Comment détecter les menaces et comment réagir ?

Qui suis-je ?

Jérémy Voisin

Chief Information Security Officer – DFi Service

Directeur de la division Cyberdéfense – CHEOPS Technology

Avec plus de 10 ans d'expérience dans la sécurité de l'information, j'ai eu la chance de travailler et de rendre service à de nombreux clients dans plusieurs domaines d'activité (industrie, banque privée, canton suisse, ONG, ...). La pluralité des domaines d'affaires dans lesquels j'ai pu travailler me permet d'avoir une vision globale sur les activités cyber et s'assurera que les services délivrés sont alignés avec les meilleures solutions et les solutions leaders de l'industrie.

Nos Services

Identification

Audit de sécurité

Ingénierie sociale

Audit de maturité

Analyse de risque

Protection

Firewall UTP/IPS

Antivirus Next Gen (EDR)

Web Application Firewall

Sensibilisation Phishing

Gestionnaire de mot de passe

Détection

Threat Monitoring

Scan de vulnérabilité

Security Operations Center

Cyber Threat Intelligence

Réponse

Analyse et réponse aux Phishing

Réponse aux incidents

Analyse Forensique

Quelques chiffres

- 50 000+ actifs sous surveillance
- 300+ To de données ingérée et analysées par an
- 50+ incidents majeurs traités par an
- 10+ investigations forensique par an

Notre CERT™

- Création en 2016
- Certifié ISO27001
- Audité conforme ISO27035
- Membre du réseau FIRST
- Listé sur TF-CSIRT

Agenda

Faire face à des cybermenaces croissantes. Comprendre le contexte cyber mondial

Eléments de base d’une stratégie de détection des menaces

Faire face aux menaces avancées

Conclusion et questions/réponses

Comprendre le contexte cyber mondial

Le context global

97
Victimes

Il y a eu en moyenne 97 victimes de cybercriminalité par heure en 2022
(Plusieurs sources)

91
Pourcent

91 % des cyberattaques commencent par du phishing, couramment utilisé pour infecter les organisations avec des ransomwares
(Security Venture)

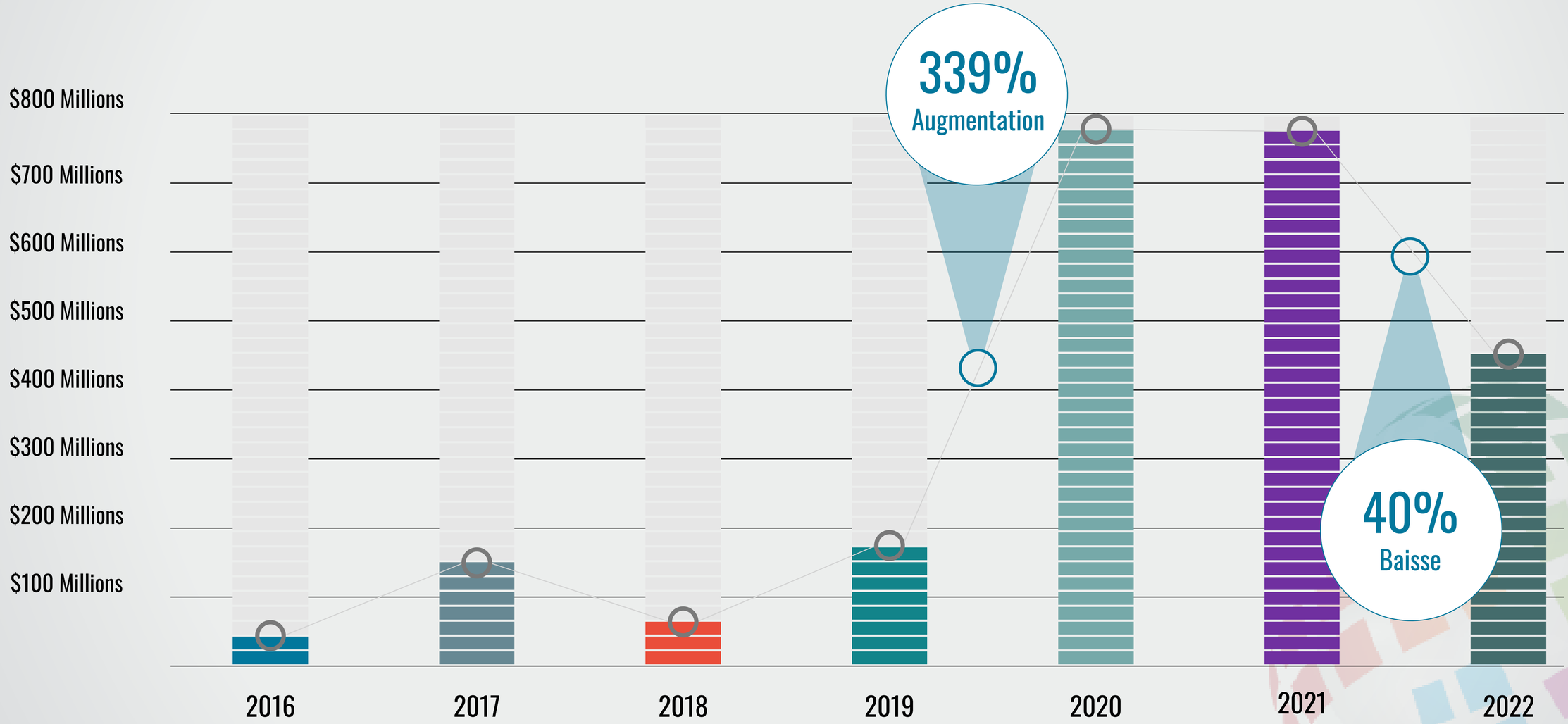
43
Pourcent

43 % des cyberattaques ciblent les petites et moyennes entreprises
(Cybint)

204
Jours

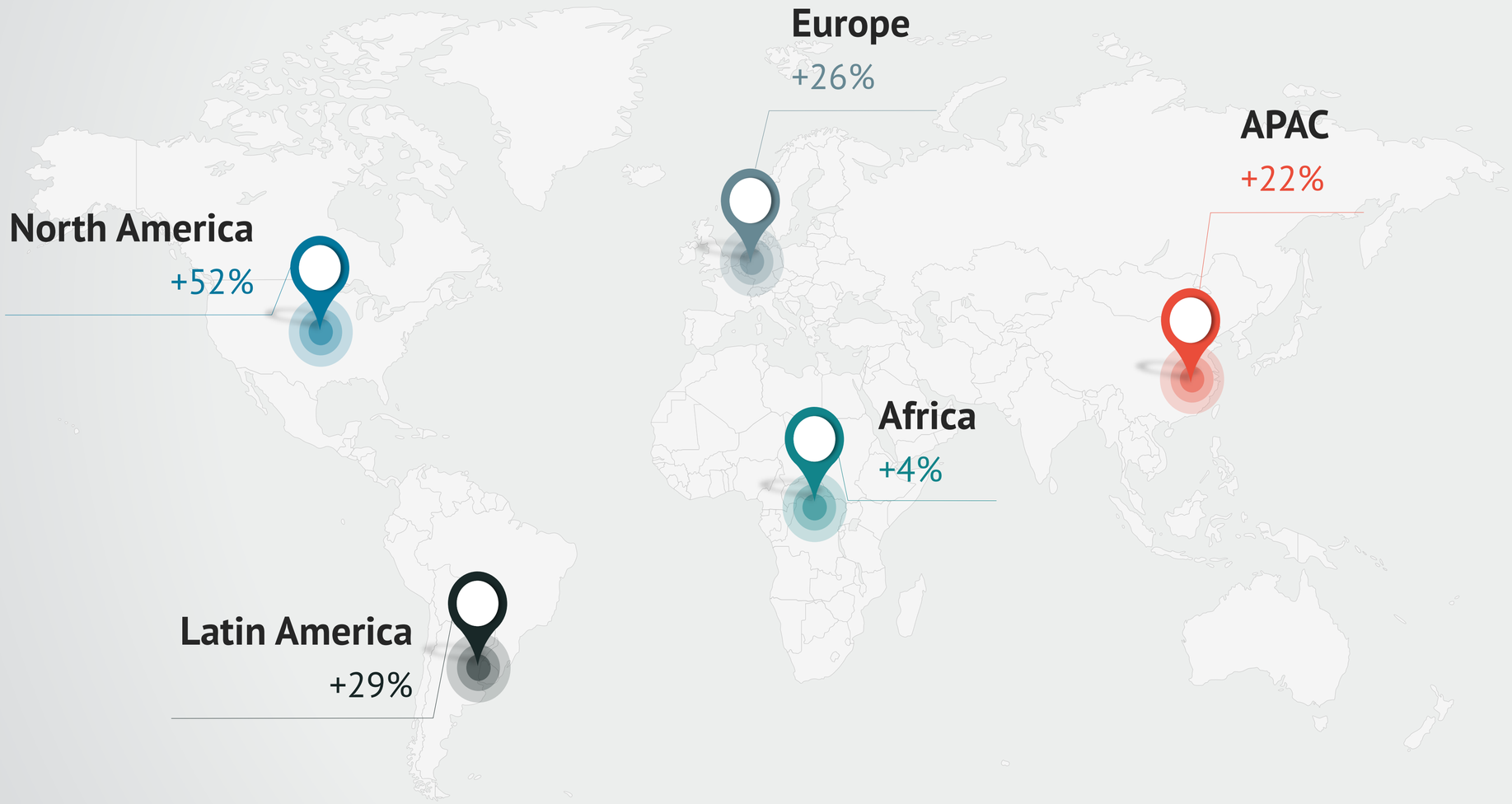
Le délai moyen pour identifier une intrusion en 2023 était de 204 jours
(IBM)

Evolution des revenues des ransomware



Source: Chainalysis

Attaques par semaine (2021 vs 2022)



Top 3 des augmentations par secteur

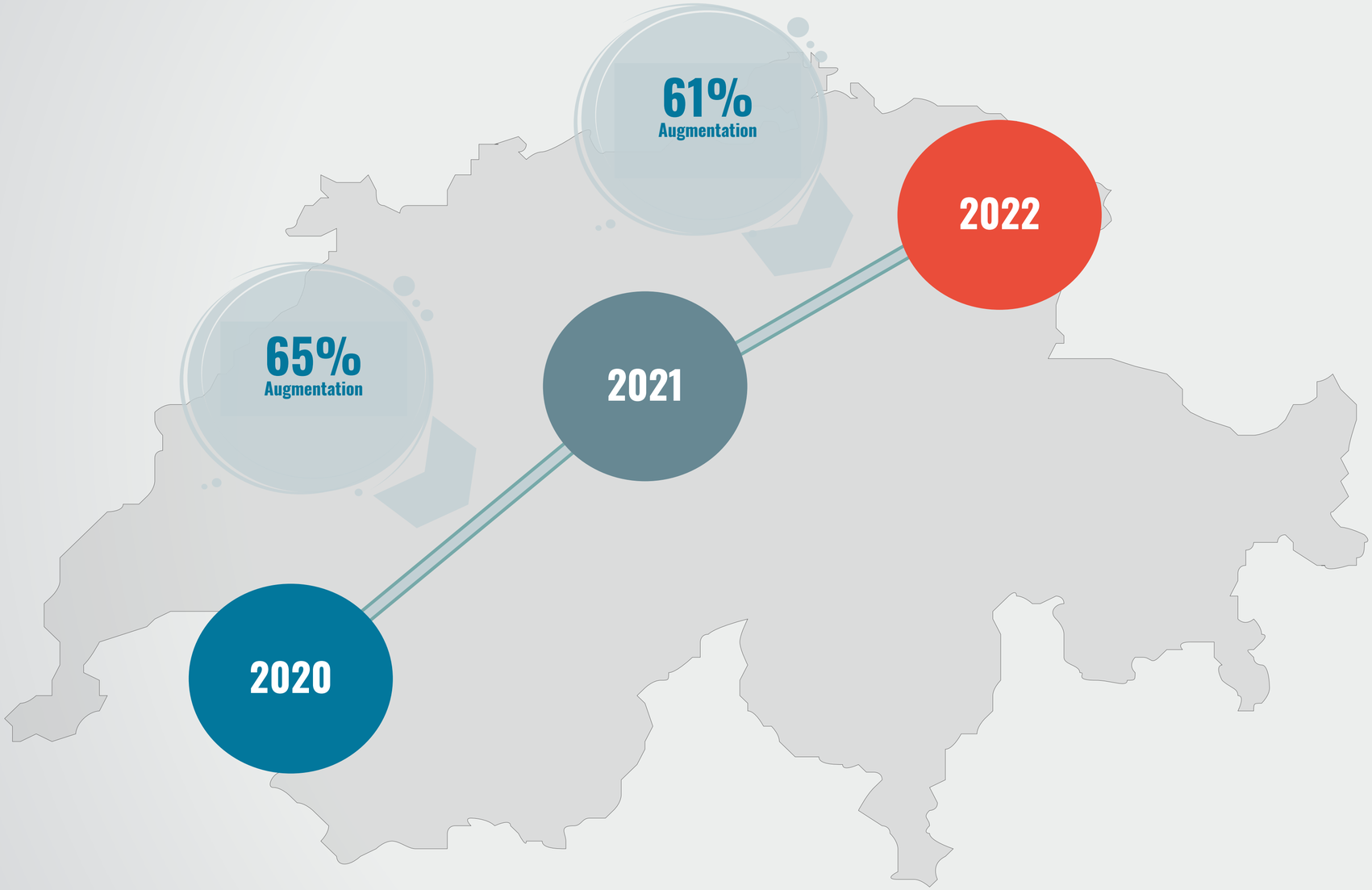
+52%
Finance

+75%
Commerce de gros

+74%
Santé

Source: Checkpoint

Et en Suisse ?



60% de plus que la moyenne mondiale

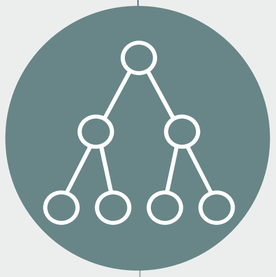
Source: Checkpoint

Eléments de base d’une stratégie de détection des menaces

La mise en place d’une stratégie

Technology

SIEM, EDR, XDR, NDR, ...



Process

Policies, Guidelines, Playbooks, etc...

People

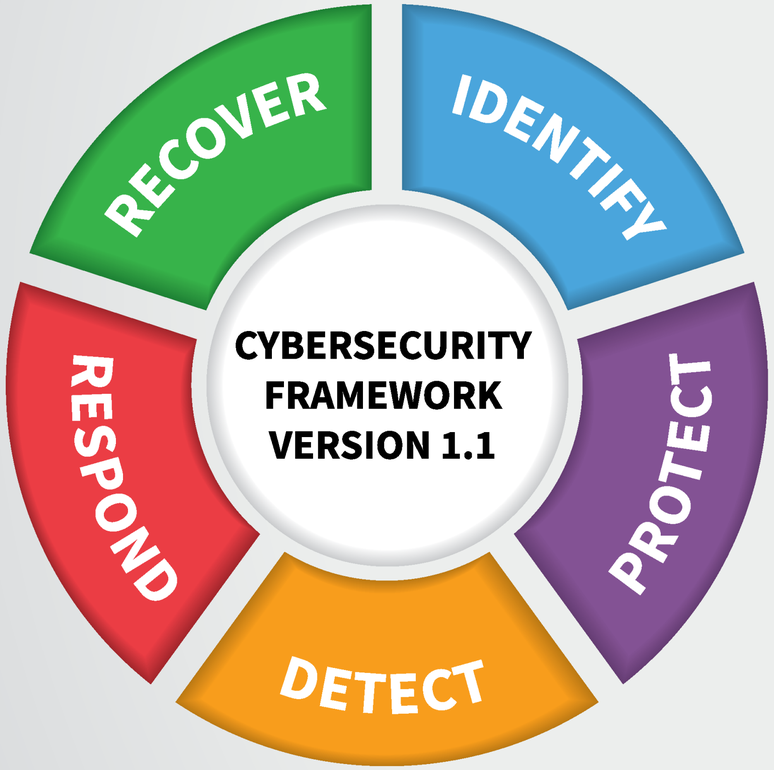
Analystes, Ingénieurs, etc...

La mise en place d’une stratégie

Une stratégie basée uniquement sur la technologie est vouée à l’échec (By-Design)

Une approche structurée via NIST CSF

Une approche structurée via NIST CSF



Identification (ID)

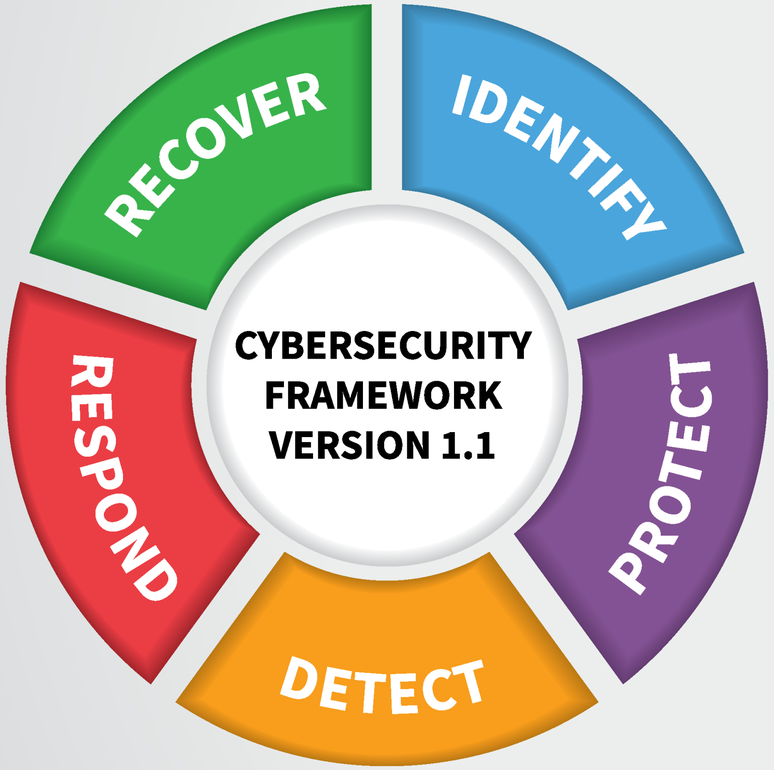
Objectifs

Identifier et gérer les actifs, les données, les capacités et les personnes nécessaires à la conduite des affaires.

Activités

- Classer les actifs informatiques en fonction de leur importance.
- Identifier les données sensibles et les points de stockage.
- Évaluer les vulnérabilités potentielles.

Une approche structurée via NIST CSF



Protection (PR)

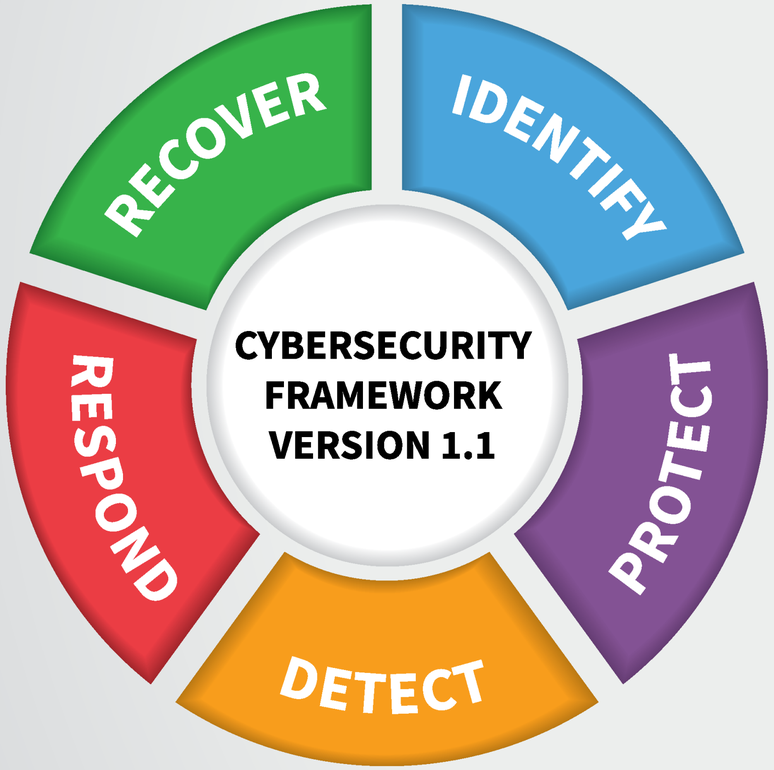
Objectifs

Développer et mettre en œuvre des mesures de protection appropriées pour assurer la livraison des services essentiels.

Activités

- Élaborer des politiques de sécurité claires et compréhensibles.
- Surveiller le réseau pour prévenir les attaques.
- Utiliser des technologies de détection d'anomalies.

Une approche structurée via NIST CSF



Détection (DE)

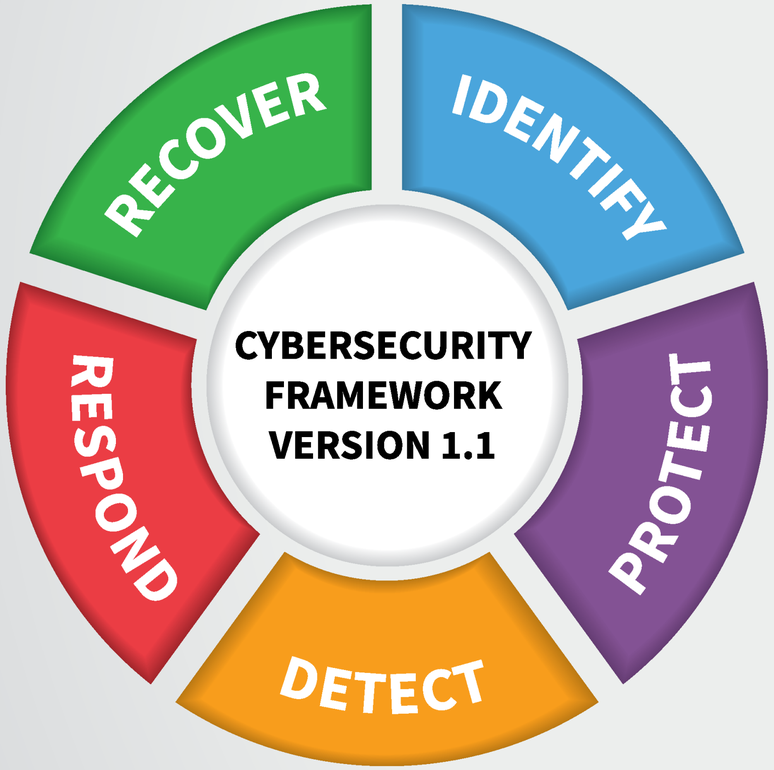
Objectifs

Identifier rapidement les incidents de sécurité.

Activités

- Mettre en place une surveillance réseau continue.
- Utiliser des outils de détection d'anomalies pour repérer des schémas inhabituels.
- Configurer des systèmes de détection d'intrusions pour signaler et bloquer automatiquement les menaces.

Une approche structurée via NIST CSF



Réponse (RS)

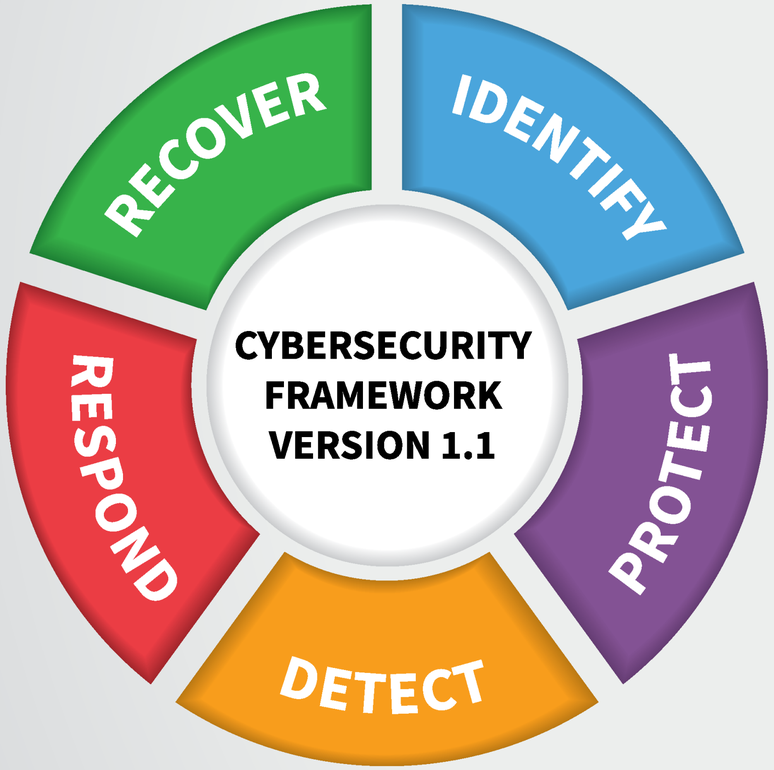
Objectifs

Répondre efficacement aux incidents de sécurité détectés.

Activités

- Élaborer un plan de gestion des incidents détaillé.
- Former et préparer une équipe d'intervention.
- Effectuer des exercices de simulation pour tester la réactivité de l'équipe.

Une approche structurée via NIST CSF



Recovery (RC)

Objectifs

Récupérer rapidement les services et les données après un incident.

Activités

- Assurer que l'équipe a les compétences nécessaires pour récupérer après un incident.
- Mettre en place des procédures de récupération, y compris des sauvegardes régulières.

Les fondamentaux – 5 must have

Architecture sécurisée

Multifacteur sur les accès externe

Firewall NG

EDR

Sensibilisation des utilisateurs

Pourquoi une conception d'architecture sécurisée ?

Qu'est-ce qu'une conception d'architecture sécurisée

Segmentation des serveurs – Isoler les serveurs dans plusieurs réseaux par rôle, classification, risque, etc...

Segmentation des utilisateurs – Isoler les utilisateurs dans plusieurs réseaux par rôle, risque, etc...

Implicit deny – Autoriser uniquement le strict minimum dans le pare-feu

Stratégie de sauvegarde solide – 3-2-1-1-0, et avec chiffrement

Pourquoi une conception d'architecture sécurisée ?

01

Rendre la compromission difficile

Appliquer des concepts et utiliser des techniques qui empêchent les attaquants de compromettre les systèmes.

02

Rendre la perturbation difficile

Contenir les perturbations dans une zone précise et éviter toute perturbation latérale

03

Rendre la détection plus facile

La connaissance et la bonne maîtrise de votre Système d'Information permettent d'identifier plus rapidement les activités suspectes

04

Réduire les impacts des compromis

Une architecture robuste permet de réduire l'impact et les temps d'arrêt

Pourquoi du MFA ?

Les mots de passe peuvent être compromis

Réutilisation – Le même mot de passe est souvent utilisé sur plusieurs sites Web

123456 – Reste le mot de passe le plus utilisé en 2023

721 millions – Mot de passe fuité en 2022

Stockage non sécurisé – Password.txt, Navigateur web, ...

24+ Milliard – Identifiants circulant sur le Dark Web en 2022 *(Source Darkreading)*

49 % des violations survenues en 2023 impliquaient l'utilisation d'identifiants volés *(Verizon)*

Pourquoi un pare-feu de nouvelle génération

Les NGFWs sont essentiels

Connaissance des applications – Identifier et contrôler les applications pour une gestion précise du trafic

Intrusion Prevention System (IPS) – Détecter et prévenir les activités malveillantes et les modèles d'attaque connus

Advanced Threat Protection – Atténuer les menaces avancées telles que les exploits Zero Day et les APT.

Intégration de Threat Intelligence – Utiliser les données sur les menaces en temps réel pour bloquer de manière proactive les connexions malveillantes

Les firewalls traditionnels ne suffisent plus à protéger contre les cybermenaces modernes et sophistiquées

Pourquoi un EDR ?

Les EDR sont indispensables

Détection des menaces en temps réel – Identifier et répondre aux menaces de sécurité en temps réel.

Analyse comportementale – Surveiller le comportement à la recherche de signes d'activité malveillante, même sans signatures connues.

Threat Hunting – Rechercher de manière proactive les signes de menaces et de vulnérabilités avancées au sein des actifs.

Réponse automatisée – Automatiser les actions de réponse pour atténuer rapidement les menaces et réduire les interventions manuelles.

Et plus – . . .

Même si l'EDR peut également être contourné, les antivirus traditionnels ne sont pas efficaces contre les menaces actuelles.

Pourquoi un EDR ?

Toutes les alertes EDR doivent être traitées

(même les Low et Info)

Pourquoi la sensibilisation des utilisateurs ?

95 % des failles de cybersécurité sont dues à une erreur humaine
(Cybint)

91 % des cyberattaques commencent par du phishing, couramment utilisé pour infecter les organisations avec des ransomwares
(Security Ventures)

Pourquoi la sensibilisation des utilisateurs ?

Les utilisateurs sont la première et la dernière ligne de défense

Phishing, Vishing, Smishing, Whaling – Augmentation du ciblage des utilisateurs avec des attaques sophistiquées d'ingénierie sociale

Point central de la stratégie – Impliquer les utilisateurs dans la stratégie Cyber (culture du reporting, etc.)

Faire face aux menaces avancées

La technologie seule ne suffit plus

La technologie que nous utilisons est sûre, jusqu'à ce qu'elle ne le soit plus

Microsoft – Patché 1292 vulnérabilités en 2022, dont 89 critiques (Zero Day, ...)

Cisco – Publication d'un correctif pour une vulnérabilité activement exploitée (score CVSS de 10/10)

Citrix – Publication d'un correctif pour une vulnérabilité activement exploitée affectant NetScaler ADC

Fortinet – Une vulnérabilité critique dans FortiGate SSL VPN pourrait permettre aux pirates d'accéder à des systèmes vulnérables

Chrome – Plusieurs problèmes de sécurité dans Google Chrome ont été exploités par des acteurs malveillants

And more...

La technologie seule ne suffit plus

Besoin d’aller au-delà des EDR

Implémentation et whiteliste – Trop permissif, défaut de configuration, whitelist %TEMP%, etc…

Contournement – Malheureusement, tous les EDR se contournent. Il s’agit d’une question de temps

Bonne pratique IT – Si l’utilisateur est local admin, « Game Over »

Limite des EDR – Les EDR ne peuvent pas bloquer dès qu’ils ont un doute

Et plus…

Trop de menaces pour se concentrer sur toutes

13 versions majeures de MITRE ATT&CK depuis 2018

Updates - April 2023

Techniques

Enterprise

New Techniques

- Acquire Access (v1.0)
- Acquire Infrastructure: Malvertising (v1.0)
- Cloud Administration Command (v1.0)
- Command and Scripting Interpreter: Cloud API (v1.0)
- Device Driver Discovery (v1.0)
- Exfiltration Over Web Service: Exfiltration to Text Storage Sites (v1.0)
- Impair Defenses: Spoof Security Alerting (v1.0)
- Masquerading: Masquerade File Type (v1.0)
- Modify Authentication Process: Network Provider DLL (v1.0)
- Obfuscated Files or Information: Command Obfuscation (v1.0)
- Obfuscated Files or Information: Fileless Storage (v1.0)
- Remote Services: Cloud Services (v1.0)
- Unsecured Credentials: Chat Messages (v1.0)

Faire face à ses propres menaces

Renseignement sur les menaces

01

Intelligence avec des données exploitables

Threat Actor actif, IOCs, Tools, TTPs, Contextualisation des menaces, ...

Émulation

02

Exécuter le scénario d'attaque pour un acteur menaçant

Comment un véritable TA tenterait de pénétrer dans les systèmes et les réseaux de l'organisation

Évaluation

03

Évaluer l'efficacité des contrôles

Évaluez les capacités de détection et les procédures de réponse aux incidents pour détecter et atténuer les attaques simulées.

Amélioration

04

Utiliser les résultats pour améliorer le SOC

Utilisez les résultats de l'émulation pour améliorer les contrôles de sécurité, mettre à jour les politiques et procédures, créer de nouveaux cas d'utilisation et améliorer la posture globale de cybersécurité.

Faire face à ses propres menaces

ADVERSARY EMULATION

RENSEIGNEMENT SUR LES MENACES

01

Intelligence avec des données exploitables

Threat Actor actif, IOCs, Tools, TTPs, Contextualisation des menaces, ...

ÉMULATION

02

Exécuter le scénario d'attaque pour un acteur menaçant

Comment un véritable TA tenterait de pénétrer dans les systèmes et les réseaux de l'organisation

ÉVALUATION

03

Évaluer l'efficacité des contrôles

Évaluez les capacités de détection et les procédures de réponse aux incidents pour détecter et atténuer les attaques simulées.

AMÉLIORATION

04

Utiliser les résultats pour améliorer le SOC

Utilisez les résultats de l'émulation pour améliorer les contrôles de sécurité, mettre à jour les politiques et procédures, créer de nouveaux cas d'utilisation et améliorer la posture globale de cybersécurité.

Adversary Emulation

Approche proactive pour tester et améliorer la posture de sécurité d'une organisation. Il s'agit de simuler les Tactiques, Techniques et Procédures (TTP) de cyber-adversaires réels pour évaluer l'efficacité des défenses d'une organisation.

L’objectif est d’identifier les faiblesses et les domaines dans lesquels des améliorations de sécurité sont nécessaires

Conclusions

Détection et réponse aux menaces

Prévenir et détecter

Détecter les activités malveillantes et les prévenir avant qu'elles ne causent des dommages.

Détection et réponse aux menaces

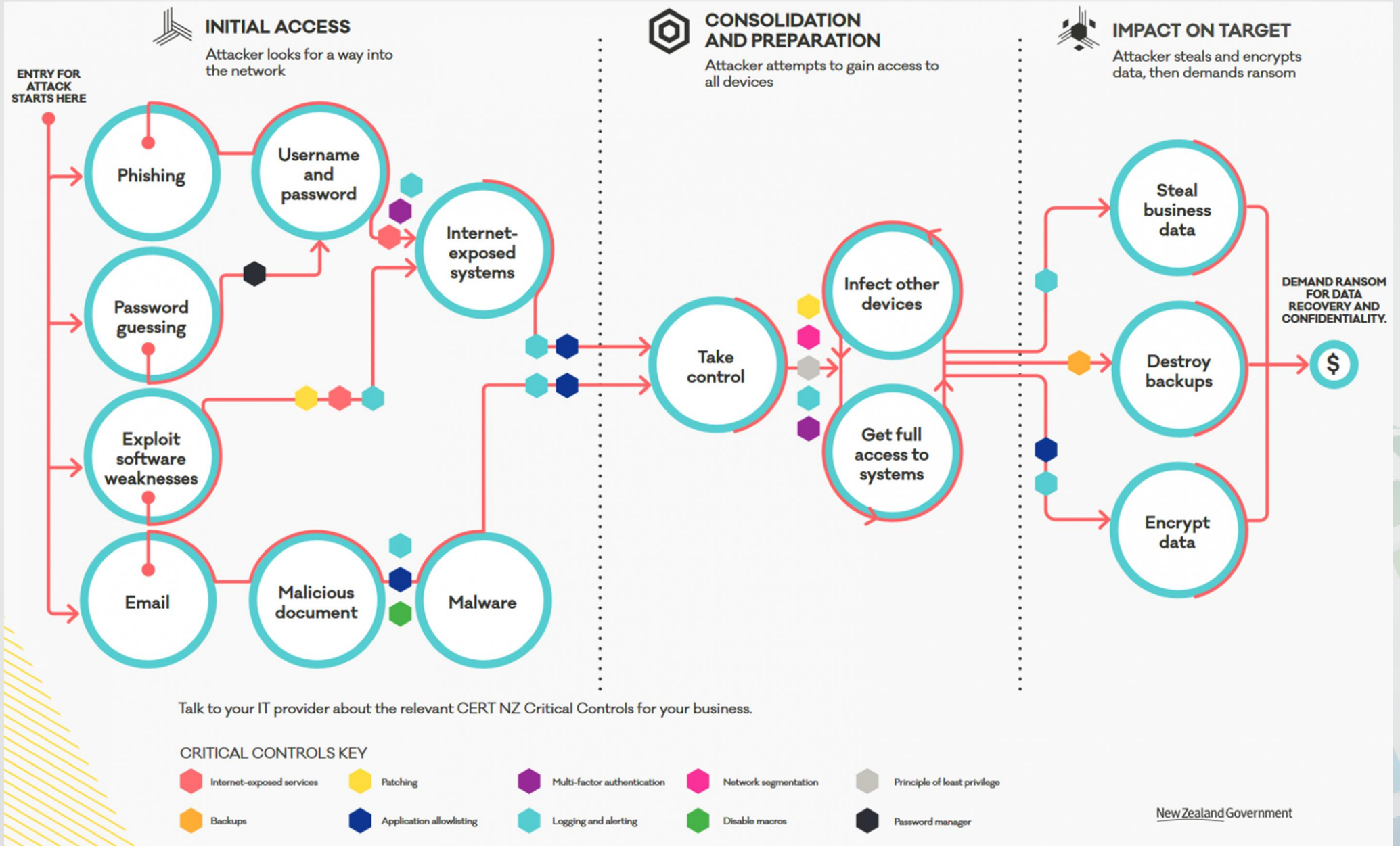
Analyse l'activité suspecte pour déterminer la nature de la menace et sa couverture.

L'analyste se place du point de vue d'un attaquant.

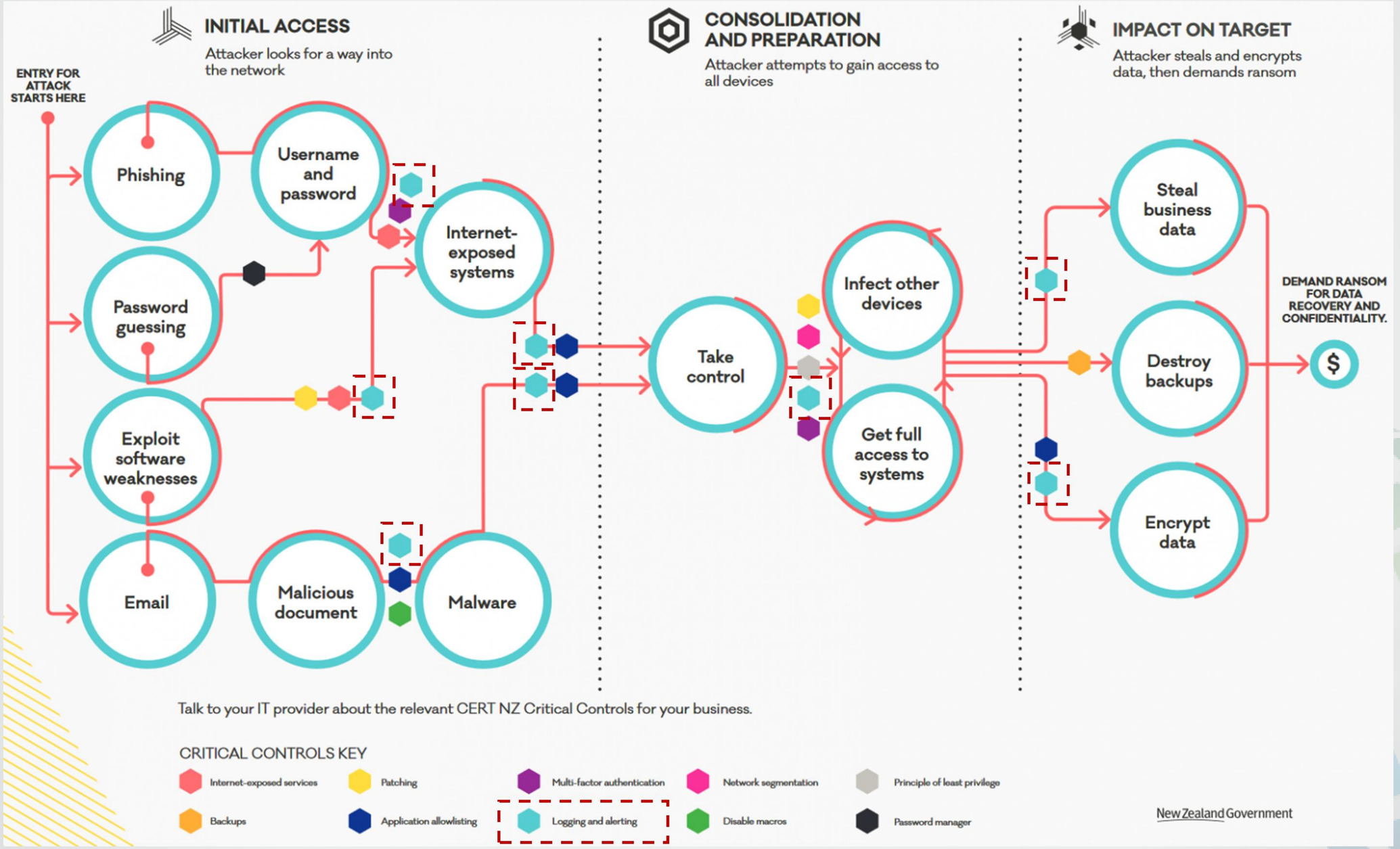
Détection et réponse aux menaces

Coordination des actions de réponse aux Incidents afin d'isoler rapidement la menace et diminuer les impacts.

Surveiller et Alerter



Surveiller et Alerter



Merci à tous

Jeremy Voisin
Chief Information Security Officer
Director of CHEOPS Cyberdefense

https://www.linkedin.com/in/jeremyvoisin

Jeremy Voisin
Chief Information Security Officer
Director of CHEOPS Cyberdefense

https://www.linkedin.com/in/jeremyvoisin

Q&A