÉ	Domaines couverts par l'offre									Organisation			Etat des lieux					
	Données	Applications	Réseaux	Mobilité	Systèmes de contrôle industriels	Identité	Objets connectés	Blockchain	Poste de travail	Conformité	Politiques de sécurité & gouvernance	Formation, sensibilisation	Classification des données	Cartographie	Analyse de risques	Analyse de vulnérabilité	Log Management	Audit de code source
BRIGHTWAY	●	●	●	●					●	◆	◆	◆	◆	◆	◆	◆	◆	
BSI FRANCE	●	●	●	●	●	●	●			▮								
BSSI CONSEIL ET AUDIT	●	●	●	●	●	●	●	●	●	◆	◆	◆	◆		◆	◆▮✖	◆▮	◆▮
BUG BOUNTY ZONE	●	●	●		●		●											
BY THE WAY	●	●	●	●	●	●	●		●	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	
CALYPT CYBERSÉCURITÉ	●	●	●		●			●			◆▲	◆	◆		◆	◆✖		◆
CAPGEMINI - SOGETI	●	●	●	●	●	●	●		●	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲
CAPGEMINI TECHNOLOGY SERVICES	●	●	●	●	●	●	●		●	◆	◆	◆	◆	◆▮	◆	◆▮	◆▮▲	◆▮
CEGEDIM OUTSOURCING		●	●	●					●	◆▮▲	◆▮▲		◆▮▲	◆▮▲		◆▮▲		
CEIS	●	●	●							◆	◆	◆	◆	◆▮	◆▮	◆	◆▲	
CGI FRANCE	●	●			●	●	●			◆▮▲	◆▮	◆	◆▮	◆▮	◆▮	◆▮	◆▮▲	◆▮▲
CLARANET	●	●					●		●	◆▲	◆▲	◆▲			◆	▲	▲	▲
CNPP CYBERSECURITY	●	●	●	●	●	●	●		●	◆	◆	◆	◆	◆	◆	◆	◆	◆
CO-C	●	●	●	●	●	●	●	●	●			◆▮				◆▮		◆▮
COESSI	●	●	●	●	●		●			◆	◆	◆	◆	◆	◆	◆		◆
COGITAL	●	●		●	●				●	◆▮	▮		▮					◆▮
CONIX	●	●	●	●	●		●		●	◆	◆	◆	◆		◆	◆	◆	◆
CONSEILPREV CYBER			●	●	●		●			◆▮	◆▮	◆		◆	◆	◆	◆	
CONSORT	●	●	●	●		●	●		●	◆▮▲			◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲
COREYE	●	●	●			●				◆▲	◆▮▲		◆▲		◆▮▲	◆▮▲	◆▮▲	
CORTEXERA	●	●	●	●	●	●	●	●	●	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮
C-RISK										◆	◆	◆			◆			
CS GROUP	●	●	●		●	●	●		●	◆▮▲✖	◆▮▲✖	◆	◆▮▲	◆▮▲✖	◆▮	◆▮	◆▮✖	◆
CYBER-EGIDE	●		●			●				◆						◆		
CYBERENS	●				●		●			◆✖	◆		◆	◆	◆			
CYBERGLOBAL	●	●	●	●		●	●		●		◆	◆	◆▮	◆▮	◆▮	◆▮		
CYBERSEC&YOU	●	●	●	●	●	●	●		●	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮
CYBERSOLUTIONS	●	●	●						●	◆▮	◆▮▲	◆	◆	◆	◆▮	◆▮	◆▮	◆
CYBERZEN	●										◆	◆▮✖	◆	◆	◆			
DATA PRIVACY PROFESSIONALS	●	●	●	●	●	●	●	●	●	◆	◆	◆	◆	◆	◆			
DAVID INFORMATIQUE	●		●	●					●					◆▮▲		◆▮▲	◆▮▲	
DBM PARTNERS		●	●	●		●	●		●	◆	◆	◆	◆	◆	◆	◆		
DEEPIT	●	●	●		●	●			●		◆	◆						
DELOITTE	●		●	●	●	●	●	●	●	◆	◆	◆	◆	◆	◆	◆	◆	◆
DEVELOPPEMENT CONSEIL COMMUNICATION	●		●	●	●	●	●		●	◆▮▲	◆▮	◆✖	◆	◆▮▲	◆▮	◆▮▲✖	◆▮▲	
DEVENSYS CYBERSECURITY	●	●	●	●	●	●	●		●	◆▮	◆▮	◆▮▲			◆▮	◆▮▲	◆▮▲	
DEVOTEAM	●	●	●	●	●	●	●	●	●	◆✖	◆	◆	◆	◆▮	◆	◆		◆▮
DIGITAL SECURITY	●	●	●		●	●	●	●	●	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮▲	◆▮▲
DIGITEMIS (CYBERSECURITY & PRIVACY)	●	●	●	●	●		●		●	◆	◆	◆	◆	◆	◆	◆		◆
DIGORA	●	●									◆▮▲			◆▮▲	◆▮▲			
DILITRUST	●	●		●							◆✖		✖					
DPO CONSULTING	●									◆✖	◆✖	◆✖	◆✖	◆✖	◆✖	◆✖		
EBRC	●	●	●	●		●			●	◆▮▲✖	◆▮▲✖	◆▮▲✖	◆▮▲	◆▮▲	◆▮▲✖	◆▮▲	◆▮▲	
E-CATALYST	●		●	●		●	●		●	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆	◆▮▲		
ECO HARDWARE SAS	●	●	●	●	●	●	●	●	●									
EIFFAGE ENERGIE SYSTÈMES - CLEMESSY	●	●	●	●	●	●	●		●	◆▮	◆▮	◆▮	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲
EIGHT TECH	●	●	●						●	◆▮▲	◆▮▲		◆▮▲	◆	◆	◆▮▲	◆▮▲	◆

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction.

de Services

◆ Conseil ▮ Intégration ▲ Infogérance ✖ Edition

Protection							Exploitation							Contrôles			CERT	FORM	Adhésion				
Threat Intelligence	Contrôle d'accès et gestion des données	Protection de la donnée	Protection applicative	Protection des postes de travail	Protection réseau & infrastructure	Protection des terminaux mobiles	Sécurité & DevOps	SIEM	SOC	Dashboards sécurité	Réponse à incident	Analyses forensiques	Contrôles continus	Tests d'intrusion	Audit d'architecture	Audit organisationnel	CERT	Organisme de Formation	NUMEUM	CLUSIF	CESIN	Hexatrust	Label ExpertCyber
		◆	◆	◆	◆			◆	◆▮▲	◆✖	▲	◆▲	◆	▲	▲	▲				●			
		◆▮						▮						◆			●	●		●			
◆	◆▮	◆▮	◆	◆▮	◆▮	◆▮	◆▮▲	◆	◆▮	◆▮	◆▮	◆▮	◆▮▲	◆▮▲	◆▮	◆▮	●	●		●			
			◆		◆									◆									
◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲							
◆	◆	◆	◆	◆	◆	◆	◆		◆	◆	◆	◆	◆	◆	◆	◆		●					
◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲			●				
◆▮▲	◆▮▲	◆▮	◆▮	◆▮▲	◆▮▲	◆▮▲	◆▮	◆	◆▮▲	◆▮▲	◆	◆	◆	◆	◆	◆			●	●			
	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		●	●				
◆								◆	◆▮▲	◆▲✖	◆▮			◆▲		◆		●		●			
		◆▮	◆	◆			◆	◆▮▲	◆▮▲	◆▮	◆▲	◆	◆▮▲	◆	◆	◆			●				
▲		▲	▲	◆▲			▲	◆▲	▲	▲	▲	◆▲	◆▲	◆▲	◆	◆			●				
◆	◆	◆	◆	◆	◆	◆	◆	◆		◆	◆	◆		◆	◆	◆				●			
		◆▮	◆▮		◆▮							◆▮		◆▮				●					
		◆	◆	◆	◆	◆	◆	◆		◆		◆		◆	◆	◆			●	●			
▮	▮	▮	▮	◆▮	◆▮	◆▮		◆▮	▮		▮	▮		◆▮	◆▮	◆▮							
◆							◆	◆	▮▲	◆	◆	◆		◆	◆	◆	●			●			
◆	◆			◆			◆	◆▮	◆	◆▮						◆							
◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲					●				
◆▲	◆▲	◆▲	◆▮▲		◆▮▲		◆	◆▲	◆▮▲		◆▲	◆▲			◆	◆			●				
	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮							
								◆												●			
◆▮✖	◆▮✖	◆▮▲✖	◆▮▲✖	◆▮▲	◆▮▲✖	◆▮▲	◆	◆▮▲✖	◆▮▲✖	◆▮▲✖	◆▮▲✖	◆▮▲	◆▲	◆	◆	◆			●				
						✖		◆							◆	◆							
		◆✖						◆							◆	◆							
	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮					◆▮		◆▮	◆▮	◆▮	◆▮							
◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮							
◆▮▲	◆▮		◆▮	◆▮	◆▮		◆▮	◆▮			◆▮		◆▮▲	◆▮					●				
		◆			◆					◆						◆		●					
	◆	◆	◆	◆	◆			◆			◆				◆	◆		●	●				
	◆	◆			▲																		
◆		◆	◆	◆		◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆		●		●			
◆▮▲✖	◆▮	◆▮	◆▮▲✖	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲✖	◆▮▲✖	◆▮▲	◆▮	◆▮▲	◆▮	◆								
	◆▮▲	◆▮▲	◆	◆▮▲	◆▮▲	◆▮▲	◆	◆▮	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮	◆▮						●	
◆▮	◆▮	◆	◆	◆	◆		◆▮	◆		◆▮	◆	◆	◆	◆	◆	◆	●		●	●			
◆▮▲	◆▮▲	◆▮▲	◆▮	◆	◆▲	◆	◆▮	◆▮	◆	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	●	●		●	●		
	◆	◆	◆	◆	◆	◆		◆		◆	◆			◆	◆	◆			●			●	
																			●	●			
		◆																	●				
								◆								◆✖			●				
◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲						●	
◆▮▲				◆▮▲✖		◆▮▲		◆▮▲						◆▮▲					●				
	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮	◆	◆▮▲	◆▮▲			◆▮▲	◆▮▲					●			
◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲							

Consultez le site web, qui peut comporter des mises à jour : www.solutions-numeriques.com/securite/annuaire-cybersecurite/. L'éditeur ne peut pas garantir l'exactitude des informations et décline toute responsabilité.

Prestataires

SOCIÉTÉ	Domaines couverts par l'offre									Organisation			Etat des lieux					
	Données	Applications	Réseaux	Mobilité	Systèmes de contrôle industriels	Identité	Objets connectés	Blockchain	Poste de travail	Conformité	Politiques de sécurité & gouvernance	Formation, sensibilisation	Classification des données	Cartographie	Analyse de risques	Analyse de vulnérabilité	Log Management	Audit de code source
EITA CONSULTING	●	●	●				●			◆			◆				◆	◆▮
ELIT-CYBER	●	●	●						●		◆▮▲		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲
ENGIT	●	●	●			●			●	◆	◆		◆	◆	◆	◆	◆	◆
ETELCOM	●	●	●	●					●	◆▮▲	◆▮▲	◆▮			◆▮▲	◆▮▲		
EXAPROBE - GROUPE ECONOCOM	●	●	●	●		●	●		●	◆▮				▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲
EXCELLIUM SERVICES	●	●	●	●		●		●		◆▮	◆	◆			◆▮	◆▮	◆▮	◆▮
EXPONENS	●					●				◆	◆		◆		◆			◆
EXTERN IT	●	●	●	●					●	◆	◆▮▲	◆		◆▮▲	◆	◆	◆▮▲	
EXTIA		●	●	●						◆	◆					◆	◆	◆
EXTREMIT	●	●	●						●		▮▲	▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		
FIDENS	●	●	●	●	●	●	●		●	◆	◆		◆	◆	◆			
FORMIND	●	●	●	●	●	●	●		●	◆	◆	◆	◆▮		◆	◆▲	◆▮▲	◆
G-ECHO	●	●	●						●	◆▮✖	◆▮✖	◆▮✖	◆▮	◆▮	◆▮	◆▮▲		◆▮
GPLEXPERT	●	●	●						●	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	
GRAND E NOV	●	●	●	●	●	●	●	●				◆						
GROUPE INFODIS			●	●					●		◆▮▲			◆▮▲				
GROUPE SII	●	●	●	●			●			◆	◆	◆		◆		◆	◆	◆
HARMONIE TECHNOLOGIE	●	●	●	●		●	●			◆▮	◆▮	◆▮	◆▮	◆▮	◆▲	◆		
HEADMIND PARTNERS	●	●	●	●	●	●	●	●	●	◆	◆	◆	◆	◆	◆	◆	◆	◆
HELIX SECURITY SAS	●		●							◆▮	◆▮	◆▮▲			◆▮	◆▮	◆▮▲	
HEXANET	●	●	●	●		●			●		◆		◆	◆	◆	◆	◆▮	
HIRMES	●		●				●		●	◆▮	◆▮	◆▮		◆▮	◆▮	◆▮▲		
HIUMA	●	●	●						●	◆▮▲	◆▮▲	◆▲			◆▮▲✖	◆▮▲✖	◆▮▲	
HOLISEUM	●	●	●	●	●	●	●	●	●	◆	◆	◆	◆	◆	◆	◆	◆	◆
HUB ONE	●	●	●	●	●	●			●	◆▮✖	◆▮✖	◆▮✖	◆▲		◆	◆▮▲	◆▮▲	◆
I.S. MANAGEMENT	●	●	●	●	●				●	◆▮▲✖	◆▮▲✖	◆						
IBC DIALOG	●	●	●	●					●	◆▮▲	◆▮▲	◆▮▲		◆▲	◆▮▲	◆▮▲	◆▲	
IDAXIO	●										◆▮							
IDENTO	●	●		●		●	●											
ID-LOGISM	●	●	●	●		●	●		●	◆▮	◆▮	◆	◆▮		◆▮			
IDNA	●	●	●	●	●	●	●		●	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲
IMS NETWORKS	●	●	●	●	●	●			●	◆▮▲	◆▮▲✖		◆	◆	◆	◆▮▲	◆▮▲	◆
INDATABLE	●	●	●	●					●	◆	◆	◆	◆	◆	◆	◆		◆
INET SYSTEM	●		●						●			◆▮▲		◆▮▲		◆▮▲		
INETUM	●	●	●	●	●	●	●		●									
INFOCLIP	●	●	●	●		●		●	●	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲
INFORSUD TECHNOLOGIES		●	●	●					●	◆▮▲		◆▮▲	◆▮		◆▮	◆▮▲		
INFOSYS	●	●	●	●	●	●	●	●	●	◆▮▲	◆▮▲	◆	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲
INOPS	●	●	●	●	●		●	●		◆▮	◆▮▲		◆▮		◆▮	◆▮		
INQUEST	●	●	●		●	●	●		●	◆	◆	◆	◆	◆	◆	◆		
INTEGRALE IP			●		●									◆▮				
INTEGRASYS	●		●	●			●		●						◆▮▲✖	◆▮▲✖		
INTERDATA		●	●	●		●	●		●		▮					◆▮▲	◆▮▲	
INTRINSEC	●	●	●		●		●		●	◆	◆▲	◆	◆	◆▲	◆	◆▮▲	◆▮▲	◆▲
ISATECH	●	●	●	●						◆▮	◆▮▲	◆▮	◆▮	◆▮	◆▮			
ISE SYSTEMS	●	●	●		●					◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮
IT&M REGIONS	●	●	●	●					●	◆▮▲	◆▮▲			◆▲				
IT3 INFORMATIQUE	●	●	●	●		●			●	◆▲	◆▮▲	◆	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction.

de Services

◆ Conseil ▮ Intégration ▲ Infogérance ✖ Edition

Protection							Exploitation							Contrôles			CERT	FORM	Adhésion				
Threat Intelligence	Contrôle d'accès et gestion des données	Protection de la donnée	Protection applicative	Protection des postes de travail	Protection réseau & infrastructure	Protection des terminaux mobiles	Sécurité & DevOps	SIEM	SOC	Dashboards sécurité	Réponse à incident	Analyses forensiques	Contrôles continus	Tests d'intrusion	Audit d'architecture	Audit organisationnel	CERT	Organisme de Formation	NUMEUM	CLUSIF	CESIN	Hexatrust	Label ExpertCyber
		◆	◆▮✖		◆▮		◆▮	◆		◆▮		◆▮							●				
◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲			◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲							
◆	◆	◆	◆	◆	◆		◆	◆			◆			◆	◆	◆			●				
		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲			◆▮▲		◆▮▲		◆▮▲	◆▮▲							●
◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲✖	◆▮▲	◆▮▲	▮▲	◆▮	◆▮▲	▮▲	◆▮▲	▮▲	◆▮▲	▮▲	▮▲	▮▲			●				
◆▮		◆▮	◆▮	◆▮	◆▮	◆▮▲	◆▮▲	◆▮	◆▮▲✖	◆▮▲	◆▮▲	◆▮▲	◆▮▲✖	◆▮	◆▮		●	●					
	◆							◆	◆	◆		◆			◆	◆							
	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆	◆▮▲	◆			◆▮▲	◆▮	◆▮▲	◆▮▲			●				
	◆			◆▮	◆▮	◆▮	◆▮	◆	◆					◆▮									
		▮▲	▮▲	▮▲	▮▲	▮▲					▮▲				▮▲	▮▲							
		◆	◆	◆		◆		◆							◆	◆		●		●			
◆	◆▮	◆▮	◆▮	◆▮▲	◆▮	◆▮▲	◆	◆	◆▮▲	◆	◆	◆		◆▲	◆	◆			●	●		●	
		◆▮	◆▮	◆▮			◆▮	◆▮						◆▮		◆▮✖		●	●				
	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲							
		◆																	●				
	◆▮▲		◆▮▲	◆▮▲	◆▮▲			◆▮▲		▮▲			▮		◆▮				●				
	◆▮	◆▮	◆	◆	◆		◆▮	◆				◆		◆	◆	◆		●					
	◆▮	◆▮	◆▮				◆▮	◆▮		◆▮	◆▮	◆▮		◆▮	◆▮	◆▮			●				
◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆							
◆▮	◆	◆▮	◆▮	◆▮	◆▮		◆▮▲	◆▮	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮	◆▮	◆▮							
◆	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲			▲	▲	▲				◆	◆							
				◆	◆▮	◆		◆▮			◆		◆	◆▮	◆▮								
◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲							
	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆	◆		◆		◆		◆	◆	◆				●			
◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆	◆▮	◆▮▲	◆▮▲	◆	◆▮	◆▮▲	◆	◆	◆			●	●			
		◆▮▲✖		◆▮▲✖				◆▮▲															
	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮	◆▮		◆▮▲	◆▮							
		◆▮																					
	◆▮▲																						
◆	◆▮	◆▮	◆	◆	◆	◆	◆▮	◆▮	◆	◆	◆		◆	◆	◆	◆							
◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲				●			
✖	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲			◆▮▲	◆▮▲	◆▮▲✖	◆▮▲	◆	◆▮▲	◆	◆	◆							
								◆						◆	◆	◆							
	◆▮▲			◆▮▲		◆▮▲													●				
																			●				
	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲		◆▮▲	◆▮▲				●			
	◆▮▲	◆▮▲	◆▮	◆▮	◆▮▲	◆▮▲		◆▮▲					◆▮▲	◆▮	◆▮				●				
◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲			●				
	◆	◆	◆				◆▮	◆▮	◆			◆▮	◆▮	◆▮	◆▮	◆▮			●				
◆	◆	◆	◆	◆	◆	◆		◆			◆	◆			◆	◆							
		◆▮	◆▮		◆▮▲							◆▮	◆▮		◆▮					●			
	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲					◆▮▲			◆▮▲	◆▮	◆▮	◆▮							
◆▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲				◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮									
◆▲		◆▲	◆▲	◆▲	◆▲	◆▲	◆▲	◆	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▲	◆	◆			●		●		
		◆▮▲	◆▮▲		◆▮▲	◆▮▲		◆▮			◆▮		◆▮▲		◆▮	◆▮		●	●				
◆▮	◆▮	◆▮	◆▮	◆▮	◆▮		◆▮	◆▮	◆▮	◆	▮	◆▮	◆▮	◆▮	◆▮	◆▮						●	
	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲		◆▮▲	◆▮▲				◆	◆			●				
◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▲			◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲							

Consultez le site web, qui peut comporter des mises à jour : www.solutions-numeriques.com/securite/annuaire-cybersecurite/. L'éditeur ne peut pas garantir l'exactitude des informations et décline toute responsabilité.

Prestataires

	Domaines couverts par l'offre									Organisation			Etat des lieux					
SOCIÉTÉ	Données	Applications	Réseaux	Mobilité	Systèmes de contrôle industriels	Identité	Objets connectés	Blockchain	Poste de travail	Conformité	Politiques de sécurité & gouvernance	Formation, sensibilisation	Classification des données	Cartographie	Analyse de risques	Analyse de vulnérabilité	Log Management	Audit de code source
I-TRACING	●	●	●	●	●	●			●	◆▮▲	◆▮▲	◆	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲
ITS GROUP	●	●	●	●		●	●		●	◆	◆▮▲		◆▮		◆▲	◆▲	◆▲	
ITS INTEGRA	●	●	●						●	▲	▲		◆▮		◆▲	◆▲	◆▲	▲
IVISION	●	●	●						●	◆▮▲	◆▮▲	◆▮▲	◆	◆	◆	◆		◆
JANUA		●	●	●		●	●											
JLLNET	●		●						●	◆	◆		◆▮	◆▮▲			◆▮	
JS	●									◆			◆	◆	◆			
K SECURITY	●		●									◆			◆			
KPMG	●	●	●	●	●	●	●	●	●	◆	◆	◆	◆	◆	◆	◆	◆	◆
KUDELSKI SECURITY	●	●	●	●	●		●	●	●	◆▮	◆▮	◆▮	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮
KYRON SI	●	●	●	●	●	●	●		●	◆▮▲	◆▮▲	◆▮	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	
LECPAC CONSULTING	●	●	●			●			●	◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	
LEXFO	●	●	●	●	●	●	●	●	●					◆		◆	◆▲	◆
LISIS CONSEIL	●	●	●	●	●		●		●	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮		
LOGIFORM CONSEIL	●	●	●	●					●		◆▮	◆▮		◆▮				
LOGIN SECURITE	●	●	●	●	●	●	●	●	●	◆▮▲	◆▮▲	◆▮▲	◆	◆	◆▮	◆▮	◆▮	◆▮
MANIKA	●	●	●	●	●		●		●	◆	◆	◆	◆	◆	◆	◆		◆
MASTER SECURITY CONSEIL	●	●	●			●	●		●	◆▮▲	◆▮▲	◆▮	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲
MATILAN	●	●	●	●					●	◆	◆▮▲	◆▮			◆			
MCA	●	●	●		●						◆	◆	◆		◆	◆	◆	
MEDIANE SYSTEME					●		●			◆	◆							◆
METANEXT	●		●			●				◆	◆▮				◆▮	◆▮		
METSYS	●	●		●		●	●		●	◆▮▲	◆▮▲		◆▮▲	◆▮	◆	◆	◆▮▲	
MHCONSEIL	●	●	●						●	◆▮▲	◆▮▲			◆▮▲	◆	◆		
MICROPOLE	●	●	●			●	●			◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲
MIXCOM	●	●	●						●						◆			
MODIS		●	●	●	●		●		●	◆	◆				◆	◆	◆▮	◆▮
MPTCONSEIL	●		●	●	●	●			●	◆	◆▮	◆▮	◆	◆	◆▮			
NAXIOS	●	●	●						●			◆▮▲				◆▮▲		
NBS SYSTEM	●	●	●			●				◆	◆▮	◆			◆	◆	◆▮	◆
NDA-SECURITY	●	●	●	●	●	●	●	●	●	◆▮✖	◆✖	◆	◆✖	◆	◆	◆✖	◆✖	◆✖
NET FREED	●	●	●	●		●		●	●	◆	◆	◆	◆	◆	◆	◆	◆	◆
NETFORMATIC			●						●	◆▮▲	◆▮▲		◆	◆	◆			
NEWLODE	●	●	●		●	●			●		◆▮▲			◆▮		◆▮▲	◆▮▲	
NOMIOS	●	●	●											◆▮▲		◆▮▲	◆▮▲	
NOVENCI			●	●		●			●	◆▲	◆▲	◆▲		◆▲	◆▮▲	◆▮▲	◆▲	
NOVIDY'S	●	●	●		●	●			●	◆	◆	◆	◆	◆	◆	◆	◆▮▲✖	◆
NTT FRANCE	●	●	●	●	●	●	●	●	●	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮▲	◆▮▲	◆▮
NXO FRANCE	●	●	●			●			●		◆▮▲			◆▮	▮		▮▲	
OFISS							●					◆		◆	◆	◆		
OÏKIALOG		●	●	●	●				●	◆▮▲	◆▮					◆▮▲	◆▮▲	
ONPOINT AFRICA GROUP	●	●	●		●													
ON-X GROUPE	●	●	●	●	●	●	●	●	●	◆	◆	◆	◆	◆	◆	◆	◆	◆
OPEN GROUPE		●																
OPENMINDED PART OF ACCENTURE	●	●	●		●	●				◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲
OPENSPHERE	●	●	●		●		●			◆	◆	◆	◆▮	◆	◆	◆	◆▮	

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction.

de Services

◆ Conseil ▮ Intégration ▲ Infogérance ✖ Edition

Protection							Exploitation							Contrôles			CERT	FORM	Adhésion				
Threat Intelligence	Contrôle d'accès et gestion des données	Protection de la donnée	Protection applicative	Protection des postes de travail	Protection réseau & infrastructure	Protection des terminaux mobiles	Sécurité & DevOps	SIEM	SOC	Dashboards sécurité	Réponse à incident	Analyses forensiques	Contrôles continus	Tests d'intrusion	Audit d'architecture	Audit organisationnel	CERT	Organisme de Formation	NUMEUM	CLUSIF	CESIN	Hexatrust	Label ExpertCyber
●	●	●	●	●	●		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	●	●			●		
●	●	●	●		●	●	◆▲	◆	◆▮▲			◆	◆▮▲	◆	◆								
●	●	●					◆▲	◆	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲				●			
●	●	●						◆▮▲						◆▲	◆▲	◆▲							
	●	●	●		●	●													●				
●		●						◆			◆▮▲	◆▮	◆▮▲		◆▮	◆▮							
●								◆															
●		●													◆								
●	●	●	●	●	●	●	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆							
●	●	●	●	●		●	◆▮▲	◆▮	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮	◆▮					●			
●	●	●	●	●	●	●		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲			●	●			
●	●	●			●		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆	◆▮▲							
●	●	●	●	●		●	◆	◆▮	◆	◆▮	◆▮		◆▮	◆		◆▮				●			
●	●	●	●								◆▮▲				◆▮▲			●	●				
●	●	●	●	●	●	●	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮	◆▮	◆▮			●	●		●	
●	●	●	●	●		●		◆			◆	◆		◆	◆	◆			●	●			
●	●	●			●	●	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲							
●	●	●	●				◆▮▲	◆	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		●					
●	●	●		●										◆	◆								
				●		●		◆							◆				●	●			
●		●			●		◆▮	◆	◆▮						◆▮				●				
		●	●		●			◆▲	◆▲	◆▲	◆▲		◆▮▲	◆▲	◆▲	◆▲							
●	●	●		●	●			◆✖	◆▮▲	◆▲	◆▲	◆	◆	◆	◆	◆		●					
●	●	●	●	●	●	●	◆	◆▮	◆▮▲	◆	◆▮▲	◆▮▲	◆▮▲	◆▲	◆▲	◆▲				●			
●	●	●			●				◆▮▲				▮▲	◆▮	◆▮				●	●			
						●								◆		◆	●	●					
	●	●	●	●				◆▮▲	◆▮	◆▮			◆	◆▮									
●	●	●		●																			
●	●	●	●	●	●	●	◆	◆	◆▮▲	◆	◆▮▲	◆	◆▮▲	◆	◆	◆			●	●		●	
	●						◆▮▲✖												●	●			
●	●	●		●	●		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲			●				
●	●	●		●		●	◆	◆	◆▮▲	◆▲	◆▲	◆▲	◆▲	◆▮	◆▮	◆▮			●				

Consultez le site web, qui peut comporter des mises à jour : www.solutions-numeriques.com/securite/annuaire-cybersecurite/. L'éditeur ne peut pas garantir l'exactitude des informations et décline toute responsabilité.

Prestataires

SOCIÉTÉ	Domaines couverts par l'offre									Organisation			Etat des lieux					
	Données	Applications	Réseaux	Mobilité	Systèmes de contrôle industriels	Identité	Objets connectés	Blockchain	Poste de travail	Conformité	Politiques de sécurité & gouvernance	Formation, sensibilisation	Classification des données	Cartographie	Analyse de risques	Analyse de vulnérabilité	Log Management	Audit de code source
OPTRIUM	●					●					◆▮▲		◆▮▲	◆▮▲		◆▮▲	◆▮▲	
OPTYMA SARL	●	●		●		●			●	◆▮	◆▮	◆▮	◆▮	◆	◆▮	◆		
ORANGE CYBERDEFENSE	●	●	●	●	●	●	●		●	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲
OROL SOLUTIONS	●	●	●	●			●		●	◆▮▲	◆▮▲	◆▮	◆▮	◆▮	◆▮▲	◆▮▲	◆▮▲	
OSINX - GROUPE ACTIMAC	●	●	●	●		●			●	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲		
PA CONSEIL	●			●					●			◆	◆					
PCL ASSISTANCE INFORMATIQUE	●		●						●		◆▮▲			◆▮▲	◆▲	◆▮▲		
PHOEBE					●							◆			◆	◆		
PICTIME GROUPE	●	●	●			●				◆▮▲	◆▮▲	◆	◆▮▲	◆▮▲	◆▮	◆▮▲	◆▮▲	◆▮▲
PINSENT MASONS FRANCE LLP	●	●	●	●	●	●	●	●	●	◆	◆	◆	◆	◆				
PPP-CONSEIL			●		●		●			◆▮	◆▮	◆▮		◆▮▲				
PRIAMOS	●	●	●	●	●	●	●	●	●	◆	◆	◆	◆	◆	◆			
PRIVACY IMPACT	●	●	●	●		●	●	●	●	◆	◆	◆	◆	◆	◆			
PROBE I.T	●		●				●			◆	◆	◆	◆▮	◆▮	◆▮▲	◆▮▲		
PROCESS-IT	●	●	●	●		●			●	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	
PRODWARE	●	●	●	●		●	●		●	◆▮▲✖	◆▮▲✖	◆▮▲						
PRODWARE BIS	●	●	●			●	●		●	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	
QUIETIC			●	●					●	◆	◆	◆▮		◆▲		◆▮		
QUODAGIS			●			●	●		●	◆▮▲				◆▮▲		◆▮▲		
QUODAGIS INTEGRATION		●	●	●		●			●									
QUONEX	●	●	●	●			●											
RAMPAR	●	●	●	●		●	●		●	◆▮	▮	◆▮		◆		◆▮	◆▮▲	◆▮
REALSOFT INFORMATIQUE	●	●	●															
RECOVEO													◆✖					
RGPD LEGAL	●	●				●	●		●	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮			
RHSOLUTION	●	●	●	●	●	●	●		●	◆	◆	◆						
RISK&CO	●		●		●													
RLG INFORMATIQUE	●	●	●						●									
SASETY	●	●	●	●		●	●		●					◆▮▲✖		◆▮▲✖	◆▮▲✖	
SAVANE CONSULTING	●	●	●			●					◆▮				◆▮		◆▮	
SCASSI	●	●	●	●	●	●	●		●	◆▮✖	◆▮✖		◆	◆	◆▮	◆	◆▮▲	◆▲
SCC FRANCE	●	●	●	●		●	●	●	●	◆▮▲✖	◆▮▲✖	◆▮▲✖	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲
SCHNEIDER ELECTRIC			●		●		●											
SCIURUS CONSEIL	●	●	●	●					●	◆	◆	◆		◆	◆	◆		
SEC-IT SOLUTIONS	●	●	●	●	●	●	●		●	◆	◆	◆	◆	◆	◆	◆▮	◆▮	
SECTOR					●					◆					◆	◆		◆
SECUREWARE	●	●	●	●					●	◆▮▲		◆▮▲				◆▮▲	◆▮	◆▮▲
SECUREWORKS	●	●	●	●			●			◆	◆		◆	◆	◆	▲	▲	
SECURIVIEW SAS			●						●	◆▮▲	◆▮▲		◆▮	◆▮	◆▮	◆▮▲✖	◆▮▲	◆
SERMA SAFETY & SECURITY	●	●	●	●	●	●	●		●	◆	◆	◆			◆	◆▮▲		◆▮▲
SERVAL-CONCEPT	●	●	●	●	●	●	●		●		◆	◆	◆	◆	◆	◆	◆	◆
SFR BUSINESS	●	●	●	●	●	●	●		●	◆▮	◆▮	◆	◆▮▲	◆	◆	◆▮▲	◆▮▲	◆
SII					●						▮▲							
SILICOM	●	●	●							◆	◆	◆	◆▮	◆	◆	◆▮	◆▮	◆▮
SMARTPOINT	●	●	●	●	●	●	●	●	●	◆▮▲	◆▮▲				◆▮▲	◆▮▲		◆▮▲
SNS SECURITY		●	●						●		◆▮▲	◆▮▲			◆	◆▮▲	◆▮▲	◆
SOCOA SÀRL										◆	◆	◆	◆		◆			

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction.

de Services

◆ Conseil ▮ Intégration ▲ Infogérance ✖ Edition

Protection							Exploitation							Contrôles			CERT	FORM	Adhésion				
Threat Intelligence	Contrôle d'accès et gestion des données	Protection de la donnée	Protection applicative	Protection des postes de travail	Protection réseau & infrastructure	Protection des terminaux mobiles	Sécurité & DevOps	SIEM	SOC	Dashboards sécurité	Réponse à incident	Analyses forensiques	Contrôles continus	Tests d'intrusion	Audit d'architecture	Audit organisationnel	CERT	Organisme de Formation	NUMEUM	CLUSIF	CESIN	Hexatrust	Label ExpertCyber
	◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲																	
		◆▮		◆				◆▮	◆▮	◆▮	◆					◆							
◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲✖	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲	●	●	●	●			
◆▮▲	◆▮	◆▮▲	◆▮	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▲		◆▮▲	◆	◆	◆▮▲	◆▮▲	▮▲				●			●
	◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲		◆▮▲			◆▮▲	◆▮		◆▮▲	◆▮▲	◆▮▲							
		◆																					
		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮									◆▮▲	◆▮▲							
		◆													◆	◆		●	●				
◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲			●				
	◆	◆					◆	◆			◆	◆											
◆▮								◆▮							◆▮▲	◆▮▲							
	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆							
	◆	◆	◆	◆	◆	◆	◆	◆			◆	◆	◆	◆	◆	◆							
	◆	◆	◆	◆	◆			◆						◆▮▲	◆▮▲	◆▮▲							
◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲							
								◆▮▲															
◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲							●
◆	◆	◆		◆▮▲	◆▮▲	◆		◆	◆	◆	◆		◆		◆▮▲	◆			●				
	▮▲			▮▲	▮▲			◆▮▲			▮▲		▮▲					●	●				
																			●				
					▮																		
◆▮▲	◆▮	◆▮	◆▮▲	◆▮	◆▮▲	◆▮	◆▮▲	◆▮	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲					●					
			◆▮▲✖	◆▮▲✖	◆▮▲✖													●					
	◆▮	◆▮		◆▮				◆▮								◆▮							
							◆	◆	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮							
																			●				
◆▮▲✖	◆▮▲✖	◆▮▲✖	◆▮▲✖	◆▮▲✖	◆▮▲✖	◆▮▲✖		✖	◆▮▲✖	◆▮▲✖	◆▮▲✖	◆▮▲✖	◆▮▲✖	◆▮▲✖	◆▮▲✖								
◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮			◆▮		◆▮	◆▮			◆▮	◆▮			●				
◆	◆	◆▲	◆▮	◆	◆	◆▮	◆	◆▮	◆▮▲	◆	◆▮▲	◆▮▲	◆▮▲✖	◆▮▲✖	◆▲	◆▲			●	●			
◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲			●	●			
																				●			
◆	◆	◆	◆	◆	◆	◆		◆			◆	◆		◆	◆	◆		●					
	◆	◆▮	◆▮	◆▮	◆▮	◆▮		◆		◆▮▲	◆	◆	◆▮▲	◆▮	◆▮	◆▮							
								◆															
◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮	◆▮▲	◆▮▲	◆▮	◆▮▲	◆▮▲	◆▮▲	◆▮▲							
▲		◆▲	▲	◆▲	◆▲		▲	◆	◆▲	◆	◆▲	◆▲	▲	◆	◆	◆	●						
		◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆	◆	◆				●			
	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲			◆	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲							
		◆	◆	◆		◆					◆	◆		◆▲	◆▲	◆		●					
	▮▲	◆▮▲	▮▲	▮▲	▮▲	▮▲		◆▮	◆▲	◆	◆	◆	◆	◆▮	◆▮	◆▮			●				
																			●	●			
◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆	◆	◆		◆	◆▮✖	◆▮✖	◆▮	◆▮				●				
◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	●	●					
◆▮▲			◆▮▲	◆▮▲	◆▮▲		◆▮▲		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮	◆							
	◆						◆	◆						◆	◆	◆							

Consultez le site web, qui peut comporter des mises à jour : www.solutions-numeriques.com/securite/annuaire-cybersecurite/. L'éditeur ne peut pas garantir l'exactitude des informations et décline toute responsabilité.

Prestataires

SOCIÉTÉ	Domaines couverts par l'offre									Organisation			Etat des lieux					
	Données	Applications	Réseaux	Mobilité	Systèmes de contrôle industriels	Identité	Objets connectés	Blockchain	Poste de travail	Conformité	Politiques de sécurité & gouvernance	Formation, sensibilisation	Classification des données	Cartographie	Analyse de risques	Analyse de vulnérabilité	Log Management	Audit de code source
SODIFRANCE	●	●	●	●					●	◆	◆▮▲	◆	◆	◆	◆	◆▮▲	◆▮▲	◆
SO-IT			●						●	◆▮	◆▮	◆▮	◆▮	◆▮	▮			
SOLUCEO DGPF	●		●	●		●			●	◆▮				◆▮▲	◆▮			
SOPRA STERIA	●	●	●	●	●	●	●		●	◆▲	◆▲	◆▲	◆▮▲	◆▮▲	◆▲	◆▮▲	◆▮▲	◆▮▲
SOSATOUTPC	●	●	●				●		●			◆	◆			◆		
SPIE ICS	●	●	●	●	●	●	●		●	◆	◆	◆▲	◆	◆	◆	◆	◆▮▲	
SQUAD	●	●	●	●		●	●	●	●	◆	◆	◆▮▲	◆▮	◆▮	◆	◆▮	◆▮▲	◆▮
STEEL PC	●	●	●	●					●	◆		◆▲	◆	◆	◆		◆▮▲	
STRATEGY & GOVERNANCE	●	●	●	●							◆	◆		◆	◆	◆		
SYNACKTIV	●	●	●	●	●		●		●			◆				◆✖		◆
SYNCHRONE	●	●	●	●	●	●	●	●	●	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮
SYNETIS	●	●	●	●		●			●	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲
SYNEXIE	●	●	●		●	●	●		●									
SYSDREAM	●	●	●	●	●	●	●		●	◆	◆	◆	◆		◆	◆		◆
SYSTEMIS	●	●	●			●	●		●	◆	◆	◆	◆	◆	◆	◆	◆	◆
TALC SI	●	●	●			●					◆▮▲✖		◆▮▲		◆▮▲	◆▮▲	◆▮▲✖	
TECODATA	●		●	●		●		●	●			▲						◆
TEOS CYBERSECURITY	●	●	●		●		●		●	◆	◆	◆			◆	◆		◆
TIBCO	●		●	●			●		●	◆▲	◆▲	◆▲		◆▲	◆▲	◆▲	◆▲	
TNP CONSULTANTS	●						●	●		◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮
TRAX	●	●	●	●	●	●	●	●	●									
TRÈFLE SOLUTION			●			●				◆	◆	◆		◆	◆	◆▮▲	◆▮▲	◆▮▲
TRSB		●	●	●					●		◆▮▲		◆▲	◆▲	◆▲	◆▲		
T-SYSTEMS	●	●	●		●	●	●	●							◆▲	◆▲	◆▲	
UBCOM SA	●		●		●		●			◆	◆▮	◆	◆	◆	◆	◆		◆
UBG. CYBER	●	●	●	●	●	●	●		●	◆	◆	◆			◆	◆		
UNUMKEY	●	●	●	●	●		●		●		◆▮✖	◆▮✖	◆	◆	◆	◆		
UPSAIL	●	●									◆▮▲	◆▮	◆▮		◆▮	◆▮		
URAEUS CONSULT	●									◆	◆	◆	◆	◆	◆	◆		
UTIKXO	●			●		●			●	◆	◆	◆	◆	◆	◆			
VAADATA	●	●		●			●											
VEYAN	●	●	●	●	●	●	●		●	◆	◆	◆	◆	◆	◆	◆▮	◆	
VFLIT OMR INFOGÉRANCE	●		●			●			●	◆▮▲	◆▮▲	◆▮▲	◆▲	◆▲	◆▲	◆▲	◆▮▲	
VNEXT	●	●	●	●	●	●	●	●	●	◆	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮
WALLACK	●	●	●	●	●	●			●	◆▮✖	◆▮	◆▮		◆▮	◆▮		◆▮	
WANCORE			●			●					◆▮▲		◆		◆	◆▮▲	◆▮▲	◆
WANNATH	●	●	●	●	●	●	●	●	●	◆	◆	◆	◆	◆	◆	◆	◆	◆
WAPLI INFORMATIQUE	●	●	●	●					●		◆▮▲	◆▮		◆▮		◆▮▲	◆▮	
WAPSI	●	●		●		●			●	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮
WAVESTONE	●	●	●	●	●	●	●	●	●	◆	◆	◆	◆	◆	◆	◆	◆	◆
WEODEO	●	●	●	●			●		●	◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	
WISE PARTNERS	●	●	●			●	●	●		◆	◆	◆	◆	◆	◆	◆	◆	◆
XMCO	●	●	●									◆		◆		◆		◆
XPERIZ										◆						◆		
YEC'HED MAT CONSEIL	●									◆	◆	◆						
YOGOSHA SAS	●	●	●	●	●	●	●	●								◆		◆
YOURAX	●		●	●					●	◆▮	◆▮	◆▮▲	◆▮		◆▮	◆▮▲	◆▮	
ZENIKA	●	●				●	●	●				◆				◆	◆	◆
ZERO TRUST SAS	●	●	●	●			●		●	◆▮	◆▮▲✖	◆▮	◆	◆▮▲	◆▮▲	◆▮▲	◆▮▲✖	

Sélection non exhaustive, à partir d'informations des entreprises qui se sont référencées en ligne, éventuellement modifiées par la rédaction.

de Services

◆ Conseil ▮ Intégration ▲ Infogérance ✖ Edition

Protection							Exploitation							Contrôles			CERT	FORM	Adhésion				
Threat Intelligence	Contrôle d'accès et gestion des données	Protection de la donnée	Protection applicative	Protection des postes de travail	Protection réseau & infrastructure	Protection des terminaux mobiles	Sécurité & DevOps	SIEM	SOC	Dashboards sécurité	Réponse à incident	Analyses forensiques	Contrôles continus	Tests d'intrusion	Audit d'architecture	Audit organisationnel	CERT	Organisme de Formation	NUMEUM	CLUSIF	CESIN	Hexatrust	Label ExpertCyber
◆▮▲	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆	◆▮▲	◆▲	◆	◆		◆	◆	◆		●	●				
◆▲			◆▮	◆▮▲	◆▮▲	◆▮		◆▮			◆▮▲	◆▮	◆▮		◆▮	◆▮							
◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮							◆▮▲	◆▮▲							
◆▮▲	▮▲	◆▮▲					◆▮▲	◆▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▲	◆▲	◆▲	●		●	●			
		◆		◆	◆					◆						◆		●					
◆	◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲		◆	◆▮▲	◆▮▲	◆▮	◆▮		◆	◆	◆		●	●	●			
	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆	◆▮▲	◆▮▲	◆▮▲	◆▮	◆▮	◆▮	◆	◆		●		●			
	◆▮		◆▮	◆▮	◆▮		◆▮	◆			◆▮	◆▮	◆▲		◆▮	◆▮							
		◆								◆		◆	◆	◆	◆	◆							
														◆✖	◆			●					
◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮	◆▮			●	●			
◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲			●	●		●	●
	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲			◆▮▲	◆▮▲		◆▮▲	◆▮	◆▮								
◆	◆	◆	◆	◆	◆	◆	◆	◆	◆		◆	◆		◆	◆	◆				●			
◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆			●				
	◆▮▲	◆▮▲✖		◆▮	◆▮▲	◆▮		✖	◆▮▲✖	◆▮▲			◆▮▲		◆▮								
	◆▲	◆▲	◆▲	◆▲	◆▲		◆					◆		◆	◆								
	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆							
	◆▲	◆		◆▮▲	◆▮▲	◆▮▲		◆▲	▲	▲	▲	▲	▲		◆▲	◆							
◆▮		◆▮					◆▮	◆▮	◆▮		◆▮	◆▮	◆▮	◆▮	◆▮	◆▮			●	●			
																			●	●			
◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮▲	◆	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮	◆							
	◆▲	◆▲	◆▲	◆▲	◆▲	◆▲	◆▲		◆▲	◆▲	◆▲	◆▲	◆▲	◆▲	◆▲	◆▲			●				
◆▲		◆▲	◆▲	◆▲	◆▲	◆▲			◆▲	◆▲	◆▲	◆▲	◆▲	◆▲	◆▲				●				
◆							◆	◆	◆	◆▮	◆	◆	◆										
◆	◆	◆	◆	◆	◆		◆	◆			◆	◆		◆		◆							
							◆	◆						◆▮	◆▮	◆▮		●					
	◆▮	◆▮	◆▮	◆▮		◆▮	◆▮	◆▮		◆▮						◆▮							
◆	◆▮	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆			●	●			
		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲			◆▮▲	◆▮▲	◆▮▲	◆▮▲							
	◆	◆	◆	◆	◆		◆	◆		◆	◆	◆	◆	◆	◆	◆							
◆		◆	◆	◆		◆				◆	◆	◆		◆	◆		●			●			
							◆	◆															
								◆										●					
							◆			◆			◆	◆✖				●	●	●			
	◆▮	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲		◆▮			◆▮▲		◆▮▲	◆▮	◆▮▲						●		
	◆	◆	◆	◆			◆							◆	◆			●	●				
◆▮▲		◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆▮▲	◆	◆▮	◆▮▲✖	◆▮▲✖	◆▮▲✖	◆▮▲✖	◆▮▲✖		◆	◆							

Consultez le site web, qui peut comporter des mises à jour : www.solutions-numeriques.com/securite/annuaire-cybersecurite/. L'éditeur ne peut pas garantir l'exactitude des informations et décline toute responsabilité.

AvantdeCliquer.com

L'humain au cœur de la cybersécurité

PROTÉGEZ-VOUS EFFICACEMENT DES CYBERATTAQUES



80% DES CYBERATTAQUES ONT POUR ORIGINE UN E-MAIL FRAUDULEUX

conçus / hébergés / développés en FRANCE

- Lauréat de l'intelligence économique
- BPI France — Solution pertinente pour sensibiliser les utilisateurs à la cybersécurité
- Finaliste du prix de l'innovation du Salon des Maires et des Collectivités Locales
- Lauréat de l'Innovation SANTEXPO — Transformation Digitale & Cybersécurité (santé)

FRANCE CYBER SECURITY

www.avantdecliquer.com

Comprendre

La technologie et les méthodes

Par Jérôme Saiz et Alain Clapaud

- Définitions : Buzzword
- Attaque par déni de service (Denial-of-service attack)
- Cybersécurité industrielle (OT)
- Cyber-assurance
- Contrôle d'accès et gestion des identités
- Threat Intelligence
- DevSecOps, la transformation digitale des DSI
- Protection du poste de travail
- Protection des terminaux mobiles
- Protection de la donnée
- Protection applicative
- Audit d'architecture
- SOC
- Tableaux de bord de sécurité
- SIEM

Buzzword

Ransomware

Un « ransomware » ou rançongiciel est un malware dont le mode de fonctionnement passe par le chiffrement des données de l'utilisateur afin de lui extorquer une somme d'argent contre la clé de déchiffrement. L'attaquant réclame la rançon sous forme de cryptomonnaies afin de ne pas être identifié par les autorités. La rançon varie de quelques centaines voire quelques milliers de dollars à plusieurs millions de dollars, en fonction de la taille de la cible. Une entreprise peut voir une large partie de son parc de postes utilisateurs infectés, voire des serveurs critiques, certains ransomware peuvent réaliser ce que l'on appelle des déplacements latéraux d'un poste à un autre. Certains cherchent notamment à rendre inutilisables les serveurs de backup afin de ne laisser aucune autre alternative à la victime que de payer pour récupérer ses données. Cependant, verser la rançon ne constitue en rien une garantie que la clé qui sera fournie soit efficace et permettra de déchiffrer le contenu des disques durs. De même, une entreprise attaquée, qu'elle paye ou non la rançon, doit immédiatement renforcer sa sécurité car rien ne lui garantit de ne pas être attaquée une seconde fois.

S'il est communément admis que le ransomware est apparu pour la première fois en 1989 avec le cheval de Troie baptisé AIDS, « Aids Info Disk » ou encore PC Cyborg Trojan qui s'installait dans le fichier AUTOEXE.BAT de MS/DOS, ce mode d'attaque s'est très largement développé à partir de 2012 comme le notait alors le bureau d'enregistrement des plaintes du FBI (Internet Crime Complaint Center / IC3). Depuis, l'industrie du ransomware s'est structurée et on a vu émerger des offres de type « Ransomware as a Service », où un utilisateur lambda sans connaissances techniques spécifiques peut commander en ligne une attaque s'appuyant sur des ransomware prêts à l'emploi.

Outre une protection renforcée des postes clients et des serveurs notamment au moyen de solutions de protection endpoint Next-Gen ou de solution de type EDR, la parade contre une attaque de ransomware consiste à mettre en place des solutions de sauvegarde des données efficaces et surtout à l'abri des attaquants. C'est le seul moyen de reconstituer un système d'information après une attaque en limitant au maximum les pertes de données. ■

A.C.

« Zero Trust »

L'architecture « Zero Trust », appelée aussi ZTNA (Zero Trust Network Architecture) correspond à un modèle de sécurité post-périmétrique. Celui-ci est basé sur la notion qu'il ne faut pas accorder de confiance par défaut à un terminal se connectant au réseau de l'entreprise quelle qu'en soit sa nature. Même si un terminal est connecté sur le réseau interne de l'entreprise, celui-ci doit faire l'objet de contrôle de sécurité pour s'assurer que le poste ne va pas être utilisé à des fins malveillantes. Le niveau de contrôle et les droits d'accès qui vont être accordés au poste qui se connecte vont varier en fonction de la situation dynamique de celui-ci. Les contrôles vont être particulièrement renforcés lorsque l'utilisateur souhaite se connecter au système d'information depuis une chambre d'hôtel à l'étranger, depuis un accès Wi-Fi public d'un aéroport ou son domicile.

On associe l'essor de ce modèle de sécurité au développement des utilisateurs nomades et au télétravail généralisé qui voit de plus en plus de collaborateurs vouloir accéder à des ressources IT de l'entreprise hors des locaux. La paternité du terme est attribuée à John Kindervag, analyste chez Forrester en 2009 mais ses concepts de base remontent au début des années 2000.

Le niveau de sécurité apporté par le modèle « Zero Trust » s'appuie sur 3 grands principes : D'une part, il ne faut systématiquement accorder aux utilisateurs et aux machines que des droits minimums, ne jamais faire confiance par défaut et toujours vérifier et monitorer systématiquement. Cette vérification s'appuie sur des données techniques telles que la nature du poste de travail, ses logiciels installés, son hardware, le réseau mis en œuvre, mais aussi sa géolocalisation et, bien évidemment, les moyens d'authentification qui vont être utilisés par l'utilisateur afin de lui accorder ou refuser des droits d'accès aux ressources IT de l'entreprise. La montée en puissance des services de sécurité dans le Cloud et des technologies d'Intelligence Artificielle a permis d'étendre les contrôles réalisés dynamiquement sur les accès, notamment afin d'analyser en temps réel le comportement des utilisateurs. ■

A.C.

Bug Bounty

Qui mieux qu'un hacker peut juger du niveau de sécurité d'une application ou d'un service Internet ? Des prestataires aident aujourd'hui les entreprises à organiser des campagnes de Bug Bounty pour trouver leurs failles de sécurité.

Le Bug Bounty vise à mettre en contact une entreprise qui souhaite vérifier le niveau de protection de ses développements avec des hackers éthiques qui vont chercher les failles. Ceux-ci décrochent des primes pour chaque nouvelle faille découverte, le montant étant généralement calculé en fonction de sa criticité. Les campagnes de Bug Bounty viennent se placer en aval de tous les outils de contrôle du code DevSecOps et des audits de sécurité. L'intérêt de cette approche comparée à l'audit de sécurité classique est de pouvoir diversifier les tests réalisés. Les auditeurs s'appuient généralement sur des outils bien connus et consacrent un nombre d'heures prédéfini à l'avance pour réaliser leur étude. Si les hackers éthiques vont exploiter des outils de test bien connus de la communauté, ils vont aussi essayer des méthodes plus « out of the box » afin de trouver la faille que personne ne va détecter et décrocher une plus grosse prime. Les hackers éthiques ne vont pas nécessairement compter leurs heures si le défi qui leur est présenté est intellectuellement (et financièrement) intéressant.

Si les quelques géants du Web peuvent organiser eux-mêmes des campagnes de Bug Bounty pour tester leurs services, toutes les entreprises n'ont pas l'aura qui va leur permettre d'attirer l'attention des hackers éthiques dont beaucoup conservent un certain anonymat. Des prestataires spécialisés en Bug Bounty apportent des solutions « clé en main » à toute entreprise souhaitant mettre en place une campagne de ce type. Celles-ci disposent déjà d'un vivier de hackers éthiques à qui elles proposent régulièrement des défis. Autre atout majeur de ces offres « packagées », le prestataire prend à sa charge tout le volet distribution des primes, ce qui met à l'abri l'entreprise d'éventuelles contestations quant à l'importance de la trouvaille réalisée par le hacker.

A.C.

Chiffrement post-quantique

Les futurs ordinateurs quantiques seront potentiellement capables de déchiffrer de nombreux algorithmes couramment exploités aujourd'hui, raison pour laquelle il faut préparer dès aujourd'hui leur arrivée.

Si les ordinateurs quantiques restent encore essentiellement des démonstrateurs aux capacités limitées, d'ici quelques années, quelques décennies des machines bien plus puissantes devraient faire leur apparition sur le marché. Les services de renseignements seront certainement les premiers dotés car ces machines leur offriront les moyens de déchiffrer des codes considérés aujourd'hui comme inviolables. Il faudra alors changer d'algorithme et aller vers des algorithmes dits post-quantiques, c'est-à-dire capables de résister à ces machines hors normes. Cette problématique peut sembler lointaine : à quoi bon changer d'algorithmes pour sécuriser une transaction bancaire ; D'ici 10 ans le numéro de carte bancaire ne sera plus valable. Pour certains secrets, l'arrivée d'ordinateurs quantiques dans 10, 20 ou même trente ans reste problématique. Intercepter aujourd'hui la communication chiffrée des plans d'un porte-avion ou d'un futur avion de combat peut-être intéressant pour un gouvernement étranger car ces systèmes d'armes seront toujours en service dans 30 ans.

L'algorithme conçu par le mathématicien Peter Shor est capable d'exploiter les capacités d'un calculateur quantique afin de factoriser des entiers, donc de retrouver la clé de chiffrement d'un algorithme de type RSA. Les futurs ordinateurs quantiques constituent une réelle menace sur bon nombre d'algorithmes de chiffrement actuels. C'est la raison pour laquelle le NIST a lancé dès 2016 une vaste compétition mondiale afin d'inviter les chercheurs à créer des algorithmes qui resteront inviolables lorsque les ordinateurs quantiques suffisamment puissants seront une réalité. La compétition en est à son 4ème tour et se rapproche de sa finalité : publier les algorithmes post-quantiques qui s'imposeront comme les standards de la cryptographie pour les prochaines décennies.

A.C.

Buzzword

Gestion du Risque Cyber

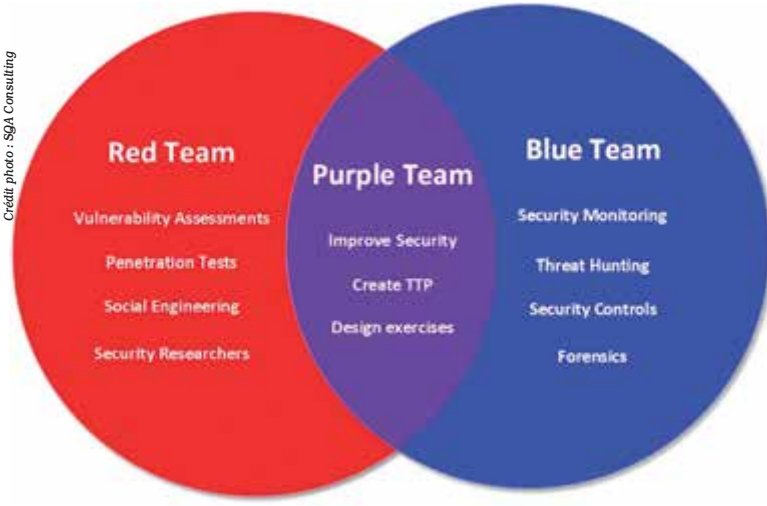
La gestion du risque cyber s'industrialise. Des plateformes permettent de gérer tous les aspects de la gestion de ce risque très particulier, depuis la cartographie des risques, la mesure et l'exécution des plans de traitement.

La gestion du risque est une approche très commune dans l'industrie. Les Risk Manager disposent de plateformes où ils vont cartographier et référencer l'intégralité des risques auxquels sont soumises leurs installations industrielles. Elles permettent de référencer en face de chacun d'eux les moyens techniques, humains et processus mis en place pour le « traiter ». Cette approche de gestion du risque a été transposée dans de multiples domaines, dont la cybersécurité. Plusieurs solutions de gestion du risque cyber ont ainsi été commercialisées ces dernières années. Certaines solutions sont clairement orientées technique et apportent une solution opérationnelle pour gérer la posture de sécurité vis-à-vis des ressources Cloud, par exemple, ou des accès.

D'autres catégories de solutions sont beaucoup plus orientées processus. Les solutions de gestion de risque traditionnelles ont en quelque sorte ajouté un nouvel onglet Cybersécurité à leurs domaines d'expertise existants, comme ils ont pu le faire il y a quelques années pour traiter les risques environnementaux par exemple. L'atout de cette approche est bien évidemment pour l'entreprise de disposer d'une plateforme unique pour gérer l'intégralité de ses risques. Tous les gestionnaires de risques, les utilisateurs métiers vont concentrer leur expertise sur un même outil, un « super ERP » du risque. Le revers de la médaille de l'approche reste le manque d'outils spécifiques liés à la nature même du risque cyber.

Une offre typée cybersécurité va ainsi fournir des outils de cartographie automatisée des ressources IT, implémente des calculs du niveau de risque, génère automatiquement des rapports synthétiques. Ces outils implémentent les normes ISO 27 005, ISO 21 434 ainsi que, pour certains, la méthodologie poussée en avant par l'ANSSI en France depuis 2018, la méthodologie EBIOS. ■

A.C.



Crédit photo : SGA Consulting

Red / Blue / Purple Team

L'organisation de simulation d'attaques par des attaquants « éthiques », la Red Team et l'équipe de défense (Blue Team) est une technique désormais bien connue pour vérifier l'efficacité d'un SOC.

Le rôle d'une Red Team est aujourd'hui bien connu : il s'agit de consultants, éventuellement de hackers éthiques qui vont attaquer le système d'information d'une entreprise afin d'en déceler les failles et surtout mettre à l'épreuve les processus internes de défense. L'idée est de mener des tests de pénétration et d'analyser la création du personnel de l'entreprise et de son équipe de sécurité qui joue alors le rôle des bleus, la Blue Team. Selon le niveau de surprise souhaité, le camp bleu peut être prévenu ou pas de l'imminence de l'exercice.
C'est un bon moyen de tester à la fois l'efficacité d'un SOC en termes de détection, mais aussi la réactivité des équipes internes dès lors que l'attaque leur est signalée. Si on pense souvent à des moyens techniques d'intrusion, la Red Team peut tout aussi bien mener des actions d'ingénierie sociale auprès du personnel pour extorquer un mot de passe, obtenir un accès au système d'information.

Vers une approche plus collaborative de la simulation d'attaques

Plus récente, la notion de Purple Team est apparue afin de transformer cet affrontement en un travail plus collaboratif entre attaquants et défenseurs : l'objectif est de créer lors de l'exercice les règles qui permettent d'éradiquer les attaques qui ont réussi à passer le rideau de défense. La Purple Team analyse les résultats, supervise les corrections à apporter. Cette évolution des simulations d'attaques vise à faire bénéficier l'entreprise de retours beaucoup plus constructifs qu'un simple rapport d'attaque et profiter des forces en présence pour améliorer significativement sa posture de sécurité. ■

A.C.

Ingénierie sociale / Social Engineering

La boutade est désormais bien connue : La première faille de sécurité se situe entre le clavier et l'écran. Elle n'en reste pas moins vraie. Miser à 100% sa sécurité sur des moyens techniques est illusoire. Il faut former et entrainer le personnel en permanence aux enjeux de la Cyber Sécurité.

Il est acquis que l'élément humain est souvent à l'origine de nombreuses attaques informatiques. L'efficacité des campagnes de Phishing et des ransomwares est relative, avec quelques clics sur des milliers de messages expédiés, mais elle est bien réelle.
Outre les indispensables moyens de protection technique, les nouveaux algorithmes d'intelligence artificielle, il faut former les employés à ce qu'il doivent faire en cas d'email, de SMS ou même d'appel téléphonique suspect. Les attaquants usent de toutes les ficelles pour obtenir un mot de passe ou même initier un transfert d'argent comme l'arnaque au président l'a démontré voici quelques années.
L'essor de technologie comme le Deep Fake rend tout à fait concevable l'appel d'un PDG plus vrai que nature sur Teams ou Zoom alors qu'il s'agit en fait d'un attaquant…
Face à cette menace avérée, la réaction la plus logique consiste à mener des sessions de sensibilisation en présentiel ou à distance afin de présenter les différents moyens utilisés par les attaquants et quelle doit être la conduite à tenir devant toute demande menaçant de manière plus ou moins évidente la sécurité de l'entreprise.
Des Serious Games peuvent aussi être organisés pour rendre ces cessions de formation plus interactives et augmenter leur efficacité. Il est aussi possible de simuler des attaques sur la messagerie de l'entreprise afin de vérifier l'efficacité de ces formations.

Des solutions de type Threat Coaching ou Phishing Coaching existent pour mener ces attaques internes et surtout exploiter les résultats pour proposer des actions de formation complémentaire auprès de ceux qui sont tombés dans le panneau. ■

A.C.

SASE

SASE s'est imposé ces dernières années comme le modèle de sécurité venu du Cloud. Acronyme de « Secure Access Service Edge », le concept SASE a été formalisé pour la première fois par le cabinet Gartner afin de définir une sécurité réalisée au niveau d'une plateforme Cloud qui assure tant des fonctions d'accès que de sécurité réseau. SASE comprend d'une part une série de services de sécurité délivrés par le fournisseur de sécurité et se voit allié à une offre de type SD-WAN. L'objectif pour l'entreprise est bien de s'appuyer sur de simples accès Internet pour se constituer un WAN virtuel intégrant tous les services nécessaires à la sécurisation des accès et des flux réseaux.

Parmi les services de sécurité les plus courants délivrés par les offreurs de services SASE, on trouve la notion de Secure Gateway (SWG). Cette passerelle de protection intègre un Firewall as a Service qui offre des services de filtrage d'URL, une fonction de détection d'intrusion (IPS). En outre, la puissance de traitement du Cloud permet aux fournisseurs de proposer une inspection du trafic chiffré SLL à grande échelle.
De plus, des fonctions liées à la protection endpoint sont intégrées aux principales offres SASE, avec une protection antimalware de type Next-Gen Anti-Virus (NGAV) ou encore un service de Managed Threat Detection and Response (MDR) afin de détecter les postes compromis. Ces fonctions permettent aux fournisseurs de services SASE de se positionner en tant que conformes à l'approche « Zero Trust » mais les deux notions ne doivent pas être confondues. On peut déployer une approche « Zero Trust » sans nécessairement basculer dans SASE.

Cette synergie entre services de sécurité Cloud et réseau SD-WAN représente une évolution majeure dans la façon dont les entreprises vont gérer leurs backbone réseau, mais aussi leur cybersécurité. Les coûteux liens MPLS vont faire la place à de simples liaisons Internet pour se connecter aux opérateurs SD-WAN. Pour la gestion opérationnelle de la sécurité, l'approche SASE est certainement une nouvelle étape dans l'externalisation de la cybersécurité : toute l'exploitation des briques de sécurité est assurée par le fournisseur SASE qui s'appuie généralement sur les datacenters des hyperscalers Cloud. Les RSSI de l'entreprise peuvent se concentrer sur la gestion de la sécurité et les nouveaux projets. ■

A.C.

Attaque par déni de service - DDoS

(Denial-of-service attack)

Submerger un service Internet sous le nombre des requêtes est sans doute le moyen le plus simple pour faire tomber un service. Les attaquants entretiennent de vastes réseaux de botnet sur des PC ou même des objets connectés pour pouvoir lancer ces attaques qui prennent aujourd'hui une ampleur considérable.

Dans une attaque de type déni de service, l'objectif initial est de mettre hors ligne un service Cloud, une API ou un site Web tout simplement en les saturant de requêtes. Face à une avalanche soudaine de requêtes, les serveurs saturent et commencent à émettre des messages d'erreur, ce qui rend le service visé inaccessible pour les véritables utilisateurs. Il s'agit généralement d'attaques DDoS (Distributed Denial-of-Service) car l'attaquant génère sa charge au moyen de milliers d'ordinateurs zombies. Des bots patiemment mis en place pendant des mois vont générer les requêtes d'attaque le jour J. Cette approche massive est aujourd'hui nécessaire pour faire tomber un site, car les défenseurs mettent en place diverses techniques pour contrer ces attaques. Outre les caches qui soulagent les serveurs, ceux-ci placent des filtres pour écarter les requêtes réseau considérées comme hostiles. Ils peuvent aussi s'appuyer sur un fournisseur de CDN (Content Delivery Network) qui va pouvoir absorber l'attaque beaucoup plus facilement grâce à son architecture réseau mondiale.

Dans ce jeu du chat et de la souris entre attaquants et défenseurs, on assiste à une inflation de l'ampleur de ces attaques. Le 1er juillet 2022, Google a annoncé avoir bloqué une attaque qui a culminé à 46 millions de requêtes par seconde, soit 76% de plus que le précédent record enregistré par Cloudflare le 14 juin 2022 avec 26 millions de requêtes par seconde. De telles attaques ont pour finalité de pénaliser un concurrent commercial, mais peuvent aussi donner lieu à une demande de rançon par l'attaquant. Elles peuvent aussi faire partie d'une stratégie d'attaque plus large, l'attaque DDoS n'étant qu'une partie visible de l'attaque, les pirates réalisant une infiltration plus discrète au moment même où l'équipe de sécurité tente de résoudre le déni de service. ■

A.C.

Cybersécurité industrielle (OT)

De plus en plus connectés à l'IT, les systèmes industriels représentent une cible très tentante pour un attaquant. Toute immobilisation d'un site industriel représente un manque à gagner énorme pour l'industriel. C'est la promesse d'une énorme rançon pour le pirate si son attaque aboutit.

Longtemps les systèmes industriels, baptisés OT (Operational Technology) par opposition à IT, ont été maintenus isolés du reste de l'informatique d'entreprise et, a fortiori, d'Internet pour des raisons de sûreté de fonctionnement. L'essor du mouvement « Industrie 4.0 » a remis en cause cette approche. Les ateliers de production ont été de plus en plus connectés au Big Data pour l'optimisation des processus, des données sont échangées avec des prestataires spécialisés via Internet pour réaliser de la maintenance prédictive ou du dépannage à distance. Ces nouveaux usages ont fait naitre le besoin impérieux de renforcer la sécurité de l'OT, ce qui a donné naissance à de nouvelles solutions de sécurité adaptées à ce marché.

En effet, sécuriser l'OT pose des enjeux très spécifiques au monde industriel. D'une part, celui-ci exploite ses propres protocoles réseaux pour permettre, par exemple, à un automate de piloter une machine outil. Regroupés sous l'acronyme SCADA (Supervisory Control And Data Acquisition), de multiples protocoles spécifiques cohabitent sur les réseaux industriels. Il est nécessaire de disposer de sondes réseau et de firewalls aptes à analyser ces protocoles spécifiques. Ce support de ces protocoles spécifiques est nécessaire pour réaliser du Deep Packet Inspection sur les flux réseaux industriels et détecter une éventuelle attaque. Une autre particularité du monde industriel est l'incapacité pour une entreprise de déployer les logiciels qu'elle souhaite sur ses équipements industriels. Les fabricants d'équipement refusent que l'intégrité logicielle de l'équipement soit affectée : impossible d'installer un anti-ransomware ou un logiciel quelconque sans perdre la garantie fournisseur. Des solutions sont apparues pour scanner les machines depuis une simple clé USB, respectant ainsi les contraintes fixées par les constructeurs. ■

A.C.

Cyber-assurance

Dans un contexte où les cyber-attaques contre les entreprises ne cessent de s'accroitre, la notion d'assurance cyber semble une évidence. De nombreux grands-comptes ont franchi le pas. Reste à diffuser cette couverture du risque cyber plus largement dans les entreprises françaises.

Le manifeste publié par Hexatrust en septembre 2020 explicitant 5 vœux pour une autonomie numérique pour l'Europe défend l'idée d'une Europe de la cybersécurité, d'un plan d'équipement cyber et un dispositif de soutien aux PME du secteur. Il inclut aussi un volet dédié à la cyber-assurance. Les auteurs du manifeste militent en faveur d'une couverture assurantielle du Cyber-risque, notamment afin de permettre aux TPE et PME de franchir le pas et se protéger enfin du risque cyber.

Des contrats très spécifiques

En attendant qu'une telle idée chemine, les contrats d'assurance cyber actuellement proposés sont souvent très spécifiques à l'entreprise. Souscrire à un contrat souvent complexe est un processus long qui exige une implication plus forte non seulement de la part du DSI et du RSSI, mais également du Risk Manager, du responsable assurances, du CIL (et bientôt Data Privacy Officer !), et potentiellement du responsable juridique ou de la RH. Il s'agit donc d'un projet très engageant qui doit être mené comme tel, notamment en créant une équipe pluridisciplinaire dédiée pour le mener à bien.
L'étape la plus structurante d'un tel projet est de loin la réponse au questionnaire d'assurance : l'entreprise va devoir y exposer son organisation et préciser à la fois les mesures de protection existantes mais aussi ses plans de réponse en cas de sinistre. C'est pourquoi bien que nous ayons choisi de placer cette étape assurantielle en début de processus, durant la phase d'organisation, elle exige toutefois qu'un premier travail de fond ait déjà été réalisé, tant en matière de cartographie des risques que de réponse aux incidents.
Idéalement, et puisque nous présentons la sécurité telle un processus itératif, le volet assurantiel sera donc traité au second passage par cette phase d'organisation.

Une couverture en trois volets

En cas de déclenchement d'une crise, le contrat d'assurance cyber couvrira l'entreprise sur trois volets principaux :
• Tout d'abord en prenant en charge les frais de réponse à incident et de gestion de crise (honoraires de consultants et de prestataires dans les domaines légaux, forensiques, de la communication, etc.).
• Ensuite un second volet pourra être activé en cas de réclamation de tiers à l'encontre de l'entreprise, qu'il s'agisse de clients ou d'employés. Celle-ci, en effet, pourra être mise en cause pour négligence ou non-respect de ses obligations légales et devra répondre juridiquement, ce qui entraînera des frais.
• Enfin, l'assurance pourra prendre à sa charge les frais supplémentaires induits par la poursuite de l'activité durant le sinistre, tels que la location de nouveaux locaux, de nouveaux équipements informatiques, le recours à des sous-traitants pour tenir ses engagements, etc.
A noter : le contrat d'assurance pourra également prendre en charge les frais spécifiques liés à une attaque par un ransomware, qu'il s'agisse de rembourser les frais d'un consultant en sécurité chargé de négocier avec les pirates, ou bien la rançon elle même (y compris les frais bancaires si l'entreprise a dû emprunter !). Bien entendu, et à la suite des grandes campagnes de ransomware durant 2017, ces primes spécifiques peuvent être élevées tant le risque est désormais fort.

Des clauses secrètes

Certaines clauses d'une police de cyber assurance doivent rester secrètes sous peine d'être nulles. C'est notamment le cas de la clause de protection contre les ransomwares (clause de cyber extorsion). Cela implique, pour l'entreprise, d'être en mesure de créer un groupe de travail "cyber-assurance" dont l'activité restera secrète vis-à-vis des autres collaborateurs. Seules les personnes-clés de l'entreprise pourront être mises au courant et généralement seulement au moment du déclenchement de la crise.
Au moment de la crise l'assureur sera souvent le premier partenaire extérieur alerté. Il permettra à l'entreprise de bénéficier d'une assistance immédiate pour la suite des opérations. Viennent ensuite généralement le temps des notifications légales, par exemple auprès de la CNIL s'il s'agit d'un vol de données personnelles ou des autorités si l'entreprise jouit d'un statut particulier (Opérateur d'Importance Vitale, entreprise de défense, etc.).
Dans tous les cas, l'assureur sera impliqué dès le début de la crise et jusqu'à sa résolution, ce qui en fait un partenaire de premier plan de l'entreprise. A ne pas négliger, donc! ■

J.S.

Contrôle d'accès et gestion des identités

La généralisation du Cloud Computing dans les entreprises fait voler en éclat la notion d'identité telle qu'on la connaissait. Celle-ci devient désormais le pivot central des ressources IT de l'entreprise dans un nouveau modèle formalisé en 2020 par le Gartner sous l'acronyme de SASE (Secure Access Service Edge).

Ce n'est pas un hasard si la métaphore de la serrure revient sans cesse dans le monde de la SSI : contrôler les accès au système d'information est au cœur du besoin de protection de l'entreprise. Ce marché est en réalité pluriel : il y a en effet bien peu de similitudes entre une solution individuelle de gestion des mots de passe que l'on installe sur son poste de travail (un « coffre-fort » à mots de passe) et une solution d'IAM (Identity & Access Management) ou de NAC (Network Access Control) déployée dans l'entreprise. Voici donc un aperçu des grands types de solutions de contrôle d'accès que vous pourrez déployer :

• **Les outils de gestion des mots de passe** (de type Single Sign-On par exemple). Installées sur le poste de travail ces solutions permettent de stocker de manière fiable de nombreux mots de passe et de les renseigner automatiquement au moment de la connexion ou de l'accès aux ressources protégées (sites web, applications internes, etc.). Ils sont largement conseillés à la place de la fonctionnalité équivalente proposée par les navigateurs web, bien moins sécurisés. En outre, ces outils offrent d'autres fonctionnalités bien utiles : enregistrer d'autres informations sensibles (numéros de cartes bancaires, par exemple), synchronisation via le Cloud afin de pouvoir utiliser ses mots de passe sur plusieurs ordinateurs, supports pour les navigateurs mobiles avec la même solution, etc.

• **Les solutions d'infrastructure.** Il s'agit ici des solutions qui vont contrôler l'accès au réseau, que ce soit localement (notamment via une borne Wifi) ou à distance (à travers un tunnel VPN). Pour les postes de travail internes, le contrôle d'accès est le plus souvent délégué à un contrôleur de domaine Microsoft Active Directory ou un annuaire similaire.

• **L'authentification forte.** Le marché de l'authentification forte offre des outils (souvent physiques, mais aussi virtuels, sur téléphone mobile) destinés à renforcer l'authentification par mot de passe, jugée insuffisante. Il s'agit d'une mesure de sécurité essentielle, tant les mots de passe peuvent être aisément dérobés et réutilisés.
L'ajout d'un second facteur (physique, par SMS ou sous la forme d'un code virtuel généré par le téléphone mobile via une application de One Time Password comme le Google Authenticator ou équivalent) vient considérablement renforcer le niveau de protection.
A choisir, mieux vaut opter pour un dispositif physique de type YubiKey ou équivalent (Google Titan Key par exemple), qui ne souffre pas des récentes vulnérabilités découvertes dans l'usage des SMS (qui ont tendance à être écartés) et permet, contrairement à un jeton virtuel de type One Time Password généré par une application mobile, d'authentifier le site visité, afin de limiter également le risque de phishing.

• **Les solutions d'infrastructure avancées.** Le NAC (Network Access Control) permet de prendre des décisions d'accès en fonction de l'identité du poste client, de son état (dispose-t-il de toutes ses mises à jour ? Son antivirus est-il activé ?) et de son comportement (détection d'un changement d'adresse MAC suspecte, par exemple). Ce marché, qui a mis du temps à décoller, a été popularisé par Cisco puis Microsoft, mais il est désormais également servi par d'autres acteurs du monde du réseau et des pure players. Un projet NAC est souvent assez long et structurant, mais il apporte une véritable amélioration du niveau de sécurité de l'entreprise, tout en offrant une plus grande souplesse dans l'accueil des visiteurs (en mettant à leur disposition un réseau réservé, par exemple)

• **Les solutions d'IAM** (Identity & Access Management). Projets structurants s'il en est, les chantiers d'IAM visent à optimiser la gestion des accès et des droits des collaborateurs en fédérant en un endroit unique les informations d'identités réparties jusqu'à présent au sein des multiples référentiels de l'entreprise (dans chaque application métier, par exemple)
Il s'agit d'une approche non seulement technique (provision automatique des comptes et destruction au moment du départ, par exemple), mais aussi organisationnelle (définition de rôles métiers spécifiques, suivi du cycle de vie de l'identité, gestion des habilitations multiples et réhabilitations, etc.).

• **La gestion des identités et des accès privilégiés** (PIM). Un marché de niche, mais essentiel, qui se focalise sur les droits d'accès des administrateurs. Une étude récente de l'éditeur Centrify indique d'ailleurs que 74% des intrusions réussies durant l'année 2018 sont passées par le vol d'un accès privilégié. Et pourtant, selon la même étude, 65% des entreprises reconnaissent encore partager au moins un compte administrateur ! L'installation d'un bastion d'administration constitue donc une mesure urgente pour les entreprises qui ne l'auraient pas encore fait.

• **Les infrastructures à clés privées** (PKI). Également très structurants, les projets de PKI permettent à l'entreprise d'émettre et de gérer les certificats numériques utilisés par ses dispositifs d'authentification (dont les cartes à puce). Jadis en perte de vitesse, ces projets connaissent désormais un regain d'intérêt grâce aux objets connectés, où l'authentification mutuelle et le chiffrement à très grande échelle seront une nécessité à terme. En dehors de ce cas d'usage particulier, un projet de PKI permet à l'entreprise de généraliser l'usage de l'authentification par certificats sur l'ensemble de son SI (utilisateurs, applications, machines…) et le chiffrement. Ce n'est pas pour tout le monde, mais une PKI peut apporter une grande simplification dans les processus de chiffrement et d'authentification au sein de l'entreprise.

L'identité dans le nuage

Le Cloud s'est imposé comme un facteur majeur de restructuration du marché du contrôle d'accès. La majeure partie des applications d'entreprises, du CRM à la gestion RH, en passant par la messagerie et la suite bureautique, ont basculé en mode SaaS. Peu adaptés au Cloud, les outils de contrôle d'accès habituels doivent donc être complétés par les CASB (Cloud Access Security Brokers), qui permettent de contrôler de manière centralisée l'accès aux applications Cloud (métier et grand public) quelle que soit l'origine de la requête (depuis le réseau interne de l'entreprise ou à l'extérieur) et le poste de travail utilisé (un poste géré par l'entreprise, un ordinateur personnel ou même un smartphone). Les CASB redonnent ainsi au service informatique de la visibilité sur l'usage des applications externalisées.

Les grandes tendances

Le tableau suivant présente quelques tendances à suivre sur le marché du contrôle d'accès et de la gestion des identités. ■

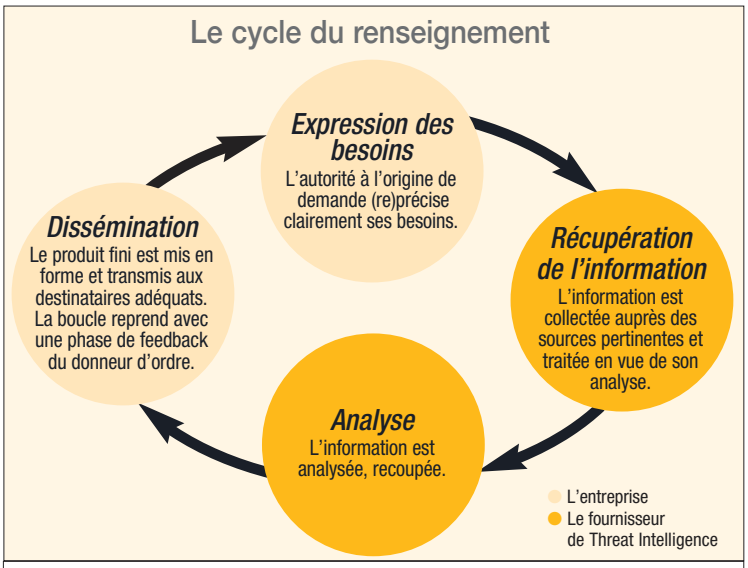
J.S.

SMS	Si jusqu'à présent l'utilisation d'un SMS envoyé sur un téléphone mobile pouvait faire office de second facteur d'authentification, cela ne sera bientôt plus le cas et vous devriez commencer à prévoir de ne plus y avoir recours. Les dernières attaques révélées contre le protocole de signalisation GSM ont démontré la vulnérabilité accrue des SMS à l'interception. En outre, si un code reçu par SMS permet bien de renforcer le mot de passe associé, il ne fait rien pour aider à authentifier le site en question, ne réglant donc pas la question du risque de phishing.
Mobile	L'usage du mobile comme outil d'authentification est l'une des tendances de l'année 2019, avec de plus en plus de services web qui supportent des applications de type OTP (telles que le Google Authenticator). Ces applications sont généralement gratuites, compatibles avec tous les sites qui proposent ce type d'authentification, et sont largement plus sûres que l'usage du code SMS.
Gestion des identités	Investissez dans la gestion des identités, car ces dernières sont là pour rester. À l'avenir, de nombreuses solutions de sécurité pourront intégrer la notion d'identité dans la prise de décision sécurité. Autant anticiper ! Les plateformes de gestion des identités peuvent être internalisées, mais aussi proposées en mode SaaS. L'on parle alors d'IaaS, pour « Identity as a Service » (à ne pas confondre avec « Infrastructure as a Service »)
Multifacteur	Cela fait des années que les spécialistes appellent de leurs vœux la fin du mot de passe simple ! Sous la pression de nombreux acteurs du web (notamment les GAFA), l'authentification forte à plusieurs facteurs se démocratise. C'est le moment d'y réfléchir si ce n'est pas déjà fait ! En 2019, la populaire YubiKey a désormais un concurrent avec la Google Titan Key proposée par Google.
Cloud	Les CASB (Cloud Access Security Brokers) permettent de contrôler de manière centralisée l'ensemble des accès aux applications dans le Cloud, qu'il s'agisse d'applications métiers (CRM, gestion des congés, des notes de frais...) ou personnelles (Dropbox, notamment). Pour l'utilisateur ces solutions apportent une simplicité d'usage (toutes les applications sont accessibles depuis un portail unique, authentification transparente), et pour l'entreprise un meilleur contrôle des accès.
SASE	Le nouveau modèle d'architecture de sécurité SASE est une conséquence directe des nouveaux usages de l'IT. Les entreprises optent de plus en plus pour des applications Saas et des services Cloud que les utilisateurs consomment non plus seulement derrière les murs de l'entreprise, mais aussi en situation de mobilité ou en télétravail. L'identité devient la clé de voûte d'une architecture qui met en œuvre des solutions telles que les CASB, les passerelles Web sécurisées et CDN, les technologies de DLP.

Threat Intelligence

La Threat Intelligence promet une veille et une analyse des menaces émergentes afin d'aider les entreprises à mieux anticiper.

Les prestataires de renseignement sur la menace (« Threat Intelligence ») collectent de l'information brute sur les cyber-menaces, les associent, les analysent et livrent à leurs clients des informations enrichies qui les aident à orienter leur stratégie de sécurité.
La matière première de ce type de service n'est pas nouvelle : à l'image de Monsieur Jourdain les (bons) éditeurs d'antivirus font de la Threat Intelligence pour leur propre compte depuis toujours ! Leurs chercheurs suivent l'activité des groupes de pirates de premier plan et documentent l'évolution de leurs capacités techniques, l'émergence de nouvelles techniques et de nouvelles menaces. Cela fait partie de leur coeur de métier.
Ce qui est nouveau, en revanche, c'est l'émergence d'un marché pour ce type d'information (voir encadré).



Dans le monde du renseignement, la collecte, l'analyse et l'exploitation du renseignement suit un cycle formel. L'entreprise devra le comprendre si elle souhaite tirer tous les bénéfices d'une solution de Threat Intelligence digne de ce nom.

Une exigence de maturité

Mais aussi séduisante soit-elle sur le papier, la Threat Intelligence exige de l'entreprise une véritable implication afin d'en tirer tous les bénéfices. Le cycle du renseignement (voir illustration) donne une bonne idée des responsabilités partagées entre le client et son fournisseur de Threat Intelligence.
Si l'on s'en tient à ce modèle, le fournisseur est responsable de la collecte et de l'analyse (étape 2 et 3) tandis que l'entreprise doit être capable de déterminer précisément ce qu'elle attend du service (étape 1) et de disséminer la bonne information aux bons destinataires (étape 4). Bien que ce modèle n'ait pas été conçu spécifiquement pour le marché de la Threat Intelligence il a le mérite de montrer que le client demeure en contrôle de ses besoins et de la dissémination de l'information. Ces deux phases exigent de l'entreprise une excellente compréhension de ses besoins et un bon niveau de maturité. Car autant les flux de données techniques pourront être livrés directement au

Un service de Threat Intelligence ?

Un bon fournisseur de Threat Intelligence sera en mesure d'associer divers flux d'informations concernant l'activité d'acteurs malveillants. Il s'agira par exemple de :

- Adresses IP ou domaines utilisés dans le cadre d'attaques présentes ou passées (notamment des serveurs de Command & Control)
- Informations sur les vulnérabilités zero-days mises en vente sur les marchés clandestins et leurs indicateurs de compromission (IoC) associés
- Statistiques sur les attaques en cours (quelles industries ? Quelles régions ?)
- Visibilité sur les groupes d'attaquants les plus actifs et leurs motivations, ou encore sur les systèmes les plus ciblés actuellement (quelle vulnérabilité a la cote ?)

Ces informations seront ensuite validées, dédoublées - automatiquement et par des experts humains - et des informations de réputation leur seront associées. Le tout sera alors livré aux clients sous forme de flux, parfois directement dans des équipements de sécurité (mise en place de listes de blocage) ou sous forme d'API, et même de fichiers Excel ! Charge alors à l'entreprise d'en faire bon usage.

SIEM ou aux équipements de sécurité sous forme de listes de blocages et seront alors immédiatement utiles, autant des informations plus prospectives ou plus "métier" exigeront un action manuelle.

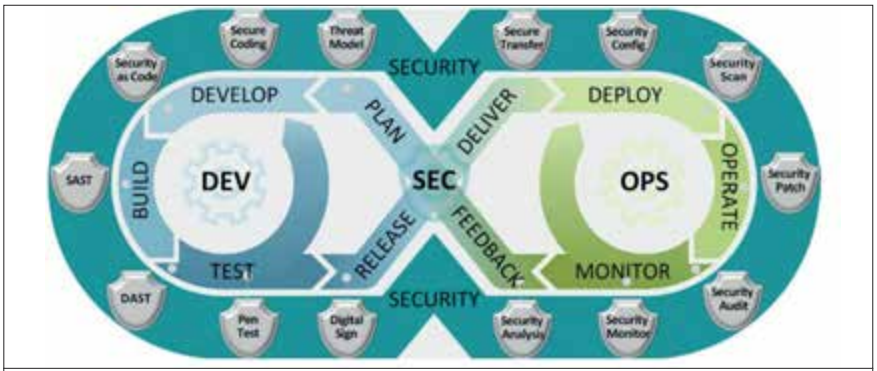
Au delà des flux techniques

Ainsi, que faire des rapports sur les menaces émergentes ou les nouvelles pratiques en cours ? Quel responsable sera le plus à même d'exploiter correctement cette information ? Quelles actions concrètes exige-t-elle ?
Ces actions seront avant tout managériales : il faudra comprendre ce qu'implique pour l'activité la recrudescence de telle ou telle pratique émergente chez les pirates, la recrudescence de telle attaque chez nos concurrents, ou encore faire le lien entre la motivation de tel groupe d'attaquants et son propre contexte : sommes-nous une cible ?
Il faudra alors valider que l'on dispose d'équipements vulnérables, ou peut-être comprendre qu'il s'agit seulement d'un problème de configuration. Et enfin déterminer la meilleure manière d'y faire face (corriger ? Isoler ?).
Et il ne s'agit encore là que d'une vision technique. Si les attaques en question intègrent une composante d'ingénierie sociale, par exemple, il faudra en outre être en mesure d'en comprendre les ressorts, déterminer si et comment ces derniers s'appliquent à l'entreprise, et enfin décider d'un plan de sensibilisation adapté. Et rien de tout cela ne s'automatise !
Tout ceci est un autre pan du marché de la Threat Intelligence, servi essentiellement par des consultants spécialisés, mais aussi par certains fournisseurs de solutions de Threat Intelligence de type « premium ». ■

J.S.

DevSecOps, la transformation digitale des DSI

Alors que le développement agile s'est désormais imposé dans de nombreuses entreprises, la cybersécurité doit désormais trouver sa place et pousser les développeurs vers le "Secure by design".



La cybersécurité doit être présente à chaque étape du SDLC (cycle de vie de l'application): Cela passe par des outils et des processus, mais aussi par une remise en cause de l'équipe de sécurité qui doit sortir du silo où elle a longtemps été enfermée. Crédit : DoD Enterprise DevSecOps Reference Design, 2019

Le besoin d'agilité a poussé les grandes entreprises à se convertir à DevOps. Ces grands groupes internationaux se sont dotés de structures de type "Agile at Scale" afin de mener à bien leur transformation digitale. Néanmoins, la sécurité a eu bien du mal à trouver sa place dans cette nouvelle organisation : administrateurs et développeurs considéraient les experts en sécurité comme un frein dans une organisation entièrement tournée vers l'efficacité. Le pari des DSI est d'intégrer pleinement les bonnes pratiques de sécurité au sein des processus de création des applications. Les équipes sécurité ne doivent plus opérer comme un silo qui intervient en dernier lieu, au moment de la mise en production de l'application. Il est temps de basculer dans l'ère du DevSecOps.

Les RSSI doivent se rapprocher des équipes agiles

Les membres de l'équipe cybersécurité doivent être intégrés au moins de façon partielle aux équipes DevOps de manière à s'assurer que les bonnes pratiques de sécurité sont effectivement bien appliquées tout au long du cycle de vie de l'application. C'est sans doute le plus grand défi à relever dans cette transformation qui doit mener aux préceptes DevSecOps. La cybersécurité doit être prise en compte à chaque étape de ce cycle de vie, depuis les phases très amont de conception de l'architecture logicielle et technique jusqu'à l'exploitation, en passant par les étapes itératives de Build. Le code source doit être écrit dans le respect des bonnes pratiques de sécurité éditées par les RSSI, testé avec des outils automatiques de test de sécurité, puis faire l'objet de PenTest (tests de pénétration) et ce souci de créer un code à la fois "Secure by design" mais qui intègre aussi la notion de "Privacy by Design" afin de s'assurer de la conformité de l'application aux diverses réglementations liées à la protection des données personnelles. ■

A.C.

Protection du poste de travail

Le bon vieil antivirus a évolué : La génération EDR (Endpoint Detection and Response) et maintenant les solutions XDR vont de plus en plus loin pour protéger les parcs de PC et les serveurs. Cette montée en puissance a été rendue nécessaire pour contrer à la fois les vagues successives de malwares qui continuent à déferler sur les entreprises, mais aussi réduire autant que faire se peut le délai de détection des redoutables APT.

Le marché des outils de protection du poste de travail est probablement le mieux connu, le plus ancien et l'un des plus vastes en matière de cybersécurité.

Parti des seuls antivirus dans les années 1980 il a évolué au fil des décennies pour aboutir à un ensemble de fonctions de sécurité intégrées au sein d'un client unique.

Sa fonction centrale demeure bien entendu la lutte contre les codes malveillants. L'antivirus s'est fait « anti-malware », un terme désormais fourre-tout qui englobe les capacités offertes par feu les anti-spywares, anti-rootkits, anti-adwares et autres « anti-tout » !
Ces outils ont donc su évoluer avec les menaces. Ils intègrent ainsi désormais aussi des protections plus génériques telles que la détection de vulnérabilités locales, la détection comportementale et le contrôle applicatif (sandboxing), la protection de la mémoire, l'analyse de réputation, et parfois même des fonctions légères de prévention des fuites de données ou de chiffrement du disque. Mais quelles que soient ses technologies l'outil de protection du poste aura toujours comme objectif d'empêcher l'exécution de code malveillant sur le poste de travail, quelle que soit la technique d'infection ou de persistance exploitée par ce dernier.

Les fonctions essentielles à exiger

ANTI-MALWARE	C'est la base et il faut le faire bien ! On inclut ici à minima les fonctions auparavant fournies par les antivirus, anti-adwares, anti-spywares, anti-rootkits, etc.
PARE-FEU PERSONNEL	Que ce soit au moment de l'infection ou pour contacter ensuite un serveur de Command & Control, les malwares exigent un accès à Internet. Et donc un pare-feu personnel est essentiel à l'anti-malware.
CONTRÔLE DES PÉRIPHÉRIQUES ET DES PORTS	Seconde voie d'infection après la navigation Internet ou l'email, les périphériques (USB notamment) doivent être contrôlés. Et cela permet en prime d'appliquer des politiques de chiffrement efficaces sur les supports externes.
TABLEAUX DE BORD & ADMINISTRATION CENTRALISÉE	L'outil doit pouvoir se déployer et s'administrer de manière centralisée, et fournir des rapports clairs sur l'état de protection du parc.
SUPPORT NON-WINDOWS	Autant aller jusqu'au bout du concept de la simplification du déploiement et de l'administration avec une solution unique disponible aussi pour Mac et Linux, voire spécifique à Microsoft Exchange et Sharepoint, par exemple.

Best of breed ou simplicité d'administration ?

Vaut-il mieux sélectionner un produit expert dans chaque fonction souhaitée, et ainsi devoir gérer une multitude de clients sur le poste de travail, ou opter pour un client unique qui ne saurait certes être excellent en tout mais dont l'administration sera largement simplifiée ? La question s'est posée dès les premières acquisitions par les grands éditeurs d'antivirus de plus petits éditeurs de technologies alors innovantes (anti-spam, détection d'intrusion locale, anti-rootkit, etc.).

Elle semble désormais réglée tant les entreprises optent majoritairement pour un client intégré et, selon l'analyste Gartner, consolident ce qui ne l'est pas encore.

Certes, des spécialistes de niche se créent encore mais ils ne manqueront pas d'être rachetés à leur tour par les poids lourds du domaine dès lors qu'ils auront fait la preuve de leur pertinence.

En définitive sur ce marché, les petits spécialistes innovent et les grands éditeurs rachètent !

SANDBOXING	L'isolation des applications est la seule approche générique susceptible de garantir pleinement la protection du poste de travail. Si elle n'est pas toujours applicable et doit être secondée, elle n'en demeure pas moins un atout important.
RÉPUTATION	L'analyse en temps réel de la réputation des sources (domaines, adresses IP) et des documents joue le rôle d'un système d'alerte collaboratif avancé. Cette approche est très efficace en complément des autres méthodes de détection.
PRÉVENTION DES FUITES DE DONNÉES (DLP)	La capacité du client antimalware à assurer un contrôle local pour le compte d'une solution de prévention des fuites de données (DLP) permettra de simplifier la mise en oeuvre de ce type de solution.
ENDPOINT DETECTION AND RESPONSE (EDR)	L'EDR apporte le volet « réponse » à des solutions jusqu'à présent plus axées « prévention ». Catégorie encore souvent à part aujourd'hui, elle sera certainement la prochaine à être intégrée aux outils de protection du poste de travail. Autant anticiper !

L'avenir est à la réponse

Si le marché de la protection du poste de travail est essentiellement tourné vers la prévention (on tente d'empêcher l'exécution du code malveillant), il a désormais tendance à évoluer vers la réponse. On voit ainsi émerger le marché du Endpoint Detection and Response, ou EDR. Ces outils surveillent en temps réel divers appels systèmes à la recherche des signes traditionnels d'exploitation d'une vulnérabilité. Ils offrent ainsi une vision temps-réel de l'activité des postes de travail, et permettent - en théorie - de bloquer l'exploitation d'une vulnérabilité inconnue.

Mais l'autre apport innovant de ces solutions - le « R » de « Response » - est leur capacité à collecter de nombreux paramètres liés à l'activité des postes de travail et ainsi permettre l'investigation poussée des brèches. Ces outils permettent notamment de récupérer immédiatement et à distance des éléments de n'importe quel poste (clé de registres, processus, dump de la mémoire vive, etc.). Les informations qu'ils collectent peuvent également être archivées et servir ultérieurement à enquêter sur une brèche ou définir plus aisément de nouveaux indicateurs de compromission (IoC) à diffuser. ■

J.S.

Protection des terminaux mobiles

Les terminaux mobiles sont encore une catégorie à part, mais pour combien de temps encore ? La tendance est à la protection de l'information quel que soit son support. Alors anticipons !

A l'heure où les ultra-portables dernier cri se font tactiles, plus légers et moins encombrants que les nouvelles tablettes professionnelles extra-larges, où se situe la frontière entre un poste de travail et un terminal mobile ? Et qu'est-ce qui distingue donc encore une solution de protection mobile de celle destinée aux postes de travail traditionnels ? Pas grand chose, à vrai dire. Mais encore suffisamment pour que la protection des terminaux mobiles fasse l'objet d'une catégorie à part dans cette édition du guide de la cybersécurité.

La sécurité tournée vers la donnée

Cela ne sera peut-être pas toujours le cas : la tendance est en effet de placer l'information - et non plus le terminal - au cœur de la stratégie de protection de l'entreprise.

Les notions de protection de l'information (le chiffrement, la classification, une gestion granulaire des droits) et du terminal (anti-malware, supervision, contrôles continus) convergent alors et doivent s'exercer à l'identique quel que soit le terminal.

C'est pourquoi il est important de rechercher dès aujourd'hui une solution de protection mobile capable de s'inscrire à terme dans cette stratégie globale : en choisissant par exemple un éditeur offrant une large couverture et ayant dès aujourd'hui une politique de convergence, ou un acteur de niche disposant d'accords (et d'API !) permettant à ses produits d'être supervisés et de s'intégrer sans heurt dans une infrastructure plus large. ■

J.S.

Le chiffrement, fonctionnalité reine de la mobilité

Le chiffrement intégral demeure la fonctionnalité incontournable des équipements mobiles, dont le risque de perte ou de vol est accru. Préférez pour cela une solution présentant des certifications internationales telles FIPS 140-2 ou Critères Communs (EAL).

Protection de la donnée

Et si l'on cherchait à protéger aussi la donnée elle-même, plutôt que seulement les systèmes qui la traitent ?

La montée en puissance des aspects réglementaires -notamment en ce qui concerne les données à caractère personnel- a rendu incontournable une nouvelle approche de protection dite "data centric", basée sur la donnée elle-même. Son objectif est de protéger le contenu plutôt que le contenant.
Pour cela le marché offre trois approches : le chiffrement, la gestion des droits numériques (EDRM) et la prévention des fuites de données (DLP).

J.S.

Gestion des droits numériques : pour garder le contrôle.

Les solutions de gestion des droits numériques (EDRM) permettent aux documents d'embarquer leurs propres règles d'accès et ainsi de garder le contrôle de la donnée lorsque celle-ci a quitté l'entreprise. Il sera ainsi possible de décider qu'un document PDF ne pourra être lu que sur une période donnée, ou encore de le mettre à jour une fois diffusé. Ces solutions permettent également de décider ce qui pourra être fait avec le document : copie, édition, impression, ouverture depuis quel type de terminal, etc.

EDRM : les questions à se poser

- Quels formats sont supportés ? (Adobe, Word, Excel, images, AutoCAD…)
- Disponibilité de connecteurs ? (CASB, DLP, ERM, partage de fichiers…)
- Simplicité de l'interface de création des politiques de sécurité ?
- Capacité à interpréter les politiques de sécurité existantes (règles SharePoint, etc.)

Le DLP, contre les fuites accidentelles

Mal comprises, jugées trop simples à contourner, les solutions de DLP n'ont pas toujours bénéficié d'une bonne réputation. Mais il s'agit assurément d'un malentendu : le marché de la prévention des fuites de données protège avant tout de l'erreur humaine et non du vol de donnée !

Associés à une solution de classification des données, les outils de DLP s'assurent, par exemple, que le document Excel signalé comme « Interne » envoyé par email n'est effectivement adressé qu'à des correspondants internes (qui n'a jamais commis d'erreurs liées à la saisie semi-automatique des adresses ?).

Sachant que l'erreur humaine est l'une des principales causes de pertes de données en entreprise, c'est un bon investissement !

Comme pour beaucoup de solutions de sécurité, les modèles d'intelligence artificielle sont en train d'étendre la vision des solutions de prévention des fuites de données. Des prestataires Cloud proposent ainsi de rechercher les données de l'entreprise qui ont déjà franchi ses protections et qui circulent sur Internet ou sur le Dark Web. Les algorithmes recherchent inlassablement les fichiers sensibles de l'entreprise afin de générer une alerte si un fichier sensible est repéré sur un forum de hackers ou tout simplement sur un disque dur portable ou la box Internet d'un salarié qu'il n'aurait pas sécurisé. Des spécialistes se chargent alors de neutraliser la fuite.

DLP : les questions à se poser

- Positionnement de la solution : sur les postes de travail, sur le réseau ou les deux ?
- Peut-on appliquer une politique unique entre réseau et postes de travail ?
- Support des applications métiers en mode SaaS ?
- Disponible sous forme d'appliance virtuelle ?
- Est-ce une solution dédiée au DLP ou s'agit-il d'une fonctionnalité complémentaire (présente sur certains pare-feux nouvelle génération, outils de classification, systèmes de détection d'intrusion, cloud access security brokers, etc.)

Le chiffrement, l'approche historique

Le chiffrement protège la donnée au repos (stockée) ou en mouvement (sur le réseau). Il intervient au niveau du matériel (équipements réseaux par exemple), du stockage ou de l'application (chiffrement des bases de données, par exemple). L'action de chiffrer peut être transparente (la donnée est alors protégée automatiquement sans intervention de l'utilisateur) ou déclenchée par ce dernier.

Le chiffrement de la donnée au repos couvrira le risque de vol des supports (ordinateur portable, supports externes tels que disques durs ou clés USB) tandis que le chiffrement de la donnée en mouvement couvrira l'interception de cette dernière (présence de l'attaquant sur le réseau).

Chiffrement : quelques questions à se poser

- Souhaite-t-on protéger des données stockées ou en transit ?
- Chiffrement du stockage, de l'applicatif, ou des bases de données ?
- Chiffrement transparent (« Full disk encryption ») ou volontaire ? (« file encryption »)
- Comment seront gérées (et générées) les clés ?
- Existe-t-il une clé maître ?
- Chiffrement individuel ou multi-utilisateurs ?
- Comment gérera-t-on les sauvegardes et l'archivage des données chiffrées vis-à-vis des changement de clés ?



Disponible dès le 7 octobre

Protection applicative

Avec 90 % des attaques ciblant la couche applicative, la protection des applications doit être une priorité. En particulier sur le Web.

Selon des chiffres du département américain de la sécurité intérieure, 90 % des attaques ciblent la couche applicative (en particulier sur le web). Heureusement, le marché propose deux approches complémentaires pour se protéger : l'une placée devant l'application à protéger, et l'autre en son cœur !

Le WAF en frontal des applications web

Le pare-feu applicatif web (WAF, pour Web Application Firewall) se place devant l'application et filtre le trafic qui lui est destiné. Fonctionnant à base de signatures le WAF va rechercher les signes d'attaques connues.
Le WAF ne demande pas de toucher à l'application, et il sera donc idéal pour protéger une application vieillissante impossible à améliorer (lorsqu'un règlement tel PCI-DSS lui impose un certain nombre de fonctionnalités de sécurité !).

La protection automatique du runtime (RASP)

Alors que le WAF est externe à l'application, l'approche du Runtime Application Self-Protection (RASP) est résolument interne : il s'agit de s'intercaler entre le code de l'application et les bibliothèques qui lui sont nécessaires, afin d'intercepter les appels jugés dangereux.
Si le RASP présente de nombreux avantages par rapport au WAF, il souffre de la nécessité d'accéder dans certains cas au code source de l'application et de déployer un outil spécifique sur le serveur. En outre ces outils ne supportent à l'heure actuelle que les technologies Java et .NET !

Exigez l'OWASP Top 10 !

La meilleure façon de protéger une application est de bien la concevoir dès le départ !
Pour cela l'association américaine Open Web Application Security Project (OWASP) œuvre depuis 18 ans à sensibiliser les développeurs web aux bonnes pratiques du développement sécurisé. Elle diffuse un outil contractuel d'une redoutable efficacité : une annexe prérédigée que tout donneur d'ordre pourra inclure au contrat de développement web qu'il s'apprête à signer. Celle-ci liste les 10 points-clés de sécurité que l'application devra respecter pour être recevable. C'est simple, c'est très efficace et c'est gratuit ! ■

J.S.

https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex

Audit d'architecture

L'audit d'architecture s'intéresse au SI dans son ensemble et cherche à valider la pertinence des choix technologiques et le respect des bonnes pratiques de sécurité

De tous les audits techniques, l'audit d'architecture est peut-être celui au périmètre le plus large. Il s'agit en fait d'un audit macroscopique ! Selon le périmètre, ce type d'audit exigera plus de temps et de ressources que les autres. Son objectif est de s'assurer que le Système d'Information (sa topologie, son organisation, ses priorités) est conforme aux exigences métiers, aux divers règlements qui s'y appliquent et aux bonnes pratiques de sécurité. L'audit d'architecture évaluera également les choix technologiques opérés par l'IT et la SSI, leur pertinence ainsi que la qualité de leur implémentation (et accessoirement leur bonne configuration, voir encadré)

Le choix du prestataire

Si dans le cadre du test d'intrusion l'entreprise suit souvent un auditeur individuel, l'audit d'architecture est une affaire d'équipe et de compétences multiples : un seul auditeur sera difficilement expert de l'ensemble des bonnes pratiques et des solutions déployées au sein de l'entreprise. En outre le prestataire devra disposer d'un volet de certifications éditeurs étendu. Ces contraintes font qu'à compétences égales, plutôt qu'un pure player du conseil il sera possible d'envisager un intégrateur spécialiste de la sécurité capable d'offrir du conseil. ■

J.S.

L'audit de configuration

L'audit de configuration est une prestation parfois distincte mais complémentaire à l'audit d'architecture. Plus ciblé, celui-ci porte sur la pertinence des configurations matérielles et logicielles du SI. Celles-ci seront étudiées sur la base des guides d'installation officiels, parfois des codes sources et surtout des meilleures pratiques de l'industrie. Là aussi, l'objectif est d'identifier les mauvaises pratiques (les configurations par défaut notamment) et de proposer un plan de correction.

SOC

Un Security Operations Center est le centre névralgique de la sécurité : il centralise, analyse et répond 24h/24, sept jours sur sept.

Le SOC est la pierre de voûte de l'édifice sécurité. Son rôle est d'unifier la fonction sécurité autour d'une organisation resserrée afin de détecter et de répondre aux menaces de manière coordonnée.
Élément central d'une stratégie sécurité, le SOC vient finaliser une démarche probablement entamée de longue date. Car pour en tirer tous les bénéfices l'entreprise devra avoir déjà atteint une maturité sécurité importante : elle devra notamment pouvoir compter sur des équipes expérimentées, des processus bien rodés et une bonne maîtrise des solutions qu'elle exploite déjà.
Ceci est particulièrement vrai, bien entendu, pour le SOC interne qu'elle animera seule. Mais c'est également le cas, dans une certaine mesure, du SOC exploité par un prestataire externe.
L'approche interne ne concernant que peu d'acteurs, nous nous intéresserons dans ce guide au choix d'un prestataire externe capable d'animer un SOC pour le compte de ses clients.

Multi-tenant or dédié ?

L'essentiel des offres de SOC externalisées est « multi-tenant » : les ressources techniques et humaines sont partagées entre tous les clients et les informations sur les menaces issues des flux d'un client bénéficient à tous les autres. Considérant que le coût de ressources dédiées serait largement plus élevé et que la mutualisation de l'analyse des flux bénéficie à l'ensemble des clients, ce n'est pas une mauvaise chose, à condition d'obtenir des garanties sur la confidentialité et l'isolation des informations clients.

La question de la confidentialité

Le prestataire devra notamment être en mesure de prouver qu'il prend les mesures nécessaires pour garantir l'isolation des informations confidentielles fournies par chaque client. En outre, le SOC étant par définition un point névralgique, il doit bénéficier lui-même d'un niveau de protection logique et physique adapté à la sensibilité des informations qu'il traite.

Les ressources internes

La mise en place d'un SOC externe n'est pas un projet mineur. Cela exigera des ressources et des efforts de la part de l'entreprise, tant avant que pendant la durée du contrat.
Avant, il sera notamment nécessaire de fournir des procédures précises de réaction aux incidents : qu'est-ce qui est normal dans le cadre de l'activité ? À partir de quel seuil tel ou tel événement devient-il une alerte ? Depuis quels pays des connexions de nos collaborateurs sont-elles légitimes ?
Enfin, durant la phase d'exploitation, il faudra être en mesure de répondre aux alertes et sollicitations du prestataire en temps et en heure, avec des procédures bien établies. Ce qui est déjà tout un projet en soi ! ■

J.S.

Les fonctions offertes par un SOC externe

- Intégration et supervision des flux de trafic de l'entreprise
- Surveillance continue des équipements et des solutions de sécurité (souvent à l'aide d'un SIEM exploité par le prestataire)
- Gestion des vulnérabilités remontées par un outil d'analyse automatisée
- Pré triage des alertes (nombreuses à ce stade !)
- Priorisation des alertes
- Gestion de la réponse selon les consignes de l'entreprise
- Analyse de la cause de l'incident
- Actions correctives (mises à jour, changement de configuration, etc.).

Ce que vous fournirez à votre prestataire de SOC externe

- Rapports d'analyses de vulnérabilités automatisées
- Liste des commandes sensibles passées aux bases de données
- Liste des commandes sensibles passées par les administrateurs systèmes
- Requêtes émises vers et renvoyées par les serveurs web
- Journaux des systèmes de filtrage de contenu web
- Journaux des équipements de sécurité (WAF, IDS, antivirus, etc.)
- Journaux du système d'authentification
- Journaux de la plateforme d'emails
- Autres journaux applicatifs (souvent centralisés au sein d'un SIEM)
- Requêtes DNS internes et vers l'externe
- Autres sources d'événements applicatifs (notamment issus d'applications hébergées en mode SaaS)

À noter : l'ANSSI propose un programme de qualification des « ***Prestataires de détection d'incidents de sécurité*** » (PDIS) qui pourra aider à présélectionner les prestataires. La liste des sociétés qualifiées est disponible ici : **https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-detection-dincidents-de-securite-pdis/**

Tableaux de bord de sécurité

Meilleure visibilité et aide à la prise de décision : les tableaux de bord de sécurité sont un outil indispensable dans le pilotage de la sécurité.

Selon l'institut SANS, la difficulté à fixer les bonnes priorités et à mesurer la sécurité sont parmi les principales causes de défaillance de la cybersécurité. Les tableaux de bord de sécurité apportent une solution à ces deux freins. Et pourtant, si les entreprises ont souvent de bons tableaux de bord commerciaux, elles peinent à mettre en place l'équivalent en cybersécurité. Et quand ils existent ceux-ci sont souvent dédiés à la seule conformité. Mais la conformité n'a jamais garanti la sécurité !

Point de départ et référentiel quotidien

De bons tableaux de bord de sécurité présentent un double avantage : ils sont d'abord un excellent point de départ pour initier une démarche de cybersécurité. Ils aident à couvrir l'essentiel des éléments de base d'une stratégie de protection.
Mais ils sont surtout au quotidien le meilleur moyen de détecter les écarts dans la posture de sécurité de l'entreprise. Ils offrent une vision globale du niveau de risque à un instant T et sa tendance (sommes-nous en progrès ou nos capacités de remédiation baissent-elles ?)

SIEM, SOC et conseil !

Parce que les indicateurs nécessaires au tableau de bord sont issus des équipements de sécurité et autres sources techniques, ils peuvent être un produit dérivé d'une solution de SIEM, voire même être fournis par le prestataire du SOC externalisé.
Mais le tableau de bord sécurité peut aussi être un projet d'entreprise à part entière.
Il pourra alors être mené en interne ou avec l'aide d'un consultant. L'essentiel de la mission consistera à identifier les indicateurs pertinents et leurs sources, à déterminer les valeurs de seuil (qu'est-ce qui est anormal ?), à mettre en place les connecteurs nécessaires pour récupérer les données et enfin à trouver une solution de présentation adaptée.

J.S.

SIEM

Alimenté par l'ensemble des événements du SI, le SIEM voit, analyse et identifie les attaques. Mais il vaut peut-être mieux le faire exploiter par un spécialiste externe.

Un Security Information & Event Manager agrège des informations en provenance de sources diverses (applications, systèmes, équipements d'infrastructure...) afin d'identifier des attaques potentielles.
La force du SIEM réside dans sa capacité à corréler des signes qui, pris individuellement, seraient restés ignorés. Et donc à produire des alertes que l'on espère plus pertinentes.
Les SIEM sont utiles en temps réel pour donner l'alerte, mais aussi a posteriori pour aider l'analyse forensique. Ils contribuent également au respect des obligations réglementaires en alertant sur des situations non conformes.
Mais comme toute solution complexe, leur mise en oeuvre et surtout leur exploitation peut s'avérer trop coûteuse en interne. C'est pourquoi ces outils sont souvent exploités par un prestataire qui fournit en retour un flux d'alertes et, en option, pourra y répondre (voir SOC).

J.S.

4 questions à poser avant l'achat

1 ***Ai-je vraiment besoin d'un SIEM ?***
Le SIEM est un outil puissant capable de détecter des attaques sophistiquées. Il ne sera utile que si l'entreprise est déjà en mesure de détecter et de répondre aux attaques plus communes. Avez-vous vous déjà, par exemple, une solution de log management bien exploitée ?

2 ***Interne ou externe ?***
Exploiter correctement un SIEM exigera très probablement des ressources supplémentaires. C'est pourquoi il est courant de déléguer l'exploitation d'un SIEM à un prestataire (voir notamment le référentiel des « Prestataires de détection d'incidents de sécurité » (PDIS) qualifiés par l'ANSSI)

3 ***Support des sources existantes ?***
Les principaux SIEM proposent un grand nombre de connecteurs vers les équipements et applications communes, mais il sera nécessaire de faire un pointage précis.

4 ***Et les sources externes ?***
Le SIEM choisi est-il en mesure d'accepter des sources d'information externes ?

Ecosystème

Les organismes et associations de référence

AFCDP

ANSSI

Campus Cyber

CESIN

Cigref

Clusif

CNIL

Cybermalveillance.gouv.fr

Hexatrust

Numeum

AFCDP

(Association Française des Correspondants à la protection des Données à caractère Personnel)

L'AFCDP, créée dès 2004, regroupe plus de 6500 professionnels de la conformité à la Loi Informatique & Libertés et au RGPD – dont les Délégués à la Protection des Données (ou DPO, pour Data Protection Officer).

Association représentative des DPD, l'AFCDP rassemble non seulement les professionnels de la protection des données et des DPD désignés auprès de la CNIL, mais aussi toutes personnes intéressées par la protection des données à caractère personnel. La richesse de l'association réside notamment dans la diversité des profils des adhérents : DPD, délégués à la protection des données, juristes et avocats, spécialistes des ressources humaines, informaticiens, professionnels du marketing et du e-commerce, RSSI et experts en sécurité, qualiticiens, archivistes et Record Manager, déontologues, consultants, universitaires et étudiants.

Dès sa création, l'association s'est attachée à deux missions :

- Mutualiser, entre professionnels concernés, les expertises et les réussites, les interrogations, les bonnes pratiques.
- Promouvoir et défendre le nouveau métier de DPO (Data Protection Officer), tant auprès des décideurs publics et relais d'opinion que des entreprises, institutions et organisations, afin de leur faire prendre conscience des nouveaux enjeux de la protection des données personnelles et des modifications juridiques.

L'AFCDP fait le lien entre les professionnels de la protection des données à caractère personnel, les institutions et décideurs publics (CNIL, Parlementaires…), et les entreprises. Par son expertise et l'expérience de ses membres, elle formule régulièrement des recommandations et/ou des avis aux autorités publiques et aux acteurs de la protection des données personnelles et de la conformité. En 2021, à l'occasion de l'Université AFCDP des DPO plus de 850 DPO se sont réunis pour ce grand rendez-vous annuel désormais incontournable, et pensé en 100% distanciel en raison du contexte. Il s'est décliné ensuite en plusieurs ateliers mensuels réunissant entre 200 et 300 personnes connectées. La prochaine édition se tiendra le 9 février 2023 en présentiel.

"L'AFCDP entend défendre une conception de la protection des données qui met en son cœur une approche active, qui concilie les droits fondamentaux de chacun avec la possibilité pour les organismes que nous représentons de continuer à créer et innover. Cette approche se fonde sur certains principes que nous sommes heureux de voir repris dans le règlement européen : la souveraineté des individus sur l'usage de leurs données et la responsabilisation des entreprises. Ensemble, ces deux principes permettent de créer la confiance nécessaire à l'épanouissement de l'usage du numérique en France."

Souligne Paul-Olivier Gibert, Président de l'AFCDP.

ANSSI

(Agence nationale de la sécurité des systèmes d'information)

Crée en 2009, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) est l'autorité nationale en matière de cybersécurité. Placée sous l'autorité de la Première ministre et rattachée au Secrétaire général de la défense et de la sécurité nationale (SGDSN), elle bénéficie d'un positionnement lui permettant de déployer une politique globale de cybersécurité et d'en assurer la coordination à l'échelle interministérielle.

La mission première de l'ANSSI est d'assurer par différents moyens la sécurité des infrastructures numériques publiques et privées les plus critiques et de les défendre en cas d'attaque informatique.

Au-delà de ces organisations les plus sensibles, elle s'adresse également à l'ensemble des acteurs de la transformation numérique du pays pour élever le niveau de cybersécurité global de la nation et favorise les conditions d'un dialogue de confiance avec ses partenaires français, européens et internationaux.

L'ANSSI en chiffres (2021)

- **255 visas de sécurité délivrés**
- **88 certifications délivrées**
- **167 qualifications délivrées**
- **47 formations labellisées SecNumEdu**
- **17 opérations de cyberdéfense**

Les Visas de sécurité

Depuis 2017, l'ANSSI s'engage dans une démarche de valorisation de ses activités de qualification et de certification : le Visa de sécurité ANSSI. Délivré par l'agence, il permet d'identifier facilement des solutions de sécurité numérique fiables et reconnues comme telles à l'issue d'une évaluation réalisée par des laboratoires agréés selon une méthodologie rigoureuse et éprouvée.

Cette évaluation prend notamment la forme de tests de pénétration poussés et d'une analyse approfondie pour vérifier la conformité de ces solutions aux référentiels correspondants.

Ce Visa se matérialise, selon le contexte et le besoin, par une certification ou une qualification. Il est un gage de sécurité pour les utilisateurs et un gage de compétitivité pour les fournisseurs et prestataires de services.

Contact

Agence nationale de la sécurité des systèmes d'information

51, boulevard de La Tour-Maubourg
75700 Paris 07 SP

Email : **communication@ssi.gouv.fr**
Site web : **www.ssi.gouv.fr/**
Twitter : **@ANSSI_FR**
Dailymotion : **DAILYMOTION.COM/ANSSI_FR/**
LinkedIn : **LINKEDIN.COM/COMPANY/ANSSI-FR**

Campus Cyber

Conçu, mis en place et dirigé par Michel Van Den Berghe, (précédemment à la tête d'Orange Cyberdefense), avec le soutien de l'Anssi cet ambitieux projet a été initié en 2019 par le président de la République, Emmanuel Macron.

Ce « Lieu totem de la cybersécurité » rassemble dans sa tour de 13 étages, sur 26 000m² , au cœur de La Défense, les principaux acteurs nationaux et internationaux du domaine : des entreprises (grands groupes, PME), des services de l'État, des organismes de formation, des acteurs de la recherche et des associations.
Il leur offre des bureaux et des services communs : showroom, amphithéâtre, 4 espaces événementiels , 3 000m² d' espaces de formation etc.

Sur les 6 premiers mois d'ouverture, plus de 2 300 experts ont été on-boardés et plus de 150 événements se sont déroulés sur le site.

Fin septembre 2022 , le Campus Cyber rassemble 167 Membres, 40 Partenaires, 120 Résidents.

Le Campus Cyber met en place des actions visant à fédérer la communauté de la cybersécurité et à développer des synergies entre ces différents acteurs.
Il permet notamment, en rassemblant les experts de l'analyse cyber de :

- Rapprocher la recherche, l'innovation et l'industrie pour faire émerger les licornes de demain
- renforcer les capacités de veille, de détection et de réponse à la menace.
- créer un observatoire de la cybermenace et une base commune de « Threat Intelligence », composée des indices de compromission assemblés par les différents partenaires publics et privés.

L'un des enjeux majeurs du Campus Cyber reste l'attractivité de la filière et la formation, avec notamment des programmes communs d'entraînement et de formation dispensés par des écoles ou des centres de formation.

Des partenariats entre le Campus national et des Campus territoriaux de cybersécurité seront développés dans les prochains mois.

Contact

Email : **contact@campuscyber.fr**
Site web : **https://campuscyber.fr/**

CAMPUS CYBER

CESIN

Le Club des Experts de la Sécurité de l'Information et du Numérique est une association regroupant des professionnels de la cybersécurité. Ses membres actifs doivent obligatoirement exercer une responsabilité dans la SSI au sein de leur organisation. Le Club compte plus de 800 adhérents.

Au-delà du partage de connaissances et de l'enrichissement du réseau professionnel de ses membres, la vocation du CESIN est de porter la voix du RSSI en tant que profession. Le club participe à de nombreux événements, édite un baromètre annuel sur l'état de la cybersécurité des grandes entreprises françaises, aide à faire reconnaître et évoluer le métier de RSSI, ainsi qu'à alimenter la réflexion autour de son positionnement dans l'entreprise. Le club se donne également pour mission de sensibiliser les dirigeants d'entreprises face au risque cyber.

Par ailleurs, au travers des partenariats avec les pouvoirs publics, le CESIN ambitionne d'accompagner les évolutions réglementaires concernant la cybersécurité.

Les membres du CESIN se retrouvent tout au long de l'année à l'occasion de groupes de travail dont les thématiques couvrent tous les domaines de la SSI, de la gouvernance ou l'analyse de risque, en passant par des thématiques plus opérationnelles, industrielles ou juridiques…

Le CESIN organise des Université d'été et un Congrès annuel en décembre, avec un programme de conférences et ateliers durant lesquels les membres, réunis en groupes de travail, se livrent à des analyses prospectives, des débats thématiques, et partagent leurs retours d'expérience.

Le Club est présidé par Mylène Jarossay, CISO du groupe LVMH.

Comment le CESIN aide les entreprises françaises

- **Echange :** le CESIN offre aux RSSI des entreprises françaises un environnement au sein duquel ils peuvent se rencontrer et échanger entre pairs.
- **Information :** A travers les travaux de ses membres, le CESIN publie des analyses et des études statistiques utiles, dont le baromètre annuel de la cybersécurité.
- **Influence :** En se donnant comme objectif d'accompagner les évolutions réglementaires et de porter la voix des RSSI, le CESIN œuvre à favoriser l'émergence de réglementations plus pragmatiques qui tiendront compte des contraintes des entreprises.

Contact

CESIN
115 rue Saint Dominique
756007 PARIS
Tél : 06 09 56 63 17
Site web : **https://cesin.fr/**
Ecrire : **https://cesin.fr/contact**

CESIN

Cigref

Le Cigref est une association indépendante et sans activité commerciale, créée en 1970, qui accompagne ses 155 membres, grandes entreprises et administrations publiques françaises exclusivement utilisatrices de solutions et services numériques, dans toutes leurs réflexions sur leurs enjeux numériques collectifs. Notre association œuvre, au profit de ses membres, en faveur d'un numérique durable, responsable et de confiance.

Alors que le nombre et l'intensité des cyberattaques affectant les organisations publiques comme privées ne décroît pas et que les enjeux cyber et géopolitiques s'entremêlent de plus en plus à l'aune du conflit déclenché par la Russie en Ukraine, le Cigref, pour sa part, intensifie ses activités sur la cybersécurité, notamment en créant un "Club Sécurité Numérique", présidé par Christophe Leray, Directeur du Système d'Information du Groupement les Mousquetaires et Vice-Président du Cigref, et en réservant une place substantielle au sujet dans le plan d'activité de l'Association. Le Cigref à notamment continué ses activités liées à son cercle cybersécurité, piloté par Christophe Leray et a proposé à ses membres un nouveau groupe de travail consacré à la gestion de crise cyber.

Le Cigref continue également d'échanger avec son écosystème et les pouvoirs publics pour promouvoir un véritable changement de paradigme de la cybersécurité. A ce titre, le Cigref a notamment contribué à l'effort collectif "Convergences numériques 2022" avec 10 autres associations majeures de l'écosystème numérique, pour faire prendre conscience aux candidats à la présidentielle de l'importance du sujet de la cybersécurité, pour les entreprises, les administrations, et au-delà pour notre société. L'association a également conclu deux partenariats stratégiques avec le Pôle d'Excellence Cyber et le Campus Cyber pour agir ensemble en faveur d'un numérique de confiance. Dans cette même optique, elle a répondu à la consultation publique ouverte par la Commission Européenne en début d'année en faveur d'un Cyber Resilience Act. Ce futur règlement propose de définir des exigences en matière de cybersécurité auxquelles devront se conformer leurs fabricants et vendeurs répondant ainsi au constat fait par l'association depuis plusieurs années concernant l'absence préjudiciable de normes sur les produits et services numériques.

Contact

Cigref
21 avenue de Messine
75008 PARIS
Tel : +33 1 56 59 70 00
Email : **cigref@cigref.fr**
Site web : **https://www.cigref.fr**

Clusif

Créé en 1992, mais déjà association de fait depuis 1982, le Clusif est l'association de référence de la sécurité du numérique en France. Sa mission consiste à favoriser les échanges d'idées et de retours d'expérience. Il réunit en parfaite équité au sein de 2 collèges, offreurs et utilisateurs, tous les secteurs d'activité de l'économie autour de la cybersécurité et de la confiance numérique.

Basé au Campus Cyber à La Défense, le Clusif est également présent en région et à l'international à travers les CLUSIR (Clubs de la sécurité de l'information en réseau).

Comment le Clusif aide les entreprises françaises et les administrations.

• **Information :** Le Clusif publie régulièrement, sur son site, des analyses, des recommandations et des méthodologies utiles, qui pourront servir l'entreprise dans l'élaboration et le suivi de sa stratégie de sécurité numérique. Le panorama annuel de la cybercriminalité ou l'étude statistique MIPS (Menaces Informatiques et Pratiques de sécurité) sont deux exemples de publications particulièrement utiles.

• **Rencontres :** Le Clusif permet le brassage des expériences et les rencontres entre offreurs et utilisateurs, au sein de groupes de travail dédiés (pour les membres) ou à l'occasion d'événements publics. Espace RSSI, espace de travail dédié uniquement aux RSSI, sans sponsors et commerciaux, favorise quant à lui l'échange de savoir-faire et de retours d'expériences en toute confidentialité.

• **Influence :** Le Clusif est membre à l'AFNOR du Comité Stratégique Information et communication numérique et de la CN 27 SSI qui s'occupe des travaux de normalisation dans le domaine de la sécurité informatique, membre Utilisateurs du GIP ACYMA (cybermalveillance.gouv.fr). Grâce à sa large représentativité dans le secteur SSI, il est régulièrement consulté par les organismes institutionnels pour recueillir l'avis de la profession que ce soit du côté prestataire ou RSSI.

Contact

Clusif
Tour Eria
5 rue Bellini
92821 Puteaux cedex
Tél : 01 53 25 08 80
Site web : **https://clusif.fr/**
Ecrire : **clusif@clusif.fr**

CNIL

La Commission Nationale de l'Informatique et des Libertés est l'autorité nationale en charge de la protection des données personnelles. Elle a été créée en 1978 par la loi Informatique et Libertés avec le statut d'autorité administrative indépendante.

Si son périmètre ne se limite pas aux technologies de l'information, le numérique occupe bien entendu une place prépondérante dans son activité.

Son action est double : elle accompagne d'une part les entreprises afin de les aider à se mettre en conformité avec la législation sur la protection des données personnelles, et elle aide d'autre part les particuliers à maîtriser leurs données personnelles et exercer leurs droits.

Enfin, en tant que régulateur, elle est amenée à enquêter et sanctionner les entreprises qui ne respecteraient pas la réglementation sur la protection des données personnelles.

Dans le domaine du numérique, la CNIL s'attache notamment aux listes et fichiers nominatifs (clients, prospects) et la nature des informations qu'ils contiennent (coordonnées, commentaires, préférences religieuses, politiques ou sexuelles, notamment). Elle s'assure du bon respect de la réglementation concernant la collecte de ces informations (consentement du sujet), de la finalité du traitement et de la conservation (ou destruction...) des fichiers.

Après l'entrée en vigueur du règlement européen sur la protection des données personnelles (RGPD), la CNIL, outre le contrôle, aide les entreprises à mettre en application les nouvelles obligations introduites par le règlement.

Comment la CNIL aide les entreprises françaises

• **Information et conseil :** La CNIL offre de très nombreuses publications destinées aux entreprises, afin de les aider à se mettre en conformité avec la législation sur la protection des données personnelles. Enfin, la CNIL dispose d'une ligne de support téléphonique dédiée aux entreprises.

• **Outils :** La CNIL propose des outils, des packs de sensibilisation ou des formulaires d'autoévaluation destinés à aider l'entreprise à structurer sa fonction de protection des données à caractère personnel (fiche de poste du Data Protection Officer, formulaires divers...)

• **Certification :** La CNIL peut attribuer une certification à des produits ou des services (des "procédures") et à des organismes. Elle peut attribuer également une certification de compétences aux DPO (non obligatoire pour exercer sa fonction).

Contact

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS
3 Place de Fontenoy - TSA 80715
75334 PARIS CEDEX 07
Tél : 01 53 73 22 22

Cybermalveillance.gouv.fr

Cybermalveillance.gouv.fr est le dispositif national d'assistance aux victimes d'actes de cybermalveillance, de sensibilisation aux risques numériques et d'observation de la menace sur le territoire français. Ses publics sont les particuliers, les entreprises (hors OIV et OSE) et les collectivités territoriales. Le dispositif est piloté par une instance de coordination, le Groupement d'intérêt public (GIP) ACYMA, composé d'une cinquantaine de membres issus du secteur public, du privé et du domaine associatif, et qui contribuent chacun à sa mission d'intérêt général. Cybermalveillance.gouv.fr référence sur sa plateforme des professionnels en sécurité numérique, répartis sur tout le territoire français, pour venir en aide aux victimes.

Cybermalveillance en quelques chiffres :

- **Plus de 570 000 victimes assistées depuis la création du dispositif**
- **50 cybermalveillances identifiées et traitées**
- **Plus de 1200 prestataires de services référencés et plus de 200 labellisés Expert Cyber sur l'ensemble du territoire**
- **56 entités publiques et privées membres du dispositif, unis pour lutter contre la cybermalveillance.**

Le label Expert Cyber :

Depuis février 2021, le dispositif propose aux professionnels un accompagnement adapté délivré par des prestataires de confiance assurant des services de sécurisation, de maintenance et d'assistance en cas d'incident.

Au travers d'un parcours de sécurisation en ligne directement accessible par la plateforme cybermalveillance.gouv.fr, les entreprises, collectivités et associations peuvent être mises en relation avec un prestataire labellisé dans le cadre d'une demande d'installation ou de maintenance, bénéficiant ainsi d'une expertise vérifiée par l'AFNOR couvrant les domaines suivants :

- les systèmes d'informations professionnels (informatique, logiciels bureautiques, messageries, serveurs …),
- la téléphonie (serveurs téléphoniques professionnels),
- les sites internet (administration et protection).

Plus d'informations : **www.expertcyber.fr**

Contact

Cybermalveillance.gouv.fr

Email : **communication@cybermalveillance.gouv.fr**
Site web : **www.cybermalveillance.gouv.fr**
Twitter et Facebook : **@cybervictimes**
Youtube : **Cybermalveillance-gouv-fr**
LinkedIn : **LINKEDIN.COM/COMPANY/CYBERMALVEILLANCEGOUVFR**
Dailymotion : **DAILYMOTION.COM/CYBERMALVEILLANCE**

Hexatrust

HEXATRUST, le groupement des champions français et européens de la cybersécurité et du cloud de confiance.

Les sociétés membres HEXATRUST, sont des startup, PME & ETI, éditeurs de logiciels, fournisseurs de solutions, sociétés de services, à la pointe de la technologie et de l'innovation, pépites françaises de la cybersécurité et du cloud de confiance.

Les sociétés HEXATRUST répondent toutes à des exigences techniques de maturité, sont reconnues en Europe et à l'international par les plus grandes organisations et s'inscrivent dans des logiques de certifications, de labellisations et de souveraineté.

Le catalogue HEXATRUST offre un panorama complet des produits innovants et développés par plus de 80 entreprises du groupement.

Le catalogue de solutions HEXATRUST est « one-stop-shop » pour les clients, il couvre l'ensemble des domaines de la cybersécurité et du cloud de confiance pour répondre aux grands enjeux de conformité réglementaire, de protection contre les cybermenaces et d'accompagnement dans les grands projets de transformation numérique.

Engagées, les entreprises d'HEXATRUST œuvrent ensemble pour promouvoir et construire la filière française de cybersécurité et Cloud de Confiance au sein du Comité Stratégique de Filière « Industrie de Sécurité ».

Les sociétés membres d'Hexatrust oeuvrent ensemble pour promouvoir et construire la confiance dans le Cloud et l'excellence en matière de cybersécurité et contribuent ainsi au rayonnement numérique européen.

Chaque année, retrouvez les sociétés d'HEXATRUST sur le pavillon du FIC, sur l'espace HEXATRUST aux ASSISES de Monaco et lors des Universités d'Eté de la Cybersécurité, qui est l'évènement de la rentrée pour les professionnels de la cybersécurité et du cloud de confiance, la première semaine de septembre.

Contact

HEXATRUST
CAMPUS CYBER
5-7 rue Bellini 92800 PUTEAUX

Email : **contact@hexatrust.com**
Twitter : **@hexatrust**
#UEHT #LesExpertsMonaco
Site web : **http://www.hexatrust.com/**

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

Numeum

Numeum est l'organisation professionnelle de l'écosystème numérique en France. Elle représente les entreprises de services du numérique (ESN), les éditeurs de logiciels, les plateformes et les sociétés d'Ingénierie et de Conseil en Technologies (ICT). Numeum rassemble plus de 2 300 entreprises adhérentes qui réalisent 85% du chiffre d'affaires total du secteur. Présidé par Godefroy de Bentzmann et Pierre-Marie Lehucher, Numeum souhaite mettre le numérique au service de l'humain avec deux ambitions fondatrices : accompagner le pays dans la généralisation et la démocratisation de la formation numérique ; agir au service d'un numérique responsable pour les entreprises, la société, l'Humain et la planète. L'engagement de Numeum repose sur 4 piliers d'actions : la valorisation et la défense des intérêts de ses membres et de leurs métiers, l'incarnation de la France numérique en Europe, l'animation de l'écosystème numérique pour favoriser les synergies et l'innovation, et le renforcement du service à toutes les entreprises du numérique. Numeum est membre de la fédération Syntec. Le secteur du numérique représente plus de 60,8 Md€ de chiffre d'affaires et 572 126 employés en France.

La cybersécurité est au cœur des préoccupations de Numeum qui a créé en 2015 une Commission Cybersécurité réunissant une centaine d'entreprises autour d'objectifs communs.

Les axes principaux d'actions de cette Commission sont :

- Favoriser les échanges et renforcer la place de Numeum au sein de l'écosystème en tant qu'acteur de la cybersécurité,
- Rendre attractive la filière cybersécurité pour attirer les talents,
- Informer et sensibiliser les utilisateurs
- Faire connaître les solutions de cybersécurité.

Contact

Numeum
148 Boulevard Haussmann,
75008 Paris
Tel : +33 (0)1 44 30 49 70
Email : **contact@numeum.fr**
Site web : **www.numeum.fr**

INFORMER
pour transformer l'entreprise

La dématérialisation, le Cloud,
les communications unifiées,
les nécessités de la cybersécurité
transforment le travail et toute l'entreprise,
les services publics.
Le magazine, le site, ses newsletters
vous informent sur cette actualité mouvante
et vous aident à décoder les tendances



Abonnez-vous

www.solutions-numeriques.com/abonnement/

Toutes les ressources et newsletters en ligne

Pour répondre à vos besoins d'information



- La cybersécurité vous concerne ? Cliquez sur l'onglet. Vous trouverez les infos, l'annuaire, le lexique, etc
- L'emploi, les salaires, les formations, les offres vous intéressent ? Le site sur l'Emploi dans le numérique est à votre disposition
- Votre site Télétravail. Infos et bonnes pratiques pour le travail à distance et le travail hybride
- Solutions Channel. L'info des partenaires, intégrateurs, distributeurs

www.solutions-numeriques.com



SPÉCIALISTE MONDIAL DE L'IDENTITÉ ET DES SERVICES DE CONFIANCE

Partenaire de confiance des Etats et des entreprises, IN Groupe porte une vision européenne de la protection des données et de l'identité comme garantie d'une cyber sécurité résiliente.

IN Groupe s'appuie sur sa marque Nexus pour fournir des solutions de confiance facilitant la gestion des identités sécurisées, des personnes et des objets.

IN GROUPE

LE DROIT D'ÊTRE SOI

CAMPUS CYBER
ACTEUR ENGAGÉ