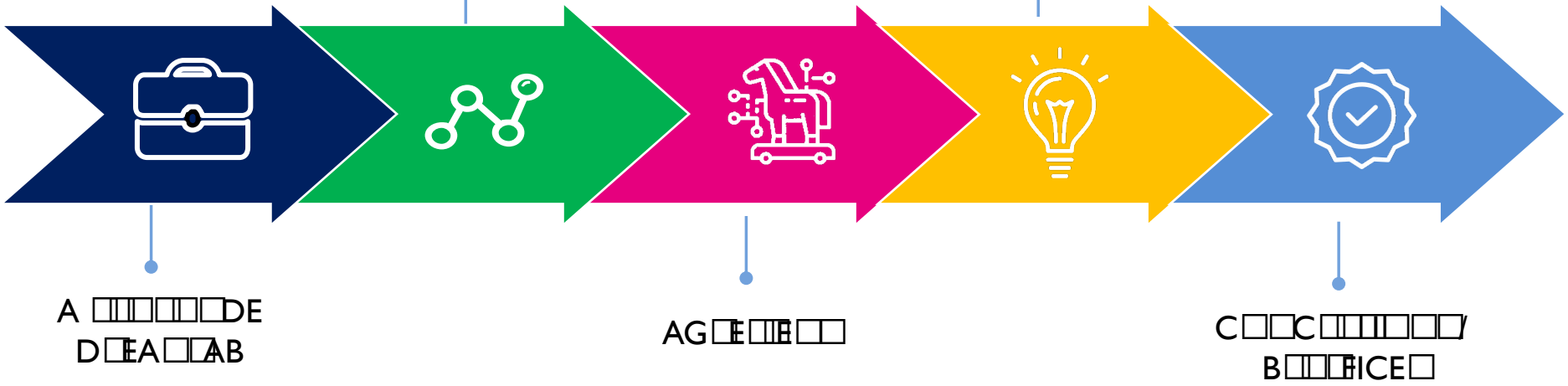
Nicht Glauben. Wissen.

Dreamlab Technologies AG

JFIN | Neuchâtel | Septembre 2023

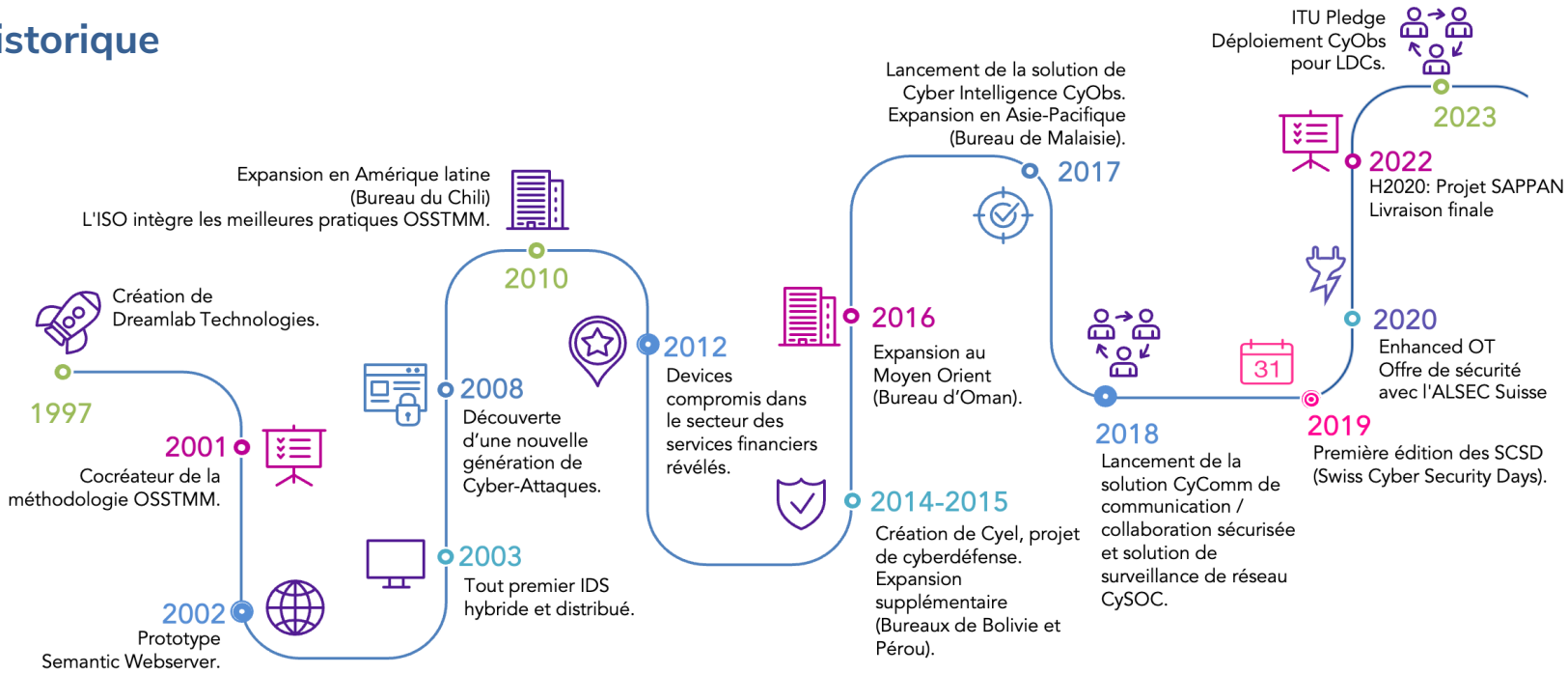
Agenda



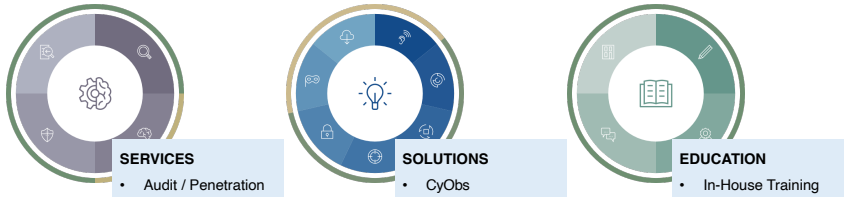
Dreamlab Technologies

DREAMLAB TECHNOLOGIES

Historique



Portfolio



SERVICES
- Audit / Penetration Testing
- Red/Blue Teaming
- Threat Hunting
- Security Consulting
- Cyber Intelligence
- Forensics

SOLUTIONS
- CyObs
- CySOC
- CyComm/KOLAB
- Anonymizer Network
- CyTac
- Honeykube
- RATspotting
- DLIS
- Cyel

EDUCATION
- In-House Training
- Workshop Facilitation
- Customised Solutions
- Certification Programmes
- Online Training

Réseau de parnetaires

ISECOM
Board member of the Institute of Security & Open Methodologies.

W3C
Member of the World Wide Web Consortium for security standards.

OWASP
Member of the Open Web Application Security Project.

ALSEC
Cybersecurity Consulting Partner specializing in the operation of critical technological infrastructure (OT)

FACHHOCHSCHULE NORDWESTSHWEIZ
Collaborator on educational and investigative cybersecurity projects.

SWIFT
Certified Partner for SWIFT's Customer Security Program (CSP)

EUROPEAN UNION
Member of the EU's investigation program Horizon 2020.

CYBERSECURITY MADE IN EUROPE
Recognition of the quality of our cybersecurity services and products.

Black Hat
Member of the Review Committee for the international cybersecurity conference Black Hat.

BERNER FACHHOCHSCHULE
Partner in investigation projects focused on e-commerce security solutions.

SWISS CYBER SECURITY DAYS
Founder & Member of the Organizing Committee

ITU – INT. TELECOMMUNICATION UNION
Telecommunication Development Sector Member

Dreamlab

Dreamlab Technologies

Focus sur 2 initiatives

SWISS CYBER SECURITY DAYS 2024
BERNEXPO | 20.02. & 21.02.2024

SHAPING CYBER RESILIENCE

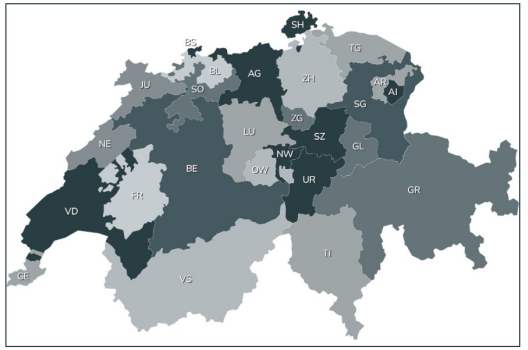
Les Swiss Cyber Security Days (SCSD) sont la principale plateforme suisse de dialogue et de connaissances dans le domaine de la cybersécurité. SCSD comble le fossé des connaissances entre la technologie, la recherche, la politique, les entreprises et le grand public, en fournissant un aperçu des menaces actuelles et futures, ainsi que des solutions innovantes pour améliorer la sécurité.

Site Web: https://scsd.ch/

Swiss Cybersecurity Start-Up Map

La carte suisse des start-ups en cybersécurité

Explorer l'avenir de l'innovation suisse en matière de cybersécurité



Explorez la Swiss Cybersecurity Start-Up Map pour en savoir plus sur les entreprises et leurs produits.

Découvrir

Retrouvez toutes les start-up suisses de cybersécurité en un seul endroit. Téléchargez la dernière version de la Swiss Cybersecurity Start-Up Map.

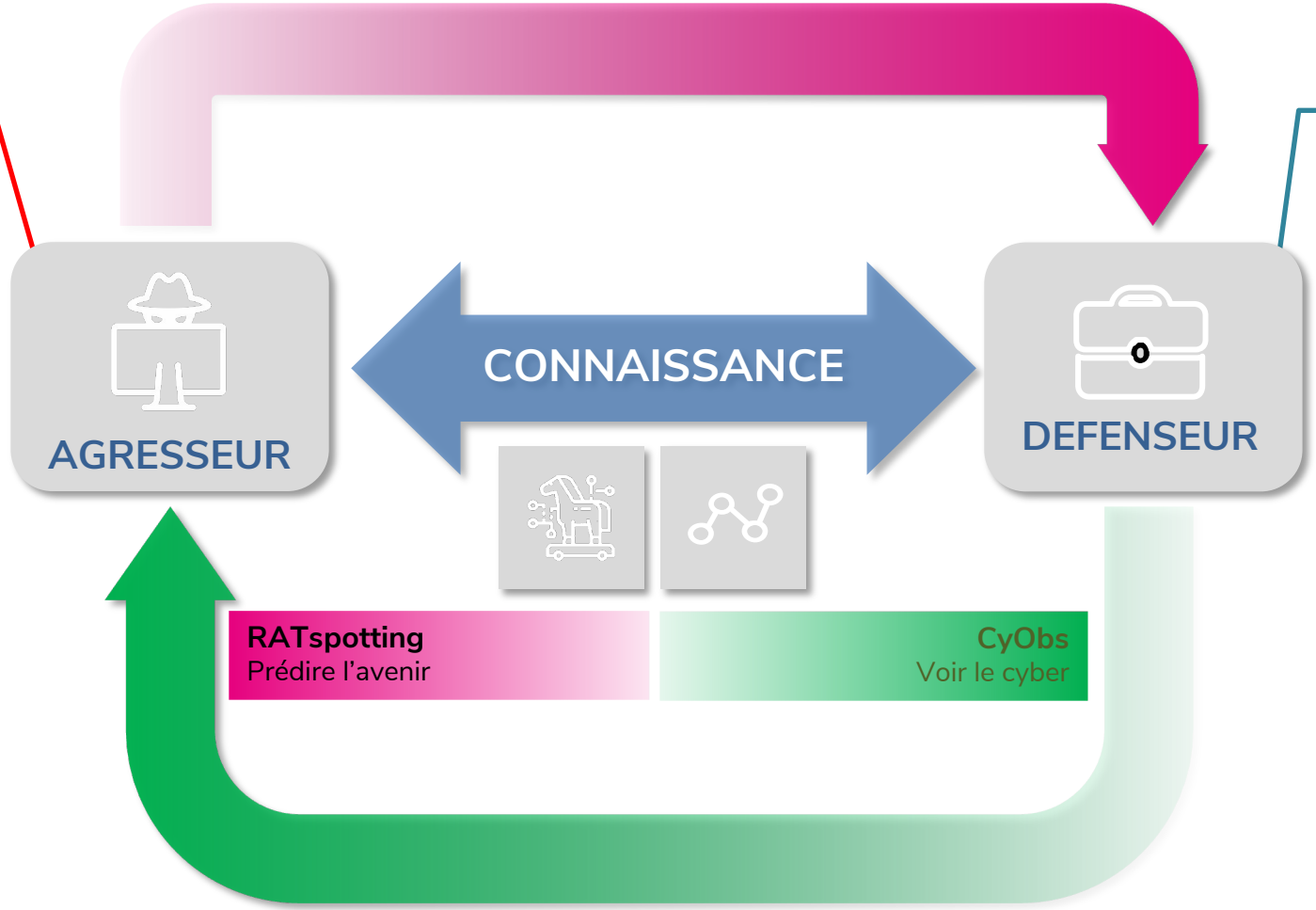
Explorer

Site Web: https://cysecmap.swiss/

Contexte / Approche Compréhensive

Le Conundrum de la Cybersécurité

- Avoir le temps
- Élaborer une stratégie
- Connaissance victimes
- Trouver une seule faille
- Être discret
- Persistance



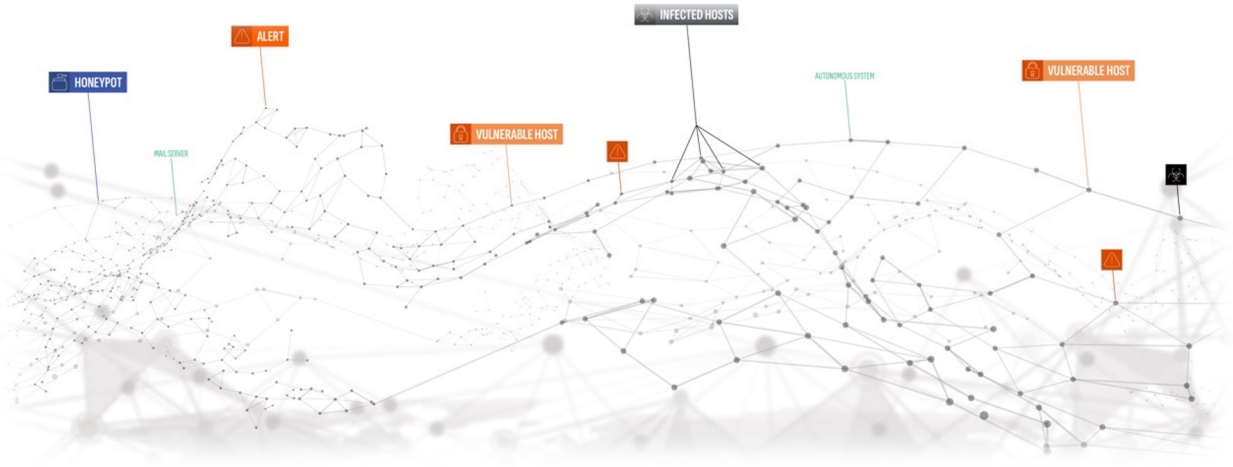
- Connaitre l'écosystème
- Se préparer
- Savoir se défendre
- Être efficace à 100%
- Prévenir les attaques
- Détecter au plus tôt
- Réagir au plus vite
- S'exercer

CYOBS
SEE THE CYBER

DREAMLAB
TECHNOLOGIES

CyObs est un système de cyber-radar de haute précision capable de **cartographier**, d'**analyser** et de **visualiser** la surface d'attaque du cyberespace de tout un pays, un secteur industriel jusqu'à un niveau granulaire d'une organisation ou SME/SMI.

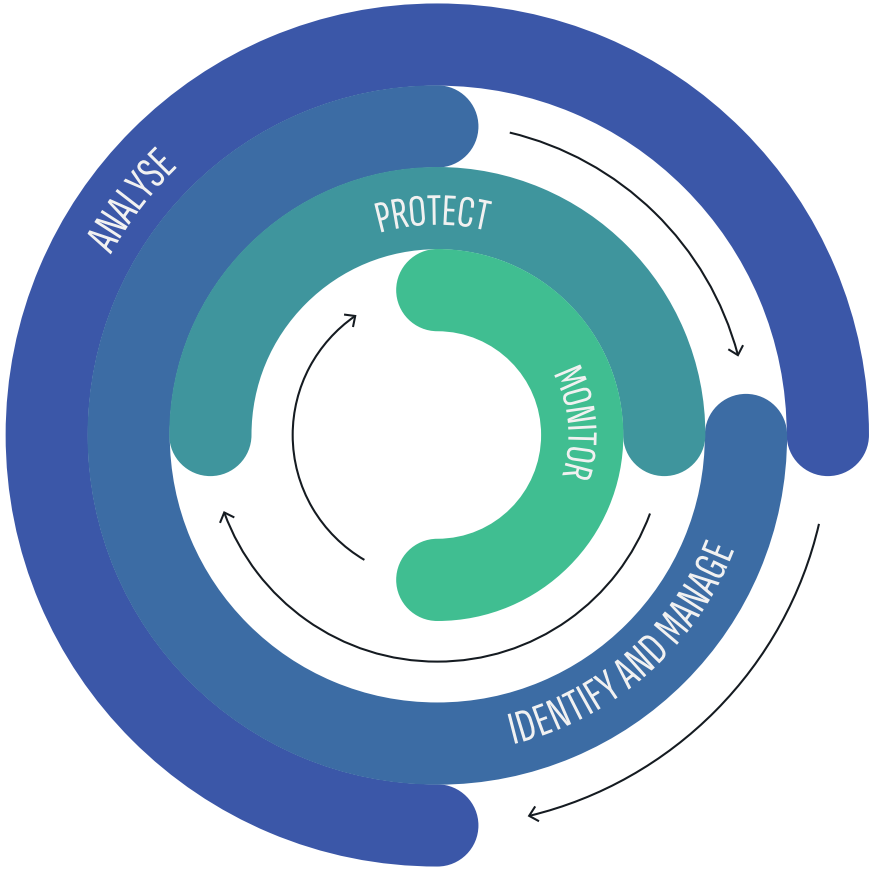
SI VOUS NE POUVEZ PAS LE VOIR,
VOUS NE POUVEZ PAS LE GÉRER.
SORTEZ DE L'OBSCURITÉ.



CyObs - Solution pour une cybersécurité gobale - Défense

Facteurs clés dans la création d'une architecture de cybersécurité sécurisée

- Obtenir une **compréhension globale** de son environnement cyber.
- **Mesurer** et **gérer** de son cyberespace de façon cohérente.
- **Identifier et gérer** de manière **proactive** les **vulnérabilités** des infrastructures numériques.
- **Classer par ordre de priorité** les correctifs pour réduire considérablement la surface d'attaque.
- Identifier les activités inhabituelles et les menaces potentielles avec une **détection d'anomalies**.
- Améliorer sa posture de sécurité globale grâce à une surveillance en **temps réel**.

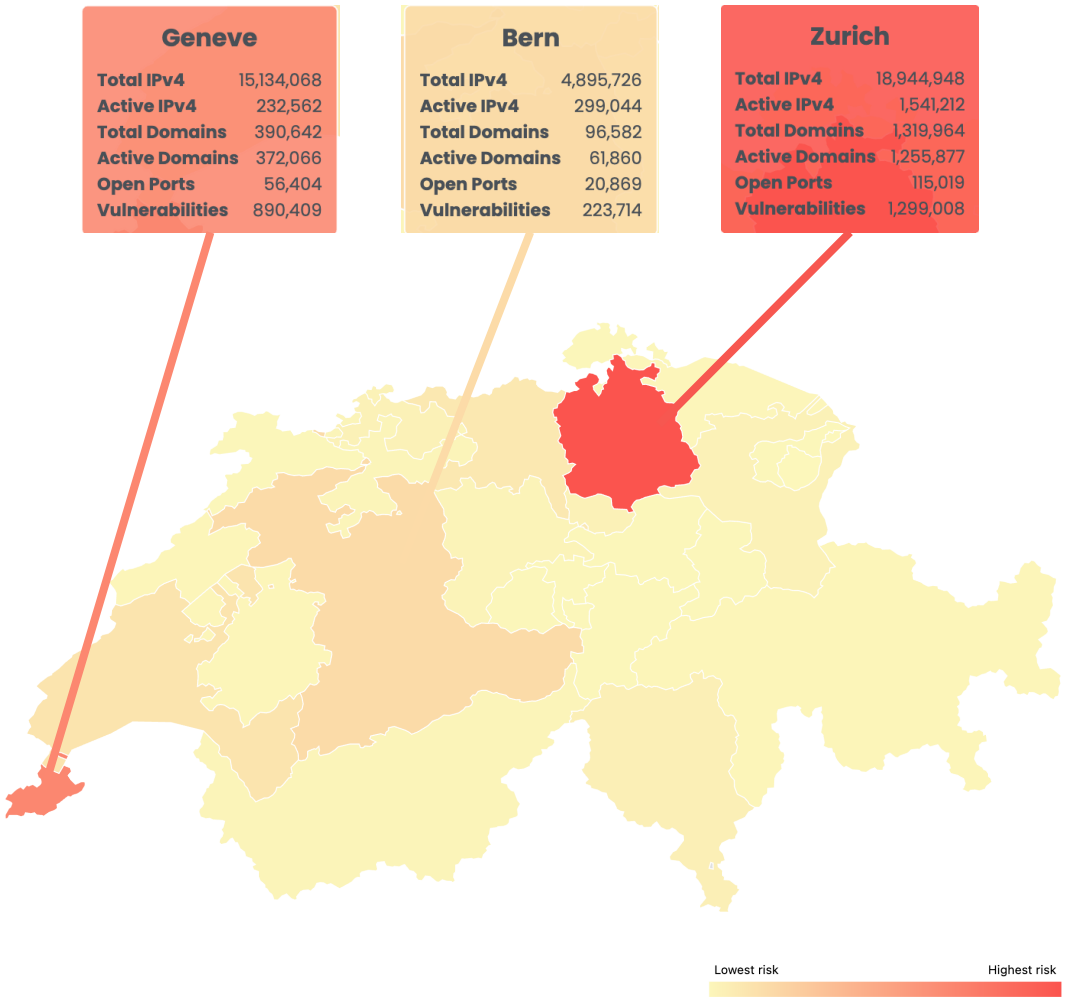


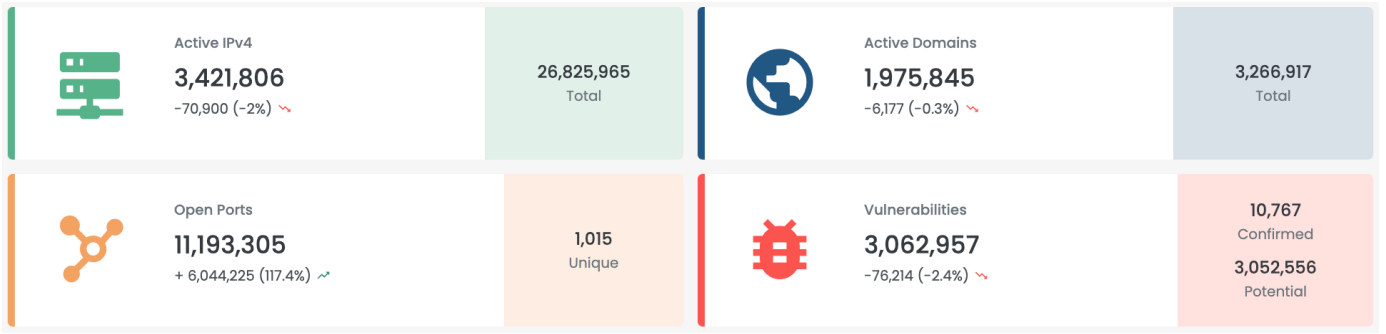
CyObs est un référentiel et moteur de recherche de surface d'attaque présente globalement :

- Numérisation / indexation / stockage,
- Données historiques,
- Cyberespace complet – **IP / Domaines / Noms de domaine / Services de messagerie**,
- Prise d'empreintes digitales - **OS / Logiciels / Services**,
- Détection des vulnérabilités avec classification automatique.

CyObs - Cyberespace Suisse

Aperçu des risques de sécurité





Le tableau de bord principal présente un aperçu rapide de l'état du cyberespace dans un pays donné, ainsi que des faits concrets collectés à partir de diverses sources, telles que :

- Espace IP utilisé,
- Nombre de domaines,
- Volume de ports ouverts exposés directement à Internet,
- Nombre de vulnérabilités trouvées,
- Dépendances,
- Entités impactées.

Le CyObs dresse un **tableau global de la maturité** du cyberespace national.

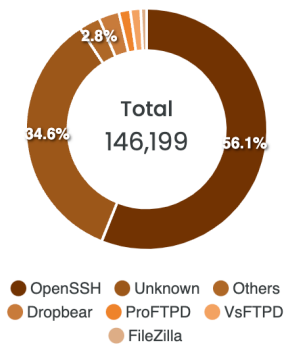
Source: Dreamlab Technologies AG, CyObs & Audit Department, Septembre 2023 - Informations collectées entre le **2 octobre 2022** et le **6 septembre 2023**.

CyObs - Cyberespace Suisse

Analyse – Systèmes d'exploitation et logiciels

5,720	155	416,828	101,417
Unique software	Unique OS	Hosts exposing	Hosts exposing OS information

Remote Administration Interfaces (RAI)



Services	
33,930	FTP
104,416	SSH
1,134	TELNET

Le scan révèle 146'199 interfaces administration à distance.

Certains groupes de hackers ciblent ces interfaces pour accéder illégalement aux organisations, organismes gouvernementaux, universités en :

- Utilisant un « brute force » des identifiants/mots de passe,
- Exploitant des services vulnérables.

Une fois récoltés, ces accès sont vendus à des groupes de ransomwares et sur des forums spécialisés sur le darknet.

>> L'EXPOSITION D'INTERFACES D'ADMINISTRATION À DISTANCE NON PROTÉGÉES EST UN RISQUE DE SÉCURITÉ GRAVE

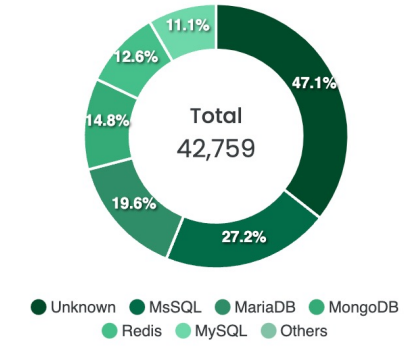
Il existe 42'759 bases de données exposées directement à Internet.

Les pratiques générales en matière de déploiement d'infrastructure consistent à ne jamais exposer directement ces services à Internet. Utilisez plutôt un reverse-proxy ou une interface d'administration via une connexion sécurisée telle qu'un VPN par exemple.

L'accès direct via Internet démultiplie la probabilité que ces bases de données soient piratées et présente un risque sérieux de fuite de données ou de perte d'intégrité des données (empoisonnement/manipulation des données).

>> PRATIQUE À ÉVITER AUTANT QUE POSSIBLE

Databases



Services	
17,259	SQL Databases
436	NoSQL Databases

Source: Dreamlab Technologies AG, CyObs & Audit Department, Septembre 2023 - Informations collectées entre le **2 octobre 2022** et le **6 septembre 2023**.

CyObs - Cyberespace Suisse
Analyse – Vulnérabilités

L'analyse des vulnérabilités aide les utilisateurs à se concentrer sur les domaines présentant le plus grand risque, en guidant les efforts de sécurité, de remédiation et de priorisation.

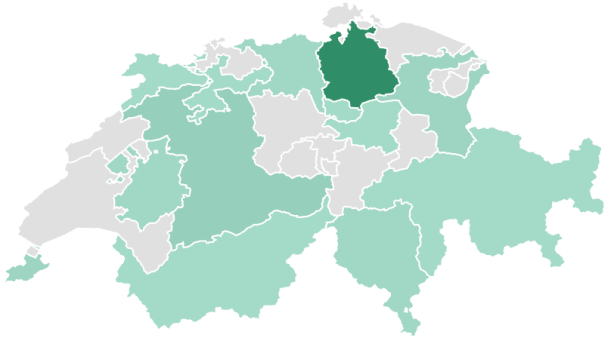
CyObs aide les gouvernements, les Agences Nationales de cybersécurité et les CERT (Computer Emergency Response Teams) à sensibiliser l'opinion aux cybermenaces et à aider d'autres organismes gouvernementaux, entreprises, universités et organisations d'infrastructures critiques à se protéger en :

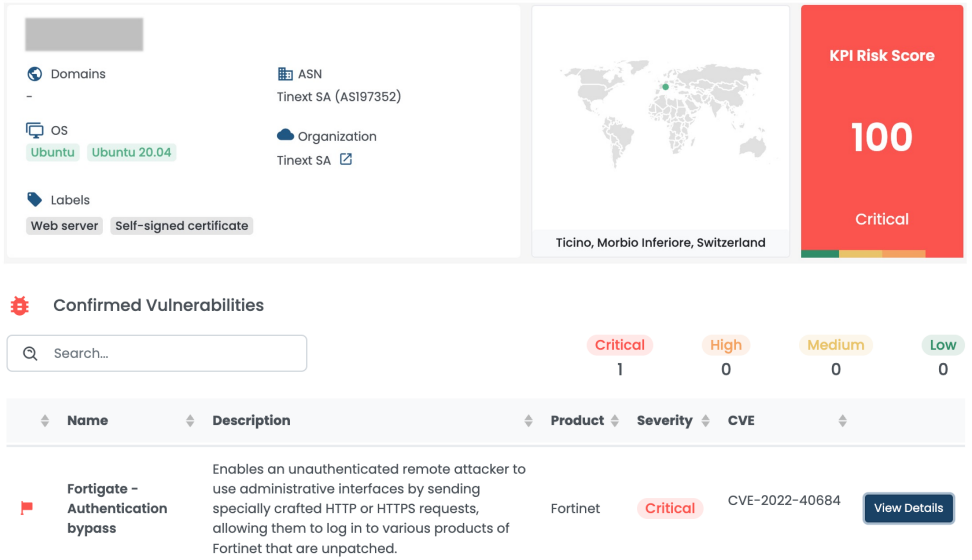
- **Préparer et déployer des stratégies de correctifs** améliorées, une gestion des vulnérabilités et des plans de protection contre la cybersécurité.
- **Identifier les campagnes de formation ou de sensibilisation nécessaires** pour des secteurs, des régions ou des communautés spécifiques.
- Fournir aux décideurs politiques les informations dont ils ont besoin pour **créer et appliquer des réglementations réduisant le risque de cyberattaques**.

Source: Dreamlab Technologies AG, CyObs & Audit Department, Septembre 2023 - Informations collectées entre le **2 octobre 2022** et le **6 septembre 2023**.

CyObs - Cyberespace Suisse

Analyse – Vulnérabilités – Example FORTIGATE





L'analyse de septembre 2023 montre que 11 mois après la publication du correctif, il existe encore 57 vulnérabilités (initialement plus de 800) affectant diverses organisations suisses.

Top Locations

Name	Quantity
Zurich	34
Bern	5
Geneve	3
Sankt Gallen	3
Ticino	2

10 octobre 2022: Fortigate permet à un agresseur distant non authentifié d'utiliser des interfaces d'administration en envoyant des requêtes HTTP ou HTTPS spécialement conçues, lui permettant de se connecter à divers produits Fortinet qui ne sont pas corrigés.

20 octobre 2022 : Patch - Versions corrigées du système d'exploitation sont disponibles.

>> VULNÉRABILITÉ HAUTEMENT CRITIQUE - ELLE PEUT ÊTRE UTILISÉE POUR CONTOURNER L'AUTHENTIFICATION. LES PRODUITS CONCERNÉS SONT UTILISÉS COMME ROUTEURS ET PARE-FEU. L'ABSENCE DE MISE A JOUR POSE UNE RELLE MENACE, PERMETTANT POTENTIELLEMENT L'ACCÈS À L'ENSEMBLE DU TRAFIC DE L'ORGANISATION.

Le CyObs identifie de nouvelles vulnérabilités dans tout le pays à une vitesse fulgurante.

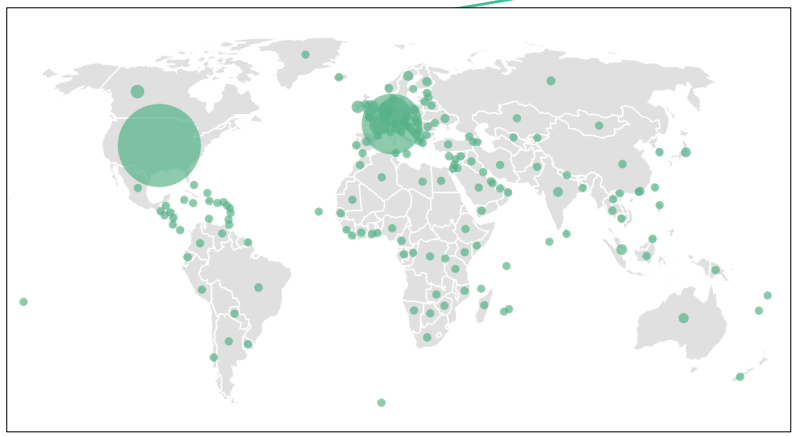
Source: Dreamlab Technologies AG, CyObs & Audit Department, Septembre 2023 - Informations collectées entre le **2 octobre 2022** et le **6 septembre 2023**.

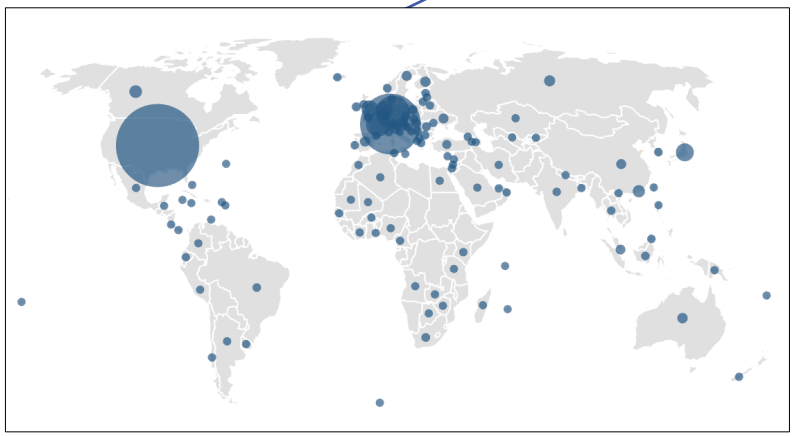
CyObs - Cyberespace Suisse

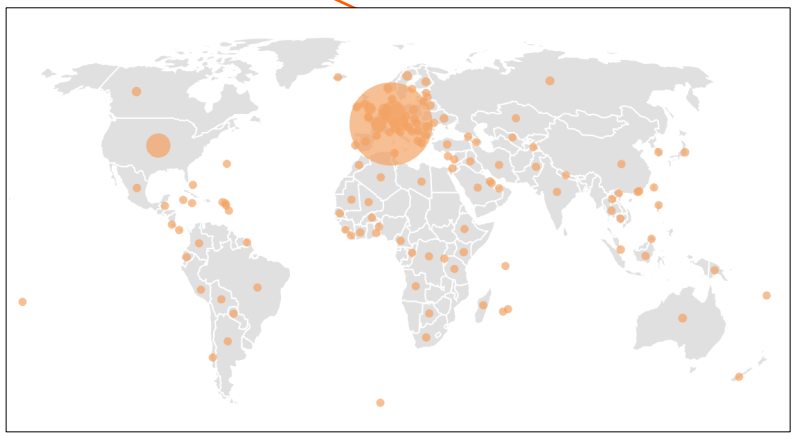
Analyse – Dépendances géographiques mondiales

DREAMLAB TECHNOLOGIES

3,266,917 Domains	Active Domains	Name Servers	Mail Exchange
	1,975,845	3,378,029	2,602,387
	1,975,845 Serving a service	35,498 Unique IP addresses	51,750 Unique IP addresses
	3,266,335 SOA configured	3,381,162 Namespaces with NS	2,602,387 Namespaces with MX







Les dépendances indiquent le degré d'autonomie d'un pays à l'égard d'autres pays pour l'hébergement de:

- **domaines**
- **serveurs de noms**
- **services de messagerie**

Les organisations doivent se conformer à de nombreux cadres juridiques (ex. RGPD,...), mais les **tensions géopolitiques** peuvent également affecter la **souveraineté** dans le cyberespace.

CyObs visualise et souligne pour la première fois ces dépendances géographiques.

Source: Dreamlab Technologies AG, CyObs & Audit Department, Septembre 2023 - Informations collectées entre le **2 octobre 2022** et le **6 septembre 2023**.

DREAMLAB TECHNOLOGIES

RATspotting adopte une **approche proactive** dans la détection de types spécifiques de **serveurs de commande et de contrôle (C2)** via une analyse massive à l'échelle d'Internet en les détectant avant que l'adversaire ne lance ses campagnes d'attaques.

RATspotting

LE POUVOIR DE **PRÉVENIR LA CYBERCRIMINALITÉ** ET **PREDIRE L'AVENIR**

RATspotting – Solution d'anticipation

Méthodes courantes de détection réactive des logiciels malveillants

Les agresseurs modifient généralement l'application client, soit en encodant le shellcode, en chiffrant la charge utile, en compressant l'exécutable, etc.

 # 01

Scan Signature-based

Se fonde sur une base de données de signatures de virus connus.

 # 02

Analyse Heuristique

Détecte les virus en termes de similitude avec d'autres virus apparentés et connus

 # 03

Analyse comportementale en temps réel

Basé sur la surveillance et l'identification des actions inattendues

 # 04

Analyse Sandbox

Déplace les fichiers suspects vers un sandbox pour protéger le reste du réseau

 # 05

Détection DGA avec ML

Techniques de ML utilisées pour classer les domaines générés en bénins/malveillants

RATspotting

RATspotting – Solution d'anticipation

DREAMLAB TECHNOLOGIES

Zoom sur le DGA - Domain Generation Algorithms -

Cadre de Recherche:
- Recherche de domaine malveillants uniquement basé sur le nom de domaine
- TLD .ch à travers la liste des domaines publiés par SWITCH .ch-zonefile

Horizon 2020

SAPPAN — *SHARING AND AUTOMATION FOR PRIVACY PRESERVING ATTACK NEUTRALIZATION*

 # 05

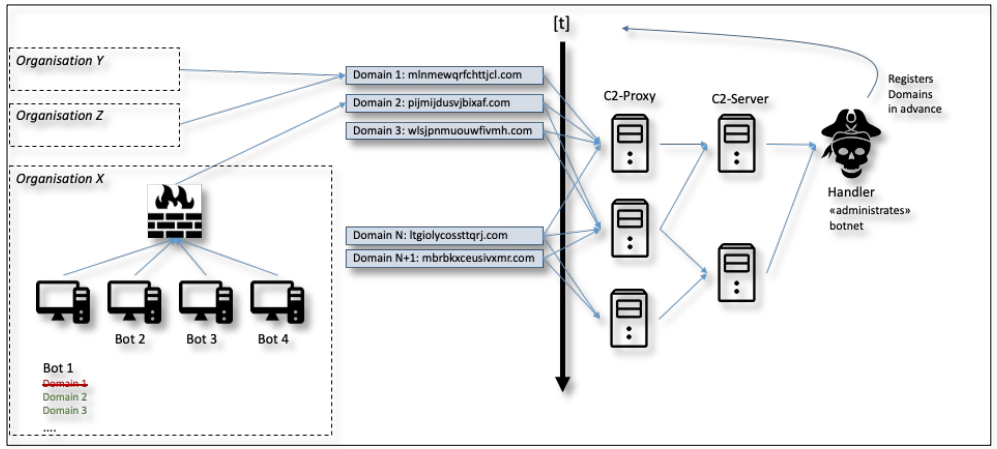
Détection DGA avec ML

Techniques de ML utilisées pour classer les domaines générés en bénins/malveillants

Malware et C2

Traditionnellement:
- Analyse échantillons logiciels malveillants
- Extraction des adresses IP et/ou des URL comme indicateurs de compromission (IOC),
- Mise sur liste noire toutes les communications impliquant ces IOCs.

Nouvelle technique: **Domain Generation Algorithms**
- Créer des domaines à partir de « seed values ».
- Algorithme déterministe: une valeur d'entrée produira toujours le même domaine de sortie



Example de campagne:
- Flubot ciblant devices Android
- APT Solarwinds/Sunburst

Site web: https://sappan-project.eu/

Article Complet: https://dreamlab.net/en/blog/post/detecting-suspicious-ch-domains-using-deep-neural-networks/

DGA

RATspotting – Solution d'anticipation

DREAMLAB TECHNOLOGIES

Horizon 2020

SAPPAN — SHARING AND AUTOMATION FOR PRIVACY PRESERVING ATTACK NEUTRALIZATION

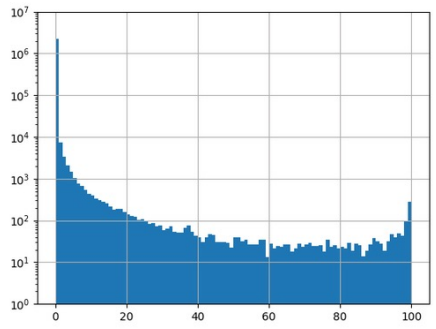
Zoom sur le DGA - Domain Generation Algorithms -

Architecture du modèle

- Différents types de **réseaux de neurones** profonds étudiés / comparés dans le passé.
- Architecture retenue « **stacked convolutional neural network model architecture / 2 layers** » (deep neural network calissifer).
- Modèle retenue capables de classer les domaines malveillants générés avec une **précision de 97-98 %.**
- **Rapide** pour l'évaluation et **précision** similaire à d'autres architectures plus complexes.
- **Temps de calcul raisonnable**.

Utilisation initiale

Application du modèle aux 3.9 millions de domaines .ch comme training dataset

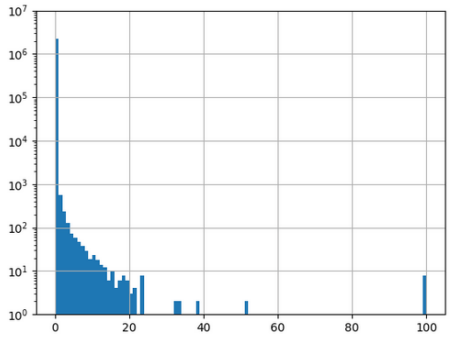


Grand nombre de classifications à haute certitude (1 699 domaines avec plus de 50%)

➢ Rend difficile une inspection manuelle

Amélioration du training dataset

Par approximation: si un domaine à au moins 1 MX record, il est plus susceptible d'être inoffensif (configuration d'un MX record signifie plus d'efforts pour un acteur malveillant).



Environ 72% de tous les domaines .ch avec 1 MX record

➢ Ajout de 1,6 million d'échantillons supplémentaires à l'ensemble de données d'entraînement).

Résultat final

Identification de 19 domaines avec une certitude >50%,

- 9 - très probablement malveillants.
- 5 - confirmés comme inoffensifs par inspection manuelle.
- 5 - domaines avec aucune adresse IP et non blacklistés.

Domain	Certainity (model output)	Analysis / Conclusion (result of manual SOC-style investigation)
abcdefghijklmnopqrstuvwxyz.ch	100%	**Likely malicious**, currently resolves to suspicious IP
adslkfalkfjlkfjdsalkfafjjflsa.ch	100%	**Unclear**, no IP resolution
8qswldnsrvb73xkczdyj.ch	99.9%	**Likely malicious**, Currently resolves to suspicious IP, used to resolve to another suspicious IP involved in coronavirus-scam
rgdfgdfgdfgdf.ch	99.9%	**Likely benign**, no suspicious observations
utitan101310bgfhnythjdukfdyjt.ch	99.8%	**Likely benign**, no suspicious observations
sfdfgdfgdfgdfgdfg.ch	99.8%	**Unclear**, no IP resolution
n7g9ipiddq9lhtx.ch	99.1%	**Likely malicious**, currently resolves to suspicious IP
testhgfjdgdfxhgxdfhx12.ch	99.1%	**Likely malicious**, currently resolves to suspicious IP, IP has been flagged as botnet C2
oiqweurpui345345jk.ch	94.1%	**Likely benign**, no suspicious observations
ymfvrcnwyw.ch	92.5%	**Unclear**, no IP resolution
aqdddwxszedc.ch	84.8%	**Unclear**, no IP resolution
ihij8qltfyfe.ch	82.2%	**Likely malicious**, domain blacklisted, currently resolves to cloudflare IP
asdfjkhdsfajdfsajhsadf.ch	77.1%	**Likely benign**, no suspicious observations
7as6q796d6s98q6qd6sdq.ch	72.6%	**Likely malicious**, Currently resolves to suspicious IP
rggrgrgrgrgr.ch	66.5%	**Unclear**, no IP resolution
fj6f8j1gbwzl.ch	54.6%	**Likely malicious**, used to resolve to suspicious cloudflare IP (with very little associated URLs)
fdsafdahkjfdhajkfdas.ch	52.2%	**Likely malicious**, Currently resolves to suspicious IP
xczjhkgdsadsa.ch	51.3%	**Likely malicious**, Currently resolves to suspicious IP
ik48lsu5dww485letzk9m7f.ch	51.1%	**Likely benign**, no suspicious observations

DGA

Site web: https://sappan-project.eu/

Article Complet: https://dreamlab.net/en/blog/post/detecting-suspicious-ch-domains-using-deep-neural-networks/

RATspotting – Solution …

DREAMLAB TECHNOLOGIES

Zoom sur le DGA - Domain Generation Algorithms -

Horizon 2020

SAPPAN — SHARING AND AUTOMATION FOR PRIVACY PRESERVING ATTACK NEUTRALIZATION

2019 - 2022

- Technique utilisée par l'industrie cybersécurité par les CERT et SOC. Cependant la méthode utilisée dans SAPPAN révèle un **nombre beaucoup plus faible de faux positifs** et d'alertes à vérifier manuellement.
- Méthode fonctionnant à un niveau acceptable pour identifier des domaines suspects à partir d'un très grand ensemble de données.
- Existe toujours des **faux positifs** dans cet ensemble, mais en **quantité plus faibles**.
- Préoccupation, **taux de détection plutôt faible** en volume. Cela peut être contré en abaissant le seuil de classification à des pourcentages inférieurs (inférieurs à 50 %), ce qui à son tour augmenterait significativement le nombre de faux positifs.
- Pour une implémentation en production, le **seuil de détection optimal doit être étudié plus en détail**.
- Une **inspection manuelle est toujours utile** afin qu'un analyste valide les domaines malveillants détectés.
- On peut également envisager d'autres moyens d'améliorer encore la précision de cette méthode en utilisant des données supplémentaires et en ne s'appuyant pas uniquement sur le réseau neuronal pour la détection.
- Nous continuons nos recherches d'approfondissement sur ces sujets. Intégration déjà disponible dans notre solution CySOC.

DGA

Site web: https://sappan-project.eu/

Article Complet: https://dreamlab.net/en/blog/post/detecting-suspicious-ch-domains-using-deep-neural-networks/

RATspotting – Solution d'anticipation

DREAMLAB TECHNOLOGIES

Méthodes courantes de détection réactive des logiciels malveillants

Les agresseurs modifient généralement l'application client, soit en encodant le shellcode, en chiffrant la charge utile, en compressant l'exécutable, etc.

 # 01

Scan Signature-based

Se fonde sur une base de données de signatures de virus connus.

 # 02

Analyse Heuristique

Détecte les virus en termes de similitude avec d'autres virus apparentés et connus

 # 03

Analyse comportementale en temps réel

Basé sur la surveillance et l'identification des actions inattendues

 # 04

Analyse Sandbox

Déplace les fichiers suspects vers un sandbox pour protéger le reste du réseau

 # 05

Détection DGA avec ML

Techniques de ML utilisées pour classer les domaines générés en bénins/malveillants

RATspotting

MAIS SI LES AGRESSEURS SE CONCENTRENT SUR LA MODIFICATION DU CLIENT, POURQUOI NE NOUS FOCALISONS PAS SUR...

LES SERVEURS MALVEILLANTS ?

RATspotting – Solution d'anticipation

Facteurs clés

- **Identifier** et comprendre les **menaces avant qu'elles ne se concrétisent**.
- Se familiariser avec les **stratégies et les tactiques utilisées par les agresseurs**.
- Ériger une **défense préventive** plutôt que réactive pour **anticiper les attaques** plutôt que d'y répondre.
- Intégrer des **analyses supplémentaires à vos IDS** ainsi qu'à d'autres outils de surveillance pour renforcer votre position globale en matière de sécurité.
- Collecter des **preuves détaillées** sur les attaques menées.
- Mettre en place des **mesures de protection** pour se défendre **contre les groupes APT** avant qu'ils n'entreprennent une campagne d'attaque.

PRÉVENTION PROACTIVE DES MENACES

SURVEILLER LES CAMPAGENES MALVEILLANTES

RENFORCER SES DEFENSES

COLLECTER DES PREUVES

RATspotting

RATspotting – Solution d'anticipation

DREAMLAB TECHNOLOGIES

Scan d'Internet massif et détection de C2 par prise d'empreintes digitales

Méthode

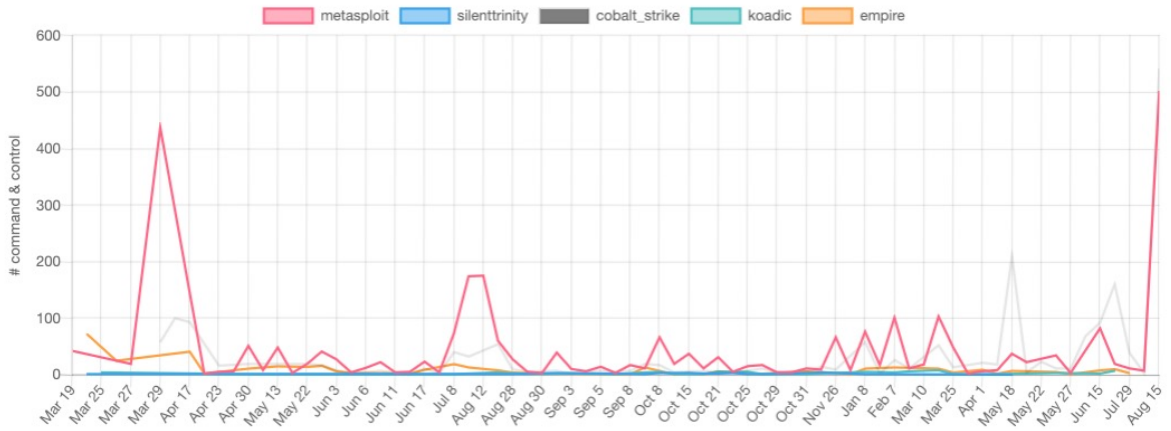
- Implique l'analyse des ports et la détection des services sur l'ensemble d'Internet.
- Les serveurs C2 prétendent la plupart du temps être un autre logiciel, comme un web serveur (IIS ou Apache).
- Faire la distinction entre les infrastructures réelles et les imitateurs.

Effets

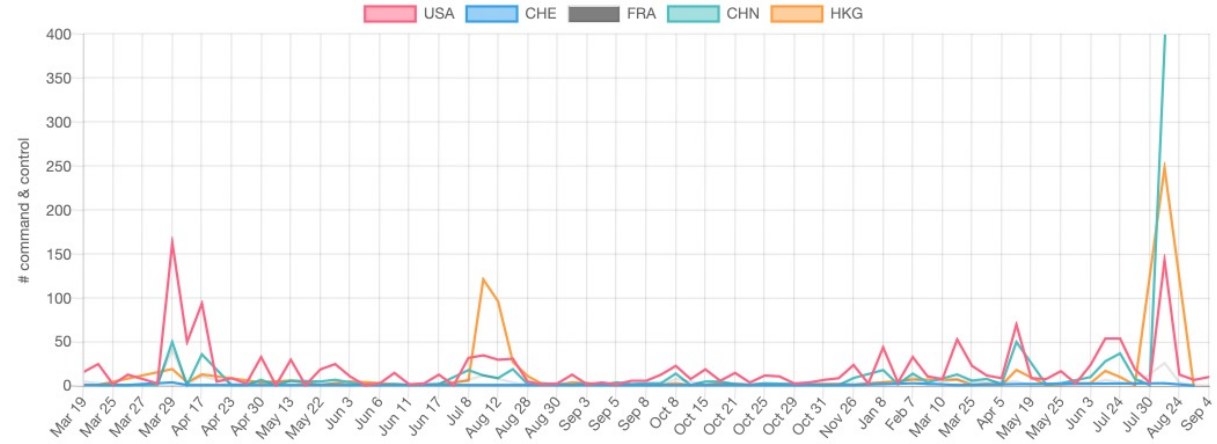
- Possible de détecter un C2 avant que le fichier malveillant ne soit produit.
- Détection alors que les adversaires sont encore en train de mettre en place leur infrastructure.
- La détection précoce permet de collecter des informations supplémentaires telles que les fichiers exposés en fonction de l'opsec de l'adversaire.
- Détecter les logiciels C2 les plus utilisés

NOMBRE	%	TYPE DE MALWARE
32176	77.5%	cobalt_strike
8364	20.2%	metasploit
491	1.2%	empire
171	0.4%	poshc2
136	0.3%	koadic
94	0.2%	responder
40	0.1%	silenttrinity
24	0.1%	merlin
6	0.0%	trevorc2
1	0.0%	pupy
0	0.0%	covenant
41503		

GRAPH MALWARE



GRAPH COUNTRY



RATspotting

RATspotting – Solution d'anticipation

DREAMLAB TECHNOLOGIES

Scan d'Internet massif et détection de C2 par prise d'empreintes digitales

Données Collectées

1. IP
2. Port
3. C2 Type
4. Payload served (tcp, http, etc)
5. Certificates
6. Detection daytime

Nouvelles infrastructures C2 – Août 2023

IP	PORT	TYPE	PAYLOAD	COUNTRY	FLAG	CERTIFICATE	FIRST DETECTION	LAST DETECTION	JARM	OTX PULSES
	443	brute_ratel		Switzerland		localhost	2023-08-31 09:33	2023-08-31 09:33	3fd21b20d00000021c43	0
	3790	metasploit	metasploit/webui	Switzerland			2023-08-15 12:48	2023-08-15 12:48		0
	3790	metasploit	metasploit/webui	Switzerland			2023-08-15 12:48	2023-08-15 12:48		0
	3790	metasploit	metasploit/webui	Switzerland		localhost	2023-08-15 12:48	2023-08-15 12:48	2ad2ad0002ad2ad0002	2

IP	PORT	TYPE	PAYLOAD	COUNTRY	FLAG	CERTIFICATE	FIRST DETECTION	LAST DETECTION	JARM	OTX PULSES
	80	responder	http_v2	France			2023-09-04 13:59	2023-09-04 13:59		0
	443	brute_ratel		France		nvidia.com	2023-08-31 09:33	2023-08-31 09:33	3fd21b20d00000021c43c	0
	443	sliver		France		localhost	2023-08-24 14:16	2023-08-24 14:16	3fd21c20d00000021c43d	0
	443	sliver		France		localhost	2023-08-24 14:16	2023-08-24 14:16	3fd21b20d00000021c43c	0
	443	sliver		France		localhost	2023-08-24 14:16	2023-08-24 14:16	3fd21c20d00000021c43d	0
	443	sliver		France		localhost	2023-08-24 14:16	2023-08-24 14:16	2ad06c00000000006c43c	0

DÉTECTION DE CAMPAGNES DE CYBER-ATTAQUES DE 2 À 4 SEMAINES AVANT QU'ELLES SOIENT ACTIVES.

RATspotting

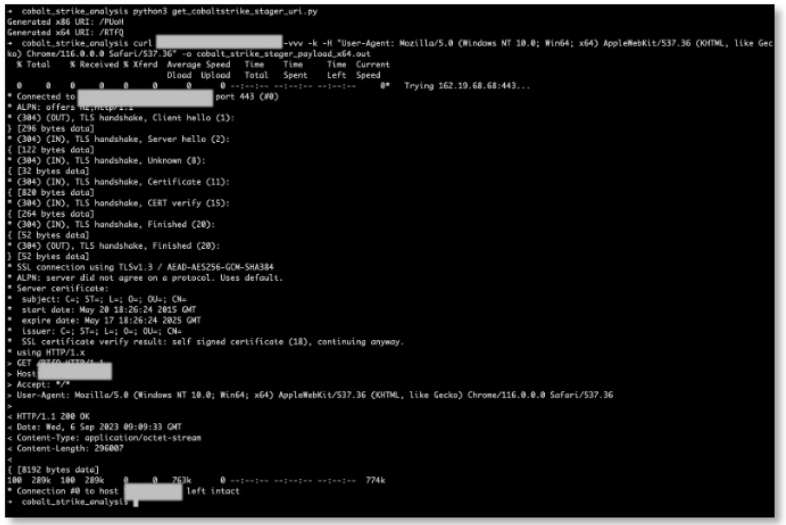
RATspotting – Solution d'anticipation

Example

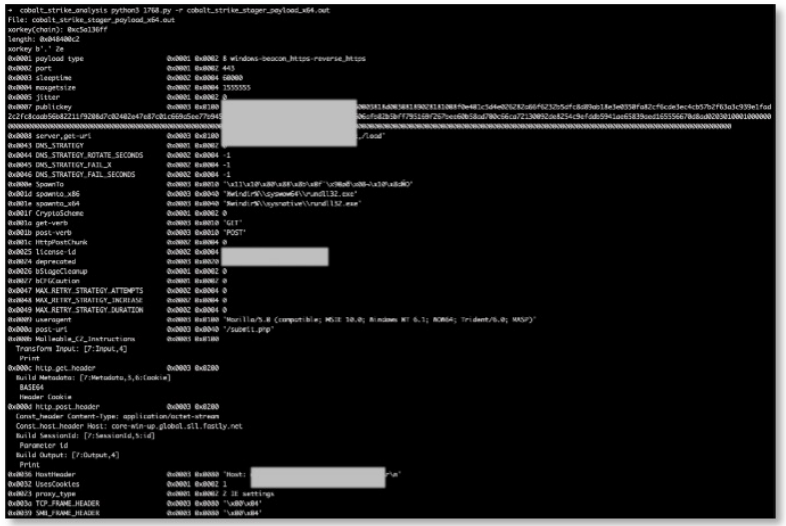
1 RATspotting détection C2

[redacted]	443	cobalt_strike	France		None	2023-08-15 12:50	2023-08-15 12:50	2ad2ad16d2ad2ad000[redacted]	0

2 Téléchargement du Cobalt Strike Beacon



3 Extraction de la configuration



4 Extraction IoCs

IP	[redacted]
URL	[redacted]
C2 GET URI	/load
C2 POST URI	/submit.php
SHA256 Beacon Sample (x86)	c9bf53b37[redacted]
SHA256 Beacon Sample (x64)	82c928cf5[redacted]

Conclusions – IA et Cybersécurité quelles bénéfices?

DREAMLAB TECHNOLOGIES

PREDICTIVE AI

GENERATIVE AI

DÉFENSE

Détection et prévention
- Menaces avancées (réseaux, host, serveur, IoT, Edge, Cloud)
- Malware / logiciels malveillants (réseaux, mémoire, fichiers)
- Campagne de phishing (Email, SMS, Instant Messaging)

Analyse
- Comportementale (en complément ZeroTrust)
- Authentification des utilisateurs (Step-In Auth)
- Analyses de sécurité
- Scénarios prédictifs
- Revue de code / identification bugs

Avancées
- Gestion automatisée des correctifs
- Réduction des menaces internes
- Sécurité adaptative

Nouvelles applications
- Formation à la cybersécurité (sensibilisations, scénarios réalistes)
- Stratégies de défenses
- Aide à la gestion de crise (crises réelles / exercices)
- Pentest (détection automatique points faible, option d'intrusion)

INVESTIGATIONS / FORENSICS

Ingestion
- Triage / Indexation / Tagging des données
- Reconnaissance de mots-clés

Détection
- Récupération de fichiers corrompus et d'artefacts
- Identification fichiers malveillants / conteneur cryptés

Analyse
- Analyse d'images et de vidéos (tagging objets, reconnaissance faciale)
- Analyse de la parole et du texte (speech-to-text, traduction / translitération linguistique)
- Identification lieux géographiques (image extraction, metadata fichiers, coordonnées GPS)
- Analyse réseaux sociaux / connections entre comptes
- Détection faux comptes / comptes dormants

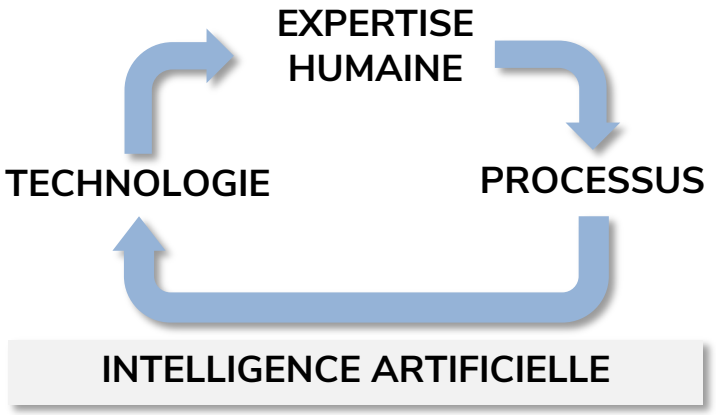
Support Enquête
- Reconstruction de chronologie
- Hiérarchisation des preuves
- Gestion de la chaîne de traçabilité

Nouvelles applications
- Indexation recherche
- Aide à la rédaction de rapport
- Suggestion axes d'enquêtes

Efficacité
- Temps de réponse plus rapides / Volume de traitement
- Automatisation de processus
- Réduction des faux positifs

L'INTELLIGENCE ARTIFICIELLE N'EST PAS UNE SOLUTION MIRACLE QUI PEUT TOUT FAIRE

La cybersécurité est un processus continu qui nécessite une combinaison:



IA en est un support transversal

- Complète les mesures de cybersécurité existantes
- Doit être intégré dans une stratégie globale de cybersécurité.
- Systèmes d'IA eux-mêmes doivent être sécurisés pour éviter qu'ils ne deviennent des cibles potentielles pour des acteurs malveillants.

IA

Contact
DREAMLAB OFFICES

Get in touch with us: contact@dreamlab.net
And follow us at: Twitter: DreamlabGlobal
Linkedin: Dreamlab Technologies AG

Dreamlab Switzerland

Dreamlab Technologies
Monbijoustrasse 36
Switzerland – 3011 Bern

Dreamlab Chile

Dreamlab Technologies
Villavicencio 361, Oficina 113
Chile – 8320154 Santiago de Chile

Dreamlab Malaysia

Dreamlab Technologies
Level 29-01, Tower A,
Vertical Business Suite
Bangsar South, Jalan Kerinchi
Malaysia – 59200 Kuala Lumpur

Dreamlab Oman

Dreamlab Technologies LLC
Minarit Al Qurum Building
2nd floor, Office No. 233
Postal Code 133
Al Khuwair, Sultanate of Oman