Cyber Formation Québec (CFQ)

Organiser sa cyberdéfense opérationnelle (PME)

Jean-François Brouillette
Fondateur et formateur

jfb@cyberformationquebec.ca

NOTE IMPORTANTE

Cyber Formation Québec

- Le contenu de cette présentation a été créé pour une formation en personne qui a été donnée au Hackfest en 2024.
- Le contenu n’est là que pour appuyer visuellement la formation et sans contexte certains aspects discutés peuvent manquer de clarté.
- Ce contenu est fourni gratuitement par Cyber Formation Québec afin de donner des idées et partager de l’information.
- Cyber Formation Québec n’est pas responsable des actions entreprises à la suite de la lecture de cette présentation et il ne faut pas voir celle-ci comme une suggestion d’actions à prendre.
- Il s’agit d’une version « en cours de développement ». Du contenu et des correctifs continueront d’être ajoutés dans le futur. Merci de votre compréhension.

MISSION & RAISON D'ÊTRE

- FAVORISER LE PARTAGE DES CONNAISSANCES
- OFFRIR DU CONTENU FRANCOPHONE DE QUALITÉ
- DISTRIBUTION DE FORMATIONS « PRATIQUE »
- ACCOMPAGNER LES PROFESSIONNELS TI
- SENSIBILISER LES ORGANISATIONS ENVERS LES ENJEUX DE CYBERSÉCURITÉ

Ce que je pensais avant…

Cyber Formation Québec

SUGGESTION DE LECTURE

Cyber Formation Québec

Quelques éléments clés

- Qu'est-ce que vous protégez et pourquoi?
- Engagez et formez des ressources de qualité
- L'importance de la réponse aux cyber incidents
- Sélectionner et ingérer les bonnes données
- Mesurez et améliorer les performances

Lien de téléchargement du livre numérique

https://bit.ly/cfq-ressource1

Solution technologique & Vocabulaire

Terminologie

Afin de bien comprendre les aspects qui seront discutés lors de cette formation, il est important de décrire certains termes utilisés.

En tout temps lors de la formation vous pouvez interagir et poser des questions afin d’être en mesure de bien comprendre ce qui est discuté.

TERMINOLOGIE

Cyber Formation Québec

Triade de la « protection »

Un concept bien connu dans le milieu est que l'essentiel afin d'assurer une protection de base de l'environnement et d'assurer une surveillance raisonnable est l'utilisation des outils suivants: EDR, NDR et SIEM.

- **EDR:** Endpoint Detection and Response
  Référence
- **NDR:** Network Detection and Response
  Référence
- **SIEM:** Security information and event management
  Référence
- **XDR:** Extended detection and response (marketing ou non? parlons-en.... ☺)
  Référence

TERMINOLOGIE

Cyber Formation Québec

SOAR
Security Orchestration, Automation and Response

Blue Team, Red Team & Purple Team

IOC
Indicator of compromission

DFIR
Digital Forensics & Incident Response

Cadre de référence / Framework !!! (Pourquoi est-ce que c'est important?)

Data Loss Prevention

IAM
Identity & Access Management

OSINT
Open-source intelligence

Rôles et Capacités d'affaire

Terminologie

Afin de bien comprendre les aspects qui seront discutés lors de cette formation, il est important de décrire certains termes utilisés.

En tout temps lors de la formation vous pouvez interagir et poser des questions afin d'être en mesure de bien comprendre ce qui est discuté.

Rappel

Une seule personne dans votre organisation peut correspondre à plusieurs équipes / rôles

TERMINOLOGIE

Cyber Formation Québec

Surveillance

L’équipe responsable d’activer, de mettre en place et d’analyser les détections reçus de vos différentes solutions de cybersécurité. (Ex: EDR, NDR, etc.)

Il s’agit de votre première ligne de défense, de où l’importance de miser sur son développement et de les former à bien comprendre les différents environnements.

Réponse aux cyber incidents (IR)

Lorsqu’un membre de l’équipe de surveillance soupçonne une activité suspecte, il escalade à un membre de l’équipe de réponse aux cyber incidents.

Cette équipe est responsable de confirmer s’il s’agit d’une menace, de déterminer la sévérité de l’incident et d’ensuite y répondre afin de mitiguer celle-ci.

TERMINOLOGIE

Cyber Formation Québec

Renseignements en cybermenace (CTI)

Ce rôle permet à l'organisation de garder un oeil sur les menaces pouvant toucher son secteur et à effectuer une vigie concernant les potentielles informations appartenant à l'entreprise disponibles sur Internet.

Travaille en étroite collaboration avec l'équipe de surveillance et de chasse à la menace afin d'améliorer les règles de détections en place et faire des recherches proactives dans l'environnement.

Chasse à la menace (Threat Hunting)

En se basant sur des hypothèses de menace, cette équipe utilisent tout les outils et solutions à leur disposition afin de déterminer si une menace est présente ou non dans l'environnement.

Cette équipe cherche en se basant sur des tactiques et techniques connues des attaquants. (**TTPs**)

TERMINOLOGIE

Cyber Formation Québec

Tests offensifs (Red Team)

Ressources spécialisées dans les opérations offensives

Les membres de la Red Team sont souvent des hackers éthiques qualifiés qui cherchent à identifier et exploiter les vulnérabilités de manière sécurisée. En jouant le rôle de l'adversaire, ils aident l'entreprise à renforcer sa sécurité en découvrant les failles avant que de véritables attaquants ne puissent les exploiter. (*)

Digital Forensics (Désolé pour l'anglais...)

Ressources spécialisées dans l'investigation et la collecte de preuves numériques

Les membres de cette équipe travaillent souvent en collaboration avec d'autres départements comme les ressources humaines, le service juridique, et les équipes de conformité.

TERMINOLOGIE

Cyber Formation Québec

Légal, Risque, PRP…

Gestion des vulnérabilités (VM)

Comme pour le rôle de surveillance, celui de gestion des vulnérabilité comporte un éventail très étendu de responsabilités.

Cette équipe devra s'assurer que l'ensemble des actifs de l'organisation, peu importe l'environnement, soit analysé et balayer afin de déterminer si des vulnérabilités existes afin d'y appliquer un plan de correction. On peut parler de vulnérabilité au niveau de la configuration comme au niveau applicatif.

Exercices et formation des ressources

Il est primordial de garder vos ressources prêtes en cas de cyber incident. En règle générale, il est peu probable que vous viviez plusieurs incidents notables dans un court laps de temps et vos équipes doivent garder en tête votre plan de réponse afin d'éviter de perdre du temps précieux.

Cette équipe va coordonner des activités de simulation d'incident et faire le suivi des parcours de formation établis par la gestion. (Ex: **TTX**, **Live-fire**, etc.)

L’IMPORTANCE DE L’HUMAIN

Il n’y a pas juste le technique...

Même si l'automatisation et l'IA jouent un rôle croissant dans la cybersécurité, l'expertise humaine reste indispensable pour une réponse efficace et adaptée aux menaces.

Un seul profil peut difficilement couvrir adéquatement la multitude de rôles mentionnés plus tôt.

PROFILS

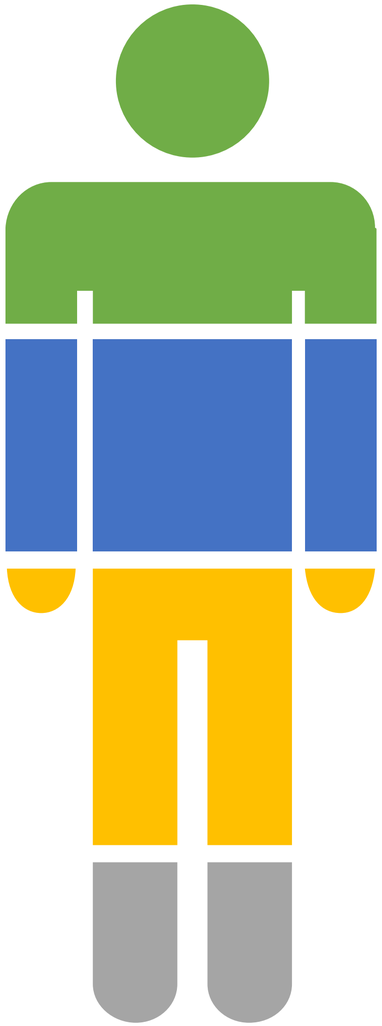
Cyber Formation Québec

Prédateur*

- Réponse aux cyberincidents
- Vise le gain rapide
- Vise la jugulaire

Vulgarisateur

- Incident majeur
- Coordination
- Gest. Vuln.
- Sensibiliation et formation (TTX)



Expert tech.

- Gest. Vuln.
- Support TTX
- Surveillance
- Réponse aux cyberincidents

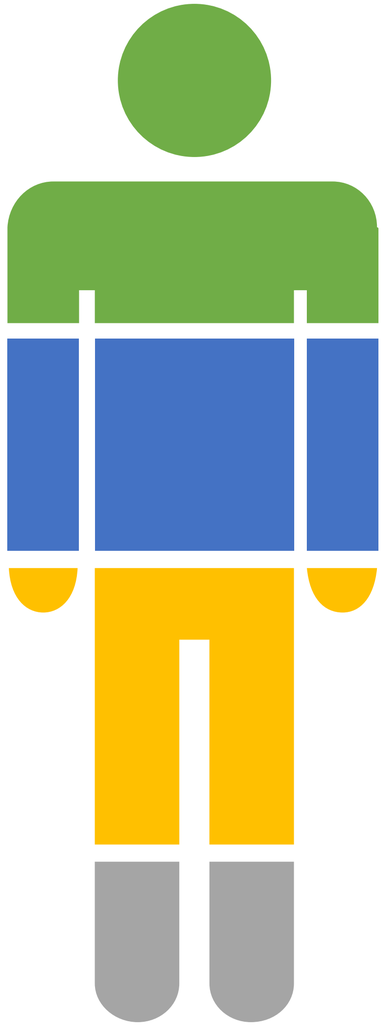
Minutieux

- Chasse à la menace
- Enquêtes numériques
- Support à la réponse aux cyberincidents
- Renseignements (CTI)

EXERCICE
CONSIGNES

À faire

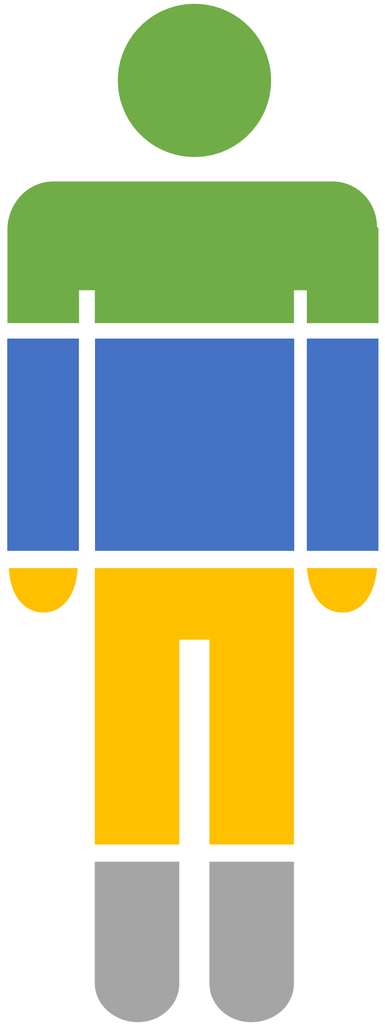
- Pour chaque profil présenté, identifiez le rôle qui lui conviendrait le mieux
- Le potentiel de développement et/ou changement de rôle futur? (résilience opérationnelle?)



EXERCICE
Quel rôle pour Arthur?

Un peu de détails...

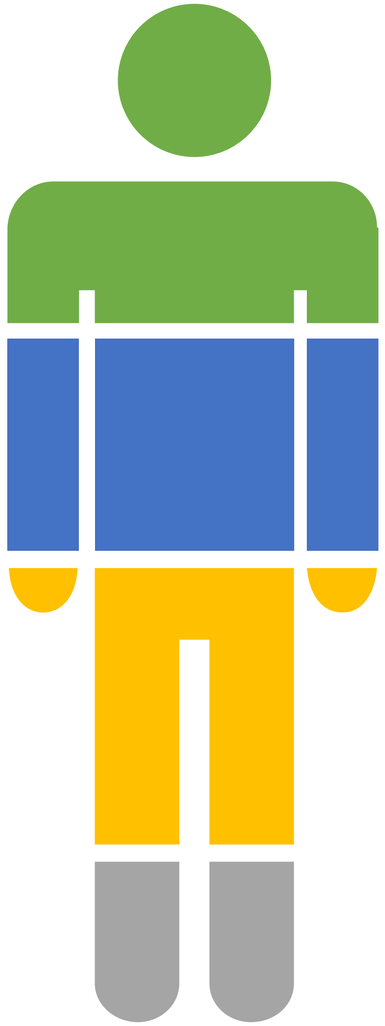
1. Adepte des randonnées en forêt
2. Fait l'élevage de lapin et participe à un groupe local d'élevage
3. S'implique dans sa communauté en effectuant du bénévolat en groupe
4. Possède des connaissances de base en cybersécurité mais s'intéresse à la technologie depuis son enfance
5. Désire un horaire stable et prévisible



EXERCICE
Quel rôle pour Alice?

Un peu de détails...

1. Adepte du café et des « bubble tea »
2. Légère expérience de travail en TI
3. Études universitaires complétées (domaine lié aux technologies)
4. Fan des séries policières et des intrigues
5. Adore la rédaction et la lecture
6. Bon esprit d’analyse



EXERCICE
Quel rôle pour Alfred?

Un peu de détails...

1. Adepte de la pêche sur la glace et de saut en parachute
2. Un passionné et mordu de cybersécurité depuis sa jeunesse
3. Participe à des CTF et plusieurs conférences techniques chaque année (assiste quelques fois les organisateurs)
4. N’aime pas beaucoup la rédaction et se limite au strict minimum
5. Aucunes études supérieures mais consomme beaucoup de formations sur Internet

EXERCICE: CHOIX D'UNE RESSOURCE

Cyber Formation Québec

Scénario

Vous avez présentement une ressource qui s'affaire à vérifier les alertes et détections dans vos différentes solutions de sécurité et prend en charge celles-ci.

Quel type de rôle/ressource auriez-vous besoin d'ajouter à votre équipe pour passer à la prochaine étape?

Discussion

En ordre de priorité, selon-vous quels rôles devraient être remplis en priorité pour augmenter sa maturité?

Liste des rôles

Tests offensifs (Red Team)

Surveillance

Chasse à la menace (Threat Hunting)

Exercices et formation des ressources

Gestion des vulnérabilités (VM)

Réponse aux cyber incidents (IR)

Renseignements en cybermenace (CTI)

PARTAGE D'EXÉRIENCE

Quels sont les aspects clés à garder en tête lorsque nous désirons optimiser les ressources (ou nous-mêmes) au sein de votre grande équipe de cyberdéfense?

- Collaboration, cohésion et « fit » humain
- Développement personnel et professionnel
- Structure claire et vision commune

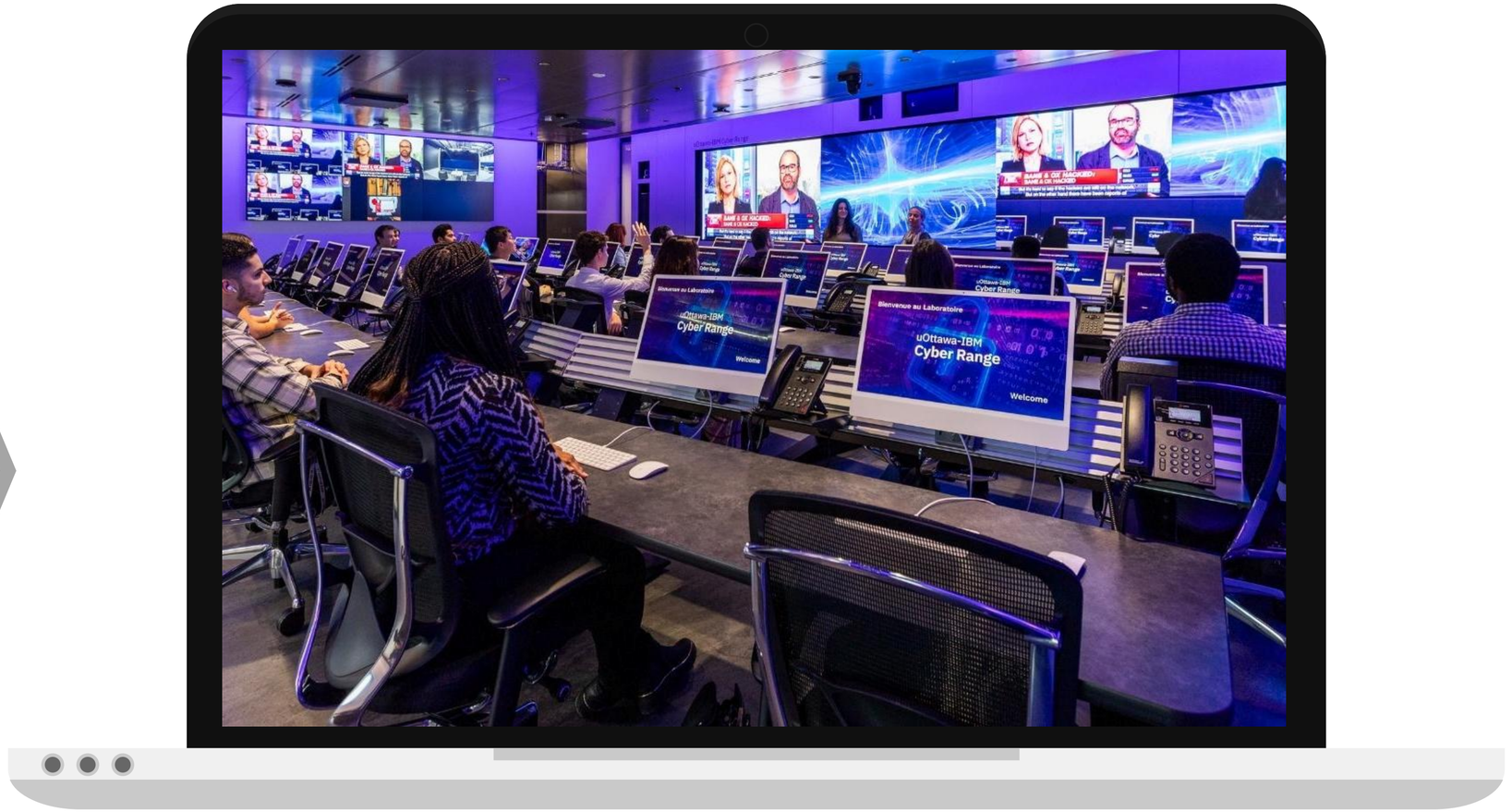
FORMATION

Cyber Formation Québec

Il est primordial de garder l'équipe à jour avec des formations. Vous voulez les meilleurs!

Offrir ou obtenir de la formation qui complémente les acquis existant de l'individu

Recette gagnante: entre 5 et 10% du temps dédié à la formation



FORMATION

Cyber Formation Québec

Le framework NICE (*National Initiative for Cybersecurity Education*) est un modèle développé par le National Institute of Standards and Technology (NIST) aux États-Unis. Il vise à établir un cadre pour les compétences et les connaissances nécessaires dans le domaine de la cybersécurité. (Référence)

WORK ROLE CATEGORIES

- Regroupe les rôles et les tâches spécifiques
- Identifier les compétences nécessaires pour différents postes

WORK ROLE

- Identifie plusieurs domaines clés, tels que la protection des systèmes, la gestion des risques, la réponse aux incidents

TASKS, KNOWLEDGE & SKILLS (TKS)

- Aligner les programmes de formation sur ces compétences
- Identifier les compétences à développer

FORMATION

Cyber Formation Québec

NIST | NICE

Protection and Defense (PD)

Protects against, identifies, and analyzes risks to technology systems or networks. Includes investigation of cybersecurity events or crimes related to technology systems and networks.

Work Roles

Investigation (IN)

Conducts national cybersecurity and cybercrime investigations, including the collection, management, and analysis of digital evidence.

Work Roles

Cyberspace Intelligence (CI)

Collects, processes, analyzes, and disseminates information from all sources of intelligence on foreign actors' cyberspace programs, intentions, capabilities, research and development, and operational activities.

Work Roles

FORMATION

Cyber Formation Québec

Protection and Defense (PD)

Protects against, identifies, and analyzes risks to technology systems or networks. Includes investigation of cybersecurity events or crimes related to technology systems and networks.

Work Roles

INSIDER THREAT ANALYSIS

VULNERABILITY ANALYSIS

DIGITAL FORENSICS

INCIDENT RESPONSE

DEFENSIVE CYBERSECURITY

Investigation (IN)

Conducts national cybersecurity and cybercrime investigations, including the collection, management, and analysis of digital evidence.

Work Roles

CYBERCRIME INVESTIGATION

DIGITAL EVIDENCE ANALYSIS

FORMATION

Cyber Formation Québec

Tasks

T0164: Perform cyber defense trend analysis and reporting
T0262: Employ approved defense-in-depth principles and practices (e.g., defense-in-multiple places, layered defenses, security robustness)
T0510: Coordinate incident response functions
T1020: Determine the operational and safety impacts of cybersecurity lapses
T1084: Identify anomalous network activity
T1085: Identify potential threats to network resources
T1109: Resolve cyber defense incidents
T1110: Coordinate technical support to enterprise-wide cybersecurity defense technicians

FORMATION

Cyber Formation Québec

Knowledges

K0674: Knowledge of computer networking protocols
K0675: Knowledge of risk management processes
K0676: Knowledge of cybersecurity laws and regulations
K0677: Knowledge of cybersecurity policies and procedures
K0678: Knowledge of privacy laws and regulations
K0679: Knowledge of privacy policies and procedures
K0680: Knowledge of cybersecurity principles and practices
K0681: Knowledge of privacy principles and practices
K0682: Knowledge of cybersecurity threats

FORMATION

Cyber Formation Québec

Skills

S0077: Skill in securing network communications
S0080: Skill in performing damage assessments
S0483: Skill in identifying software communications vulnerabilities
S0509: Skill in evaluating security products
S0544: Skill in recognizing vulnerabilities
S0547: Skill in identifying malware
S0548: Skill in capturing malware
S0549: Skill in containing malware

FORMATION

Cyber Formation Québec

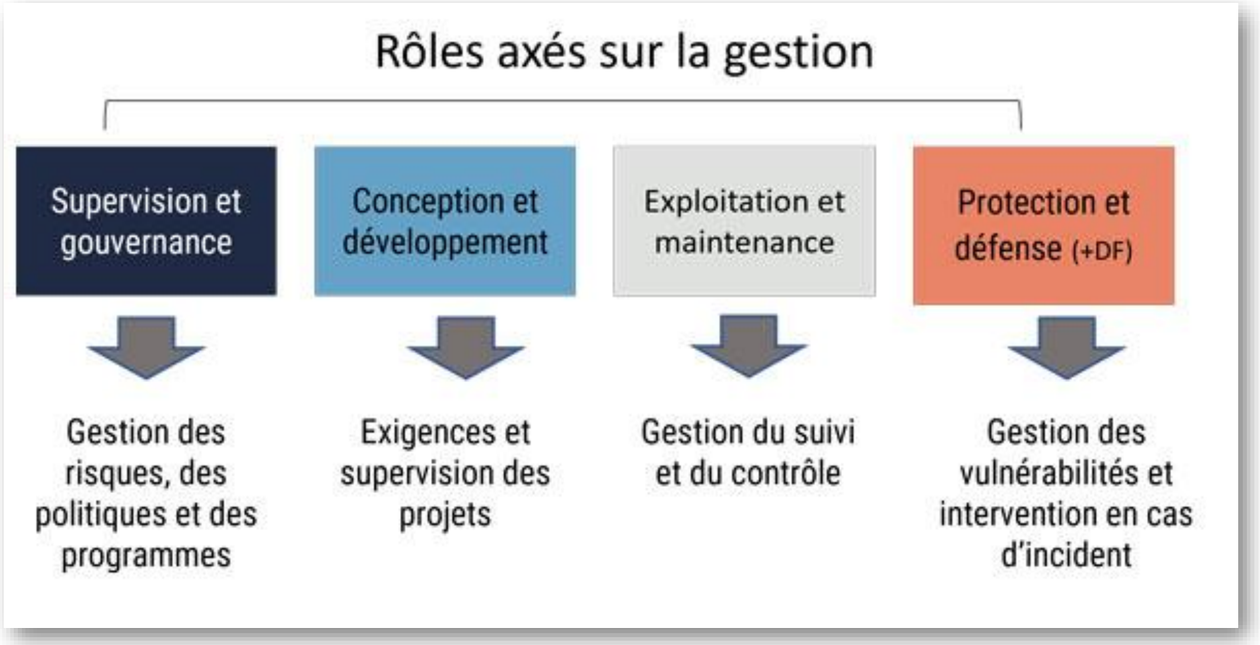
https://bit.ly/cfq-ressource2

Canadianisation du NICE

C’est un vrai mot. Le Centre canadien pour la cybersécurité (CCCS) a décidé d’utiliser le framework NICE en l’adaptant au marché canadien.

CCCS –PME

Cyber Formation Québec



Concept intéressant – Généraliste de la cybersécurité

> « Comme le démontrent les exemples illustrés dans la figure ci-dessous, on doit souvent faire appel à des compétences tirées de certains des rôles de travail appartenant à chacune des grandes catégories d'emplois. »
>
> «Dans plusieurs PMO et même des organisations plus grandes dont les activités ne dépendent pas fortement d'Internet, on retrouve des personnes à qui des responsabilités en cybersécurité ont été confiées sans qu'elles aient nécessairement d'expérience en informatique ou en cybersécurité. »

CADRE DES COMPÉTENCES

Cyber Formation Québec

Compétences et aptitudes de base

- Contexte technique (p. ex. structure informatique organisationnelle, logiciels, dispositifs et politiques)
- Contexte de la cybermenace (dont les risques délibérés, accidentels et naturels)
- Contexte opérationnel (priorités, objectifs, marché, tendances)
- Contexte juridique, politique et éthique de la sécurité
- Gestion des risques liés à la cybersécurité dans le cadre du risque organisationnel
- Gestion des incidents de cybersécurité (propres à un domaine)
- Processus de cybersécurité, technologies, tendances et enjeux émergents
- Sources d’expertise et ressources en cybersécurité

PLAN DE RÉPONSE AUX CYBERINCIDENTS

Vous subirez une cyberattaque…

Il n’y a aucun doute que tôt ou tard vous ferez face à un cyberincident majeur qui causera un impact significatif à votre organisation. Le plan de réponse aux cyberincidents sera votre phare dans les eaux troubles et lorsqu’il fera sombre.

PLAN DE RÉPONSE

Cyber Formation Québec

Introduction

Un plan de réponse aux cyberincidents est un ensemble de procédures et de directives conçues pour gérer efficacement les incidents de sécurité informatique.

- Permet à votre entreprise d'être organisé, laissant ainsi moins de place à l'improvisation.
- Permet de définir clairement les rôles et responsabilités de chacun. (RACI)
- Permet de garder une liste d'informations pertinentes disponibles rapidement. (Ex: contact des fournisseurs externes, etc.)

PLAN DE RÉPONSE

Cyber Formation Québec

PRÉPARATION

IDENTIFICATION

CONFINEMENT

ÉRADICATION

RÉCUPÉRATION

COMMUNICATION

ANALYSE POST-INCIDENT

DOCUMENTATION

PLAN DE RÉPONSE

Cyber Formation Québec

PRÉPARATION

- **Évaluation des risques :** Identifier les menaces et vulnérabilités spécifiques.
- **Évaluation de l'impact :** Déterminer les conséquences potentielles d'un incident sur l'organisation.
- **Formation et sensibilisation :** Former le personnel aux meilleures pratiques en matière de cybersécurité.
- **Établissement d'une équipe de réponse :** Désigner des membres clés et leurs rôles.
- **Liste de contact :** Firme de réponse aux cyberincidents, « *breach coach* », assureur, numéro de cellulaire des ressources clés de l'organisation, etc.

IDENTIFICATION

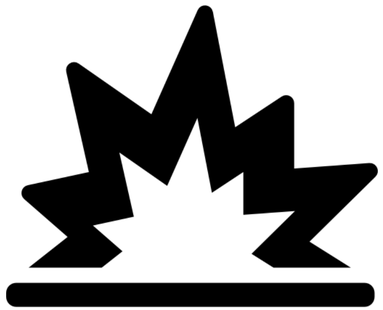
- **Surveillance continue :** Mettre en place des outils de détection pour repérer les anomalies.
- **Analyse des incidents :** Établir des procédures pour classer et évaluer les incidents.
- **Identification des systèmes affectés :** Déterminer quels systèmes, applications et données sont compromis.
- **Analyse des conséquences :** Évaluer les effets sur les opérations, la réputation de l'entreprise et la conformité réglementaire.

PLAN DE RÉPONSE

Cyber Formation Québec

CONFINEMENT

- **Stratégies de confinement :** Mettre en œuvre des mesures pour limiter la portée de l'incident.
- **Désactivation des comptes affectés :** Suspendre les comptes utilisateurs potentiellement compromis pour éviter tout accès non autorisé.
- **Isoler les systèmes affectés :** Couper l'accès aux systèmes compromis.
- **Engagement avec des experts** : Si nécessaire, faire appel à des spécialistes externes pour aider à la gestion de l'incident.



ÉRADICATION

- **Suppression des menaces :** Identifier et éliminer les causes de l'incident.
- **Mise à jour des systèmes :** Appliquer des correctifs et des mises à jour de sécurité.

PLAN DE RÉPONSE

Cyber Formation Québec

RÉCUPÉRATION

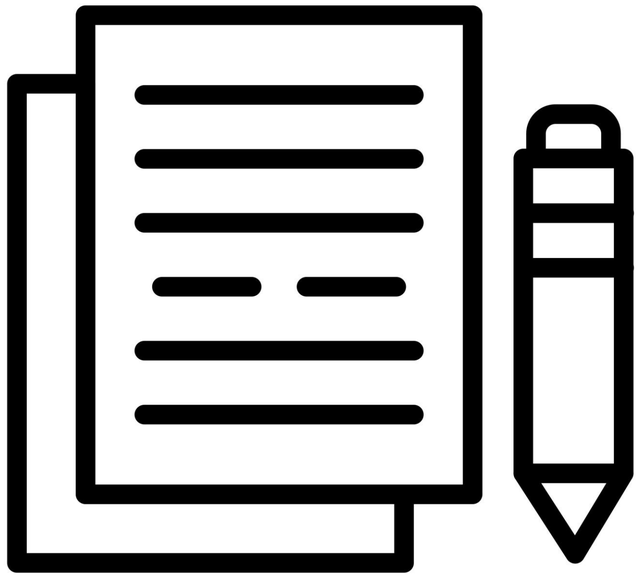
- **Restauration des systèmes :** Remettre en service les systèmes affectés.
- **Validation des opérations :** Vérifier que les systèmes fonctionnent normalement.

COMMUNICATION

- **Notification des parties prenantes :** Informer les employés, partenaires et éventuellement les clients.
    - **Protocoles de notification :** Établir des lignes directrices pour informer les parties prenantes internes et externes.
- **Gestion des relations publiques :** Préparer des messages pour le public si nécessaire.

PLAN DE RÉPONSE

Cyber Formation Québec



ANALYSE POST-INCIDENT

- **Réunion de débriefing :** Évaluer la réponse à l'incident et identifier les points d'amélioration.
- **Mise à jour du plan :** Réviser le plan de réponse en fonction des leçons tirées.
- **Exemple d’un modèle post-incident (TI) :** Lien vers la ressource

DOCUMENTATION

- **Journal des incidents :** Tenir un registre détaillé des événements, des décisions prises et des actions menées.

PLAN DE RÉPONSE

Cyber Formation Québec

https://bit.ly/cfq-ressource3

CCCS – Ressource disponible

Élaborer un plan d'intervention en cas d'incident

Guide et aide à la réflexion pour la conception de votre plan de réponse aux cyberincidents.

Autre ressource: https://cyber.gouv.fr/piloter-la-remediation-dun-incident-cyber

Élaborer un plan d'intervention en cas d'incident : Modèle à remplir et exemple

Élaborer un plan d'intervention en cas d'incident : Modèle à remplir et exemple

De : Innovation, Sciences et Développement économique Canada

Nom de l'entreprise

Plan d'intervention en cas d'incident

Avis de non-responsabilité

CyberSécuritaire Canada a élaboré ce modèle pour votre usage en relation avec les exigences de certification du contrôle de sécurité Élaborer un plan d'intervention en cas d'incident. Il fournit des conseils sur la manière dont les informations peuvent être organisées et documentées en vue de la certification. CyberSécuritaire Canada ne garantit pas que l'utilisation de ce modèle mène nécessairement à l'obtention de la certification. Les entreprises ne sont pas forcées d'utiliser ce modèle et peuvent fournir la ou les exigences

Modèle à remplir : DOCX, 100 ko

Les **modèles à remplir** fournissent des instructions sur les renseignements à consigner aux fins de certification.

[Nom de l'entreprise]

Plan d'intervention en cas d'incident

MODÈLE

Avis de non-responsabilité

Instructions CyberSécuritaire Canada a élaboré ce modèle pour votre usage en relation avec les exigences de certification du contrôle de sécurité Élaborer un plan d'intervention en cas d'incident. Il fournit des conseils sur la manière dont les informations peuvent être organisées et documentées en vue de la certification. CyberSécuritaire Canada ne garantit pas que l'utilisation de ce modèle mène nécessairement à l'obtention de la certification. Les entreprises ne sont pas forcées d'utiliser ce modèle et peuvent fournir la ou les exigences de certification dans le format documenté qui leur convient le mieux.

STANDARDISER LE SERVICE & PRISE EN CHARGE

STANDARDISER!

Standardiser le service, le niveau de sévérité et la prise en charge des événements de cybersécurité est essentiel afin de bien gérer les attentes de l'organisation et de rester optimal dans la gestion des cyberincidents.

EXERCICE

Cyber Formation Québec

- Qu’est-ce qu’un cyberincident?
- Comment défini-t-on un vrai positif vs un faux?
- Est-ce qu’une détection est un cyberincident?
- Quelles seraient les catégories de résolution d’un cyberincident?
- Quel est le temps de réponse acceptable pour un cyberincident?
- Quand peut-on considérer un cyberincident terminé?

STANDARDISATION

Cyber Formation Québec

DÉFINIR UN STANDARD

L’organisation doit s’entendre sur le vocabulaire à utiliser et doit définir ses attentes face à l’équipe ou les ressources qui gère la cyberdéfense opérationnelle.

- Vulnérabilité (VEI)
- Common Vulnerability Scoring System (CVSS)
- Menace interne vs cyberattaquant
- Service Level Agreement (SLA)
- Événement (notable, de sécurité, etc.)
- Cyberincident
- Impact sur l’organisation
- Sévérité des cyberincidents
- Vrai positif
- Faux positif
- Communication
- Heures d’opération?

STANDARDISATION

Cyber Formation Québec

https://bit.ly/cfq-ressource4

CCCS – Ressource disponible

Glossaire

Ce glossaire permet de vous fournir une référence afin de faire un choix éclairé sur les termes qu'utilisera votre organisation.

STANDARDISATION

Cyber Formation Québec

https://bit.ly/cfq-ressource5

NIST – Ressource disponible

Glossaire

Ce glossaire permet de vous fournir une référence afin de faire un choix éclairé sur les termes qu'utilisera votre organisation.

CADRE DE RÉFÉRENCE

Cyber Formation Québec

THE CYBER KILL CHAIN®

ATT&CK®

MITRE D3FEND™

Cadre de référence

- Cyber Kill Chain (Lockheed Martin)
- MITRE ATT&CK (+D3FEND)
- NIST (Cyberincidents, vulnérabilités)

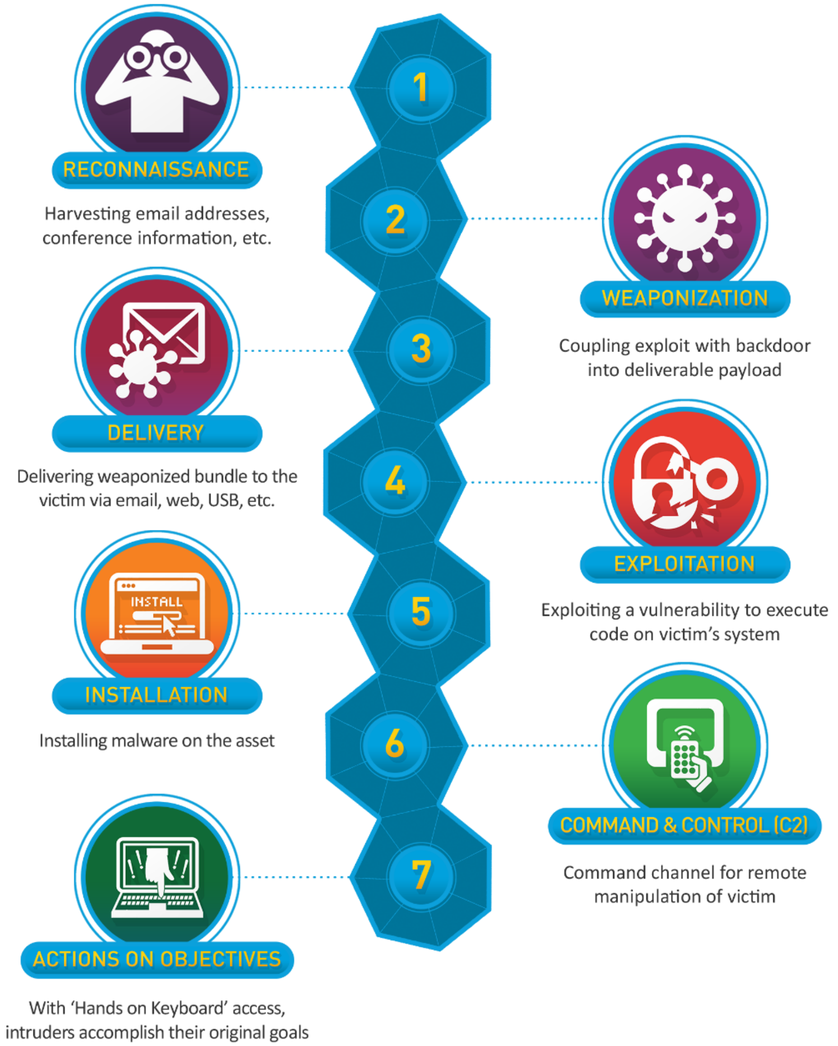
NIST
National Institute of Standards and Technology

CADRE DE RÉFÉRENCE

Cyber Formation Québec

THE CYBER **KILL** CHAIN®

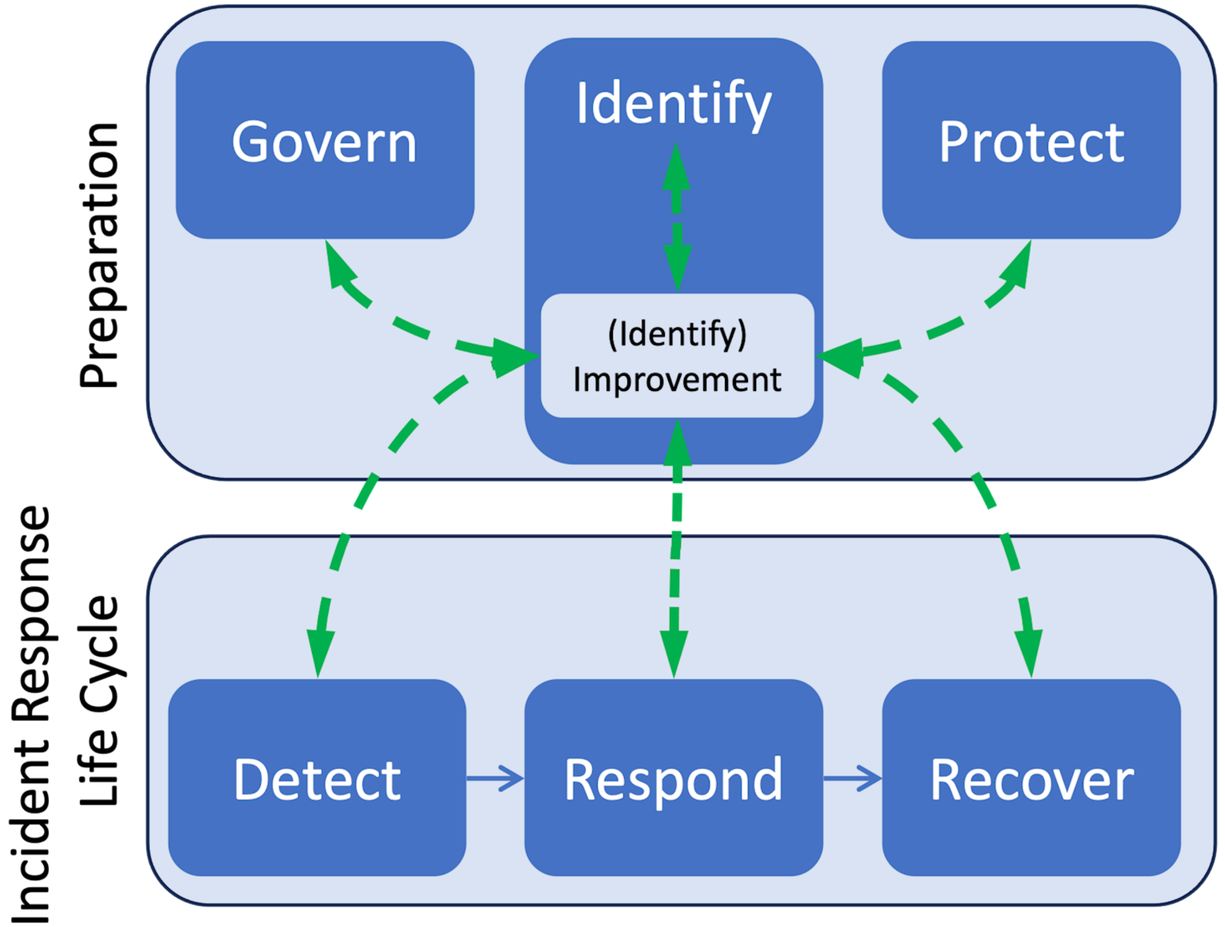
[Lien vers le site Web – Démo (Comprendre les 7 étapes)]



CADRE DE RÉFÉRENCE

Cyber Formation Québec

National Institute of Standards and Technology



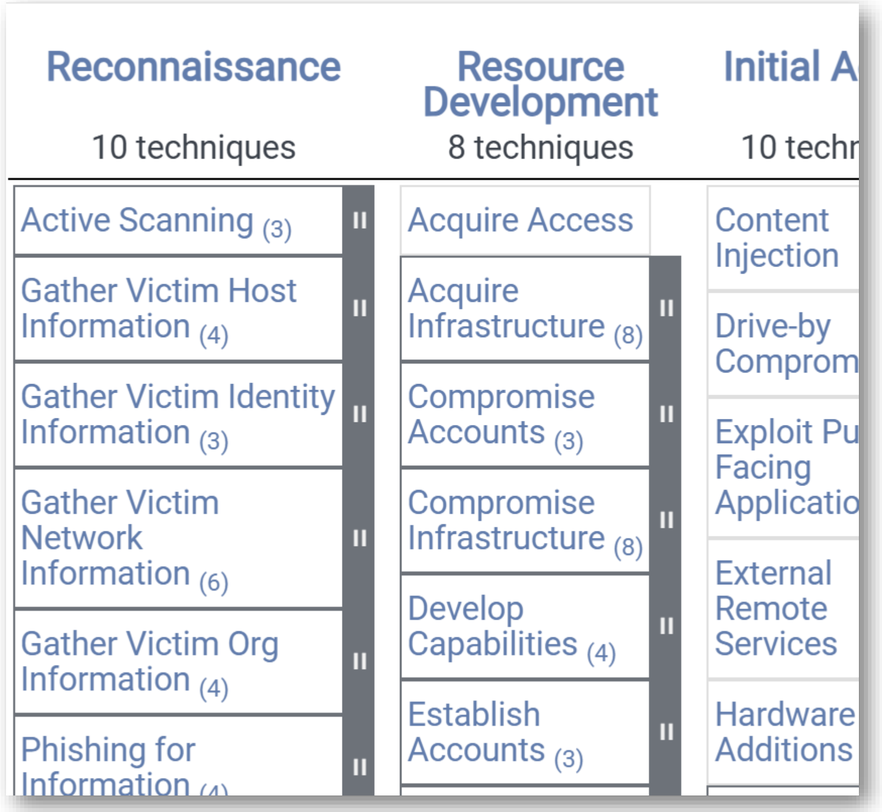
CADRE DE RÉFÉRENCE

Cyber Formation Québec

ATT&CK®

[Lien vers la présentation (Comprendre les tactiques)]

Présentation dans une présentation!

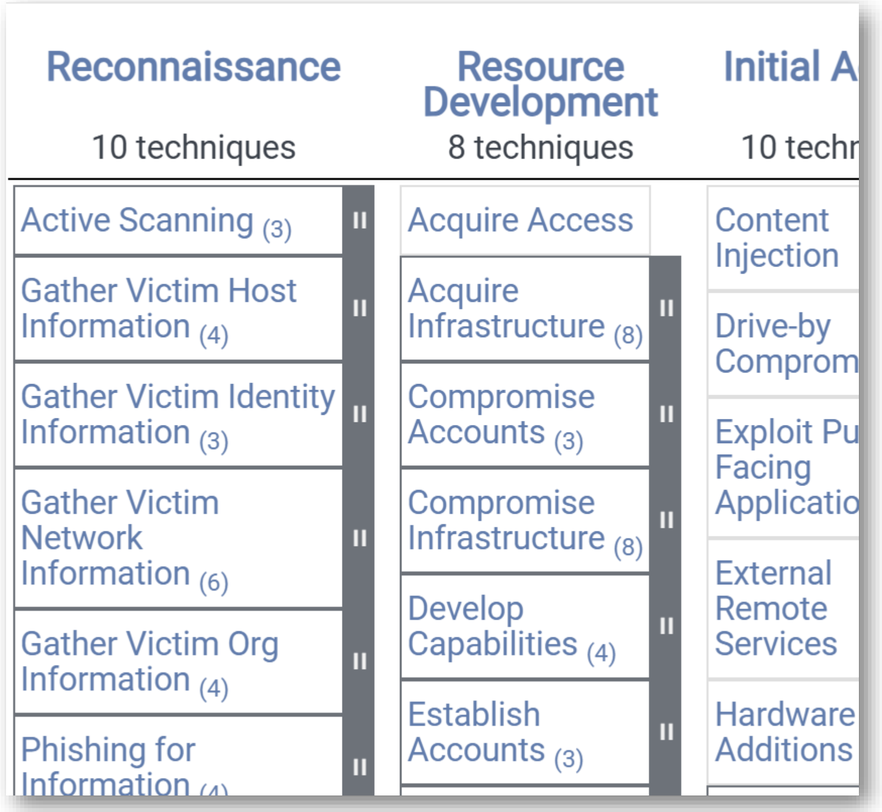


CADRE DE RÉFÉRENCE

Cyber Formation Québec

D3FEND™

[Lien vers le site Web – Démo]



STANDARDISATION (RÉPONSE)

DÉFINIR UNE GRILLE DE SÉVÉRITÉ OU DE PRIORITÉ

- Pour l’organisation
  - Sévérité et impact du cyberincident (implications légales, perte de données, intégrité, confiance des clients, impact sur les opérations, risque avec un tier, type de menace, etc.)
  - Est-ce que l’impact monétaire est un critère pour vous?

STANDARDISATION (RÉPONSE)

- En rafale :
  - Relation avec le tier? Gestion du risque?
    - Avait-il eu une évaluation sommaire? (balayage de vulnérabilité, certifications, etc.)
  - Protocole de reconnexion avec un tier? (SIFMA Reconnection Protocol)
  - Protection des renseignements personnels? Loi 25, AMF, BSIF, etc. (Trousse d’aide pour la loi 25 - mesprocedures.ca)

STANDARDISATION (RÉPONSE)

Cyber Formation Québec

TYPES DE MENACES

J’aime le concept de rester le plus générique possible dans l’établissement des procédures de réponse aux cyberincidents lorsque la situation le permet. Évidemment, il faut plus de précision lors de cas d’exfiltration de données, mais tout de même l’analyste en charge de la réponse doit être en contrôle et avoir la chance d’exercer son pouvoir d’agir. Il faut les responsabiliser.

Encore une présentation dans une présentation …

STANDARDISATION (RÉPONSE)

- Pour la cyberdéfense opérationnelle
  - Procédures opérationnelles pour chaque type de menace (On commence par catégorie, on peut y aller pour chaque cas d'usage ensuite).
    - Exemple brèche fournisseur: SIFMA
  - SLA, les définir pour chaque niveau de priorité défini. (Est-ce que vous êtes 24/7? Qu'est-ce qui mérite votre attention en dehors des heures ouvrables?)

STANDARDISATION (RÉPONSE)

Exemples de procédure de réponse – Démo

Inspiration pour des cas de DDOS, logiciel malveillant, etc.

STANDARDISATION (RÉPONSE)

Cyber Formation Québec

Sujet chaud dans les dernières années:
Quels outils externes pour l'analyse en « *sandbox* »

!!! ATTENTION À VOS DONNÉES !!!

Joe Sandbox

HYBRID ANALYSIS

VMRAY

Recorded Future®
Triage

ASSEMBLYLINE

ANY RUN
INTERACTIVE MALWARE ANALYSIS

PARTAGE D'EXPÉRIENCE

Exemple d'un cyberincident impliquant un rançongiciel dans une entreprise manufacturière.

- Désorganisation et gestion des priorités
- Pression patient-0 vs retour aux opérations
- Implication des consultants (DFIR, légal…)

PARTAGE D'EXPÉRIENCE

Exemple d'une enquête interne sans structure et procédures claires à suivre.

- Direction demande de désactiver les accès d'un employé (Suspicions de vol de données)
- Poste de travail et téléphone mobile et jetons de sessions toujours valides…
- Preuves altérées (Manipulation par les TI sans procédures claires)

INDICATEURS (IPC)

Cyber Formation Québec

INDICATEURS CLÉS DE PERFORMANCE (ICP / KPI)

INDICATEURS (IPC)

Cyber Formation Québec

INDICATEURS CLÉS DE PERFORMANCE (ICP / KPI)

MESURE DES OBJECTIFS

Ils permettent de suivre l'atteinte des objectifs fixés par l'organisation.

PRISE DE DÉCISION

Les ICP fournissent des données concrètes pour prendre des décisions éclairées.

IDENTIFICATION DES PROBLÈMES

Ils aident à repérer les domaines nécessitant des améliorations.

ALIGNEMENT DES EFFORTS

Ils assurent que les tâches et projets sont alignés avec les objectifs stratégiques de l'entreprise.

INDICATEURS (IPC)

Cyber Formation Québec

EXEMPLES

INDICATEURS CLÉS DE PERFORMANCE (ICP / KPI)

MTTA (Cyberincidents)

Mean Time to Assign
Teamps jusqu'à l'assignation

MTTR (Cyberincidents)

Mean Time to Resolve
Temps jusqu'à la résolution

ATTA (Gest. Vuln.)

Average Time To Action
Temps moyen avant la prise en charge

MTTR (Gest. Vuln.)

Mean Time to Remediation
Temps jusqu'à la rémédiation

Int. vs. Ext. (Gest. Vuln.)

Internal Vs External Exposure
Exposition interne vs externe

Asset Coverage (Multiple)

Asset Inventory/Coverage
Couverture de l'inventaire

Ces ICP aident à mesurer l'efficacité et l'efficience des opérations de sécurité, permettant ainsi d'améliorer continuellement les processus et les réponses aux menaces.

CAS D’USAGE

Cyber Formation Québec

DÉFINITION

Les cas d’usage sont utilisés afin de déterminer de quelle façon les outils et solution de sécurité en place peuvent détecter des menaces définies.

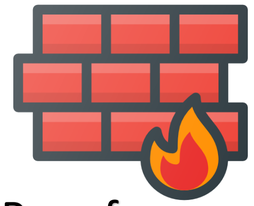
En anglais, on entendra souvent le terme “Use Case”, bien qu’il existe des cas d’usage plus génériques, votre organisation est unique et vous devrez en définir spécifiquement pour celle-ci.

- « Recette » pouvant être appliquée à plusieurs solutions de sécurité.
- Doit aider à détecter une menace concrète et possible.
- Certaines solutions offrent des centaines de cas d’usage par défaut, attention!
- Visez toujours la qualité au lieu de la quantité.

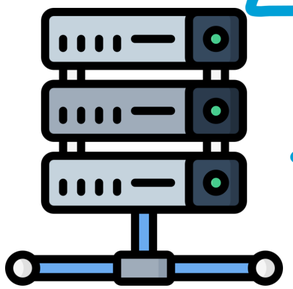
CAS D'USAGE

Cyber Formation Québec

Microsoft Entra ID
Authentification de l'entreprise



Pare-feu avec interface de gestion activée



Service SFTP exposé à l'externe via le pare-feu

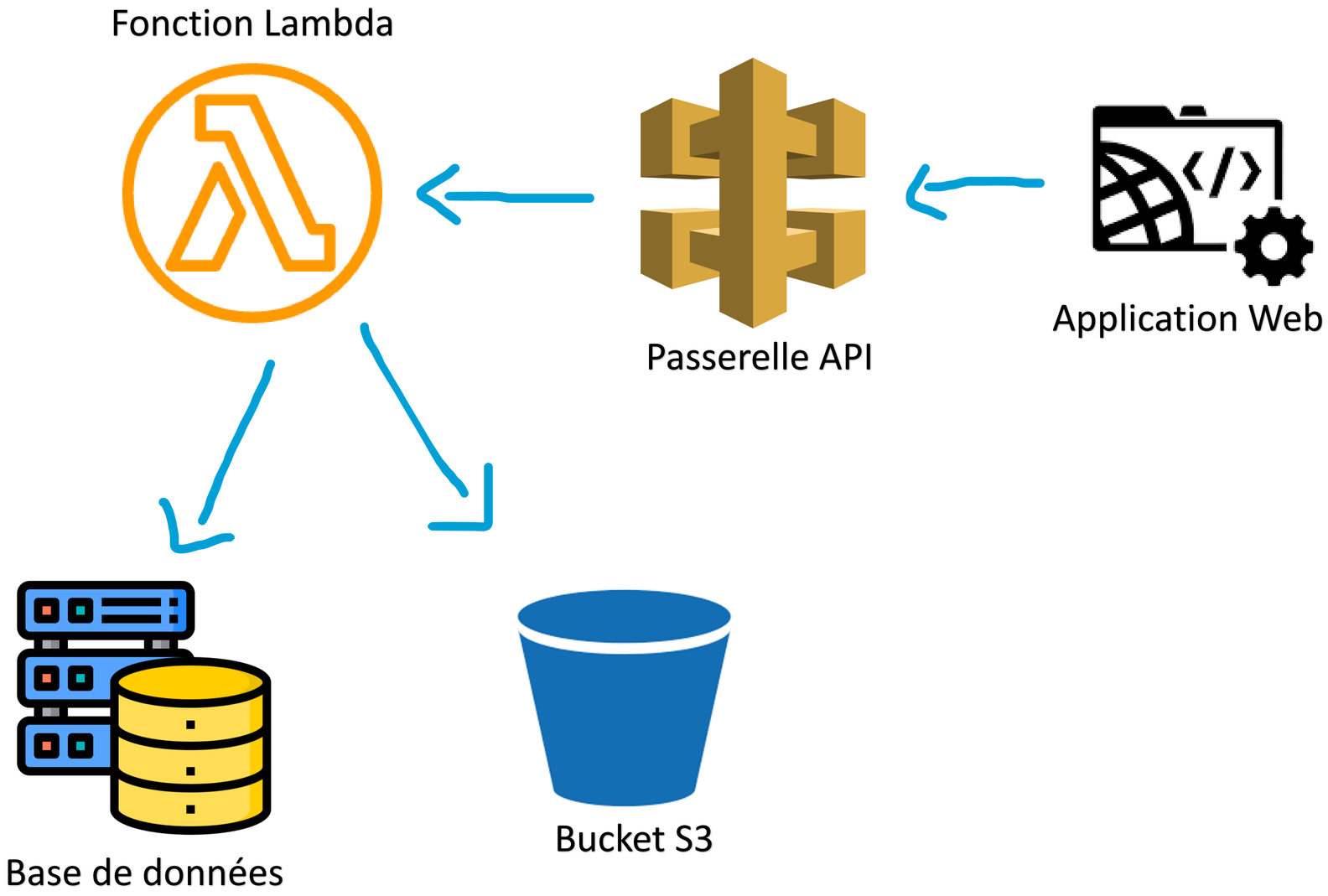
Autres ressources qui n'exposent normalement pas de service sur Internet

EXERCICE

En se basant sur les éléments dans le graphique suivant, quelles seraient des exemples de cas d'usage qui pourraient être pertinent?

CAS D'USAGE

Cyber Formation Québec



EXERCICE

En se basant sur les éléments dans le graphique suivant, quelles seraient des exemples de cas d'usage qui pourraient être pertinent?

L'application Web peut mettre à jour via une API (en passant ensuite par une fonction Lambda) sa base de données et ajouter des fichiers dans un "bucket" S3 afin de les archiver. Il s'agit de données qui ne devraient jamais être accédées directement

CAS D'USAGE

Cyber Formation Québec

- Tentative de connexion à un compte désactivé
- Échec du MFA (ou accès cond.), réussite du mot de passe.
- Déplacement géographique impossible. (2 endroits en même temps)
- Connexions en dehors des heures ouvrables
- Suppression de journaux systèmes ou applicatifs
- Connexions via des services VPN ou provenant de sources suspectes
- Connexion vers un IOC connu
- Ajout d'un utilisateur au groupe d'administrateurs de domaine
- Connexion via un compte de service

CAS D'USAGE

Cyber Formation Québec

CYCLE DE VIE

Votre infrastructure change, vos applications évoluent, vos besoins changent également. Un cas d'usage n'est peut-être plus pertinent après un certain temps.

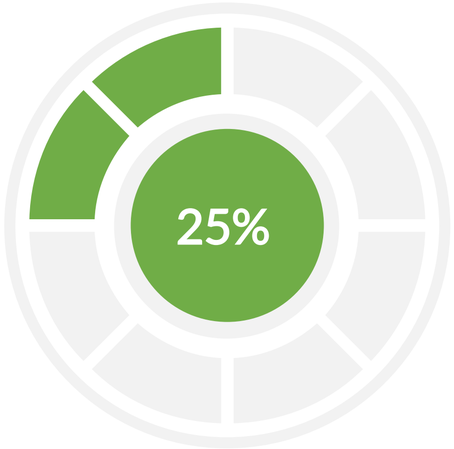
Les sources de données et intégration disponibles dans vos différents outils vont également changer, il est important d'ajuster en conséquence les cas d'usage.

- Définir l'échéance d'un cas d'usage
- A-t-on observé des faux-positif à répétition? (Qualité vs volume)
- A-t-on des nouvelles sources pouvant améliorer le cas d'usage?
- Validation d'un pair avant d'apporter des changements

COUVERTURE & ANGLES MORTS

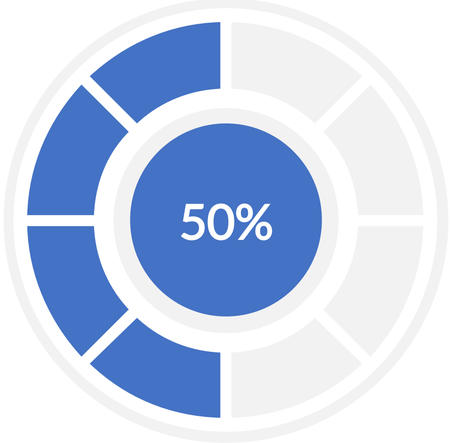
Cyber Formation Québec

Attention: à titre d'exemple et sert de base à la discussion



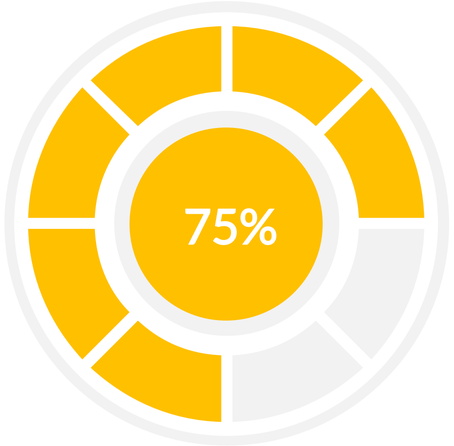
MINIMALE

- AV/EDR
- Journaux des serveurs



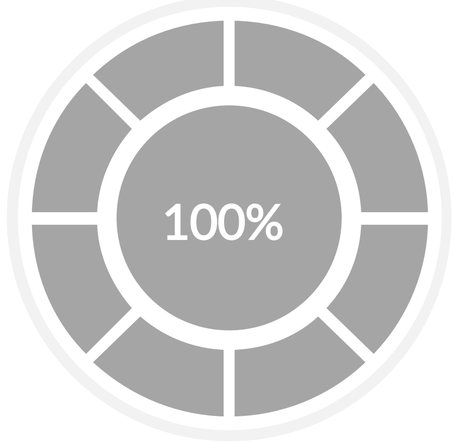
ACCEPTABLE

- NDR (Nord/Sud)
- Journaux des postes de travail
- Requêtes DNS
- VPN



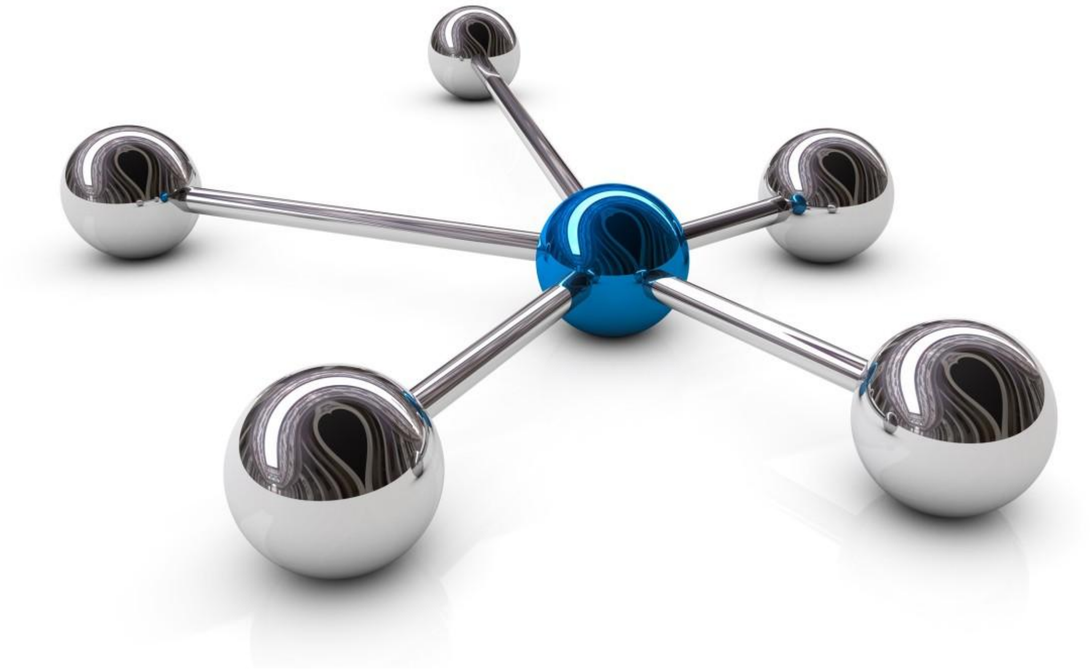
ADÉQUATE

- Déchiffrement du trafic sur les postes (Shadow IT)
- Journaux applicatifs
- Journaux pare-feu



COMPLÈTE

- Inventaire à jour
- NDR (+Est/Ouest)
- Protocol « zero trust »



CENTRALISATION DES INFORMATIONS

ALERTES, JOURNAUX, ...

Pour être en mesure de tirer partie des éléments discuté auparavant de façon optimale, il faut être en mesure de rassembler l'informations.

CENTRALISATION

Cyber Formation Québec

POURQUOI CENTRALISER L'INFORMATION?

SURVEILLANCE

Bénéficier de la corrélation d'évènements et profiter des fonctionnalités d'un SIEM/XDR.

RÉP. CYBERINCIDENTS

Être en mesure d'investiguer et pivoter dans l'ensemble des journaux au même endroit.

GEST. VULN. & AUDIT

Analyse selon les différents profils sur l'ensemble des données disponibles sans efforts supplémentaires.

AVANTAGE COMMUN: GAIN DE TEMPS

CENTRALISATION

Cyber Formation Québec

Afin de centraliser l'information, il faut avant tout posséder un inventaire à jour et le plus complet possible.

Quelles sont les technologies, applications et solutions de sécurité dans votre environnement?

Il faut bien planifier le volume de stockage requis afin d'effectuer une bonne planification des coûts.

Encore une fois, il faut prioriser la qualité au lieu de la quantité. Doit-on tout centraliser ou seulement ce qui a une raison de l'être au minimum.

CENTRALISATION

Cyber Formation Québec

Afin de centraliser l'information, il faut avant tout posséder un inventaire à jour et le plus complet possible.

Quelles sont les technologies, applications et solutions de sécurité dans votre environnement?

Plateformes infonuagiques telles que: AWS, GCP et Azure.

Postes de travail et serveurs (OS)

Plateformes SaaS: Zoho, HubSpot, CRMs, Jira, Github, Salesforce, Box.

Actifs disponibles sur le réseau (IoT, pare-feu, carte d'accès, points d'accès, etc.)

- Flux réseau (métadonnées)
- Appels API (audit, création de ressources, connexions)

- Journaux SE (OS): Windows, Linux, Mac.
- Interface de gestion du serveur
- Authentification, installation, FIM, stockage amovible, etc.

- Journaux d'audit (qui fait quelles actions, téléchargement de document, création de lien partagé, visualisation de profil client, etc.)

- Journaux d'audit (authentification, modification de configuration, création d'utilisateur, etc.)

DEPUIS TOUS LES ÉLÉMENTS: ALERTES, DÉTECTIONS, ÉVÊNEMENTS DE SÉCURITÉ

CENTRALISATION

Cyber Formation Québec

Il faut prioriser la qualité au lieu de la quantité. Doit-on tout centraliser ou seulement ce qui a une raison de l'être au minimum.

VOLUME VS QUALITÉ

- Que va-t-il arriver si vous décidez de tout récupérer par peur d'oublier quelque chose?
- Comment pourrions-nous définir ce que nous avons besoin au minimum? (Établir une stratégie)

Votre texte ici

RÉVISION DES SOURCE SUR UNE BASE RÉGULIÈRE (EX: ANNUELLEMENT)

CENTRALISATION

Cyber Formation Québec

https://bit.ly/cfq-ressource6

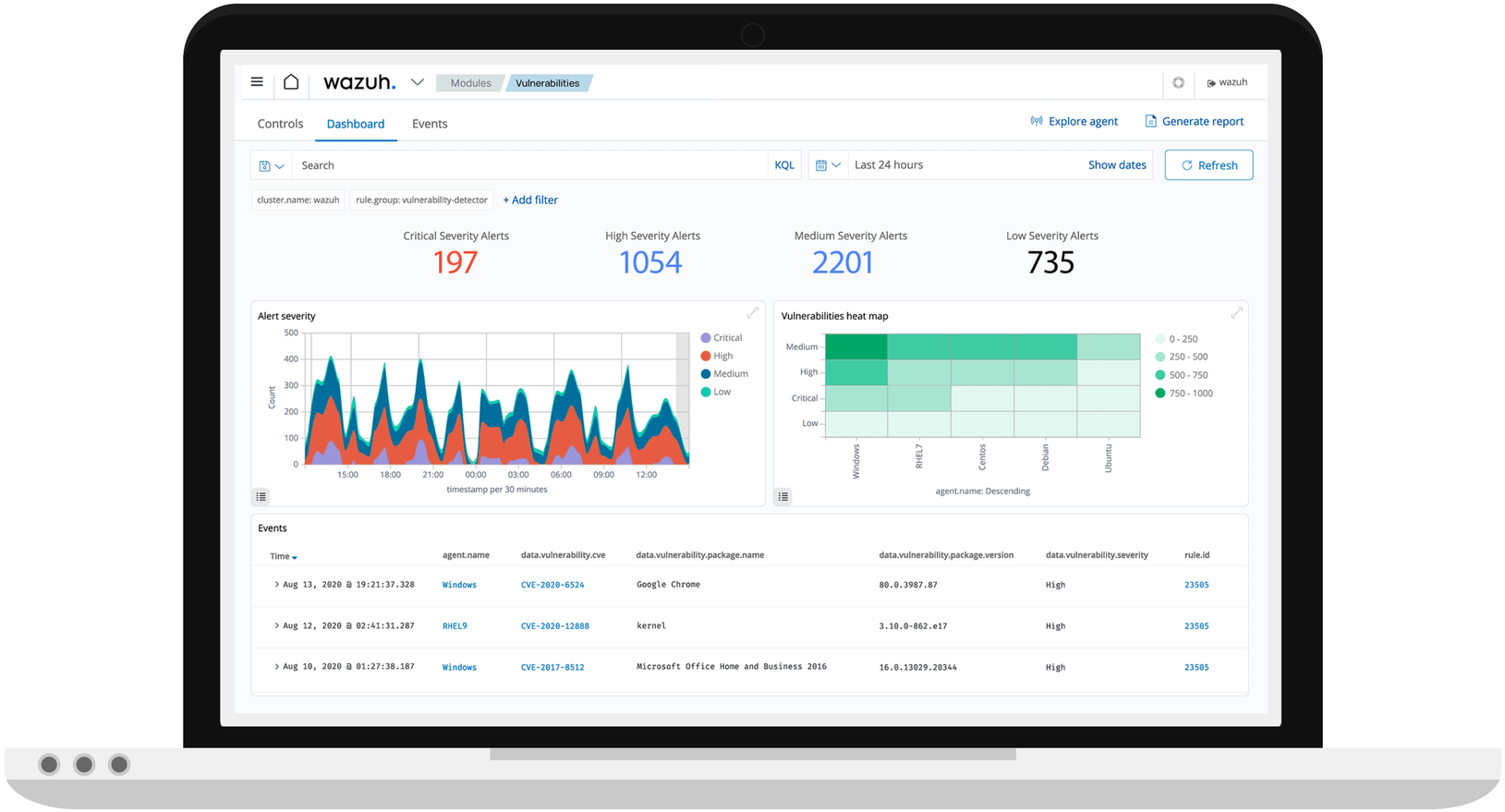
Wazuh (SIEM/XDR) - YouTube

Aperçu des capacités d'un SIEM/XDR
présenté par John Hammond.

Outre le produit (qui est très bien en passant) c'est une excellente ressource vidéo qui montre la valeur d'un SIEM/XDR (concret)

DÉMO SIEM/XDR

Cyber Formation Québec



PROTECTION DES ACTIFS

UNE AUTRE RESPONSABILITÉ

L’équipe de cyberdéfense opérationnelle possède souvent également le rôle de protecteur des actifs. Ils doit s’assurer que ceux-ci soient configurés sécuritairement, protégé et qu’ils soient à jour.

PROTECTION DES ACTIFS

Cyber Formation Québec

ASPECTS CLÉS

La gestion des vulnérabilités et la protection des actifs sont souvent mis ensemble dans une organisation de petite ou moyenne taille. La mission: empêcher un acteur de menace de compromettre votre environnement ou vos données.

- Définir une façon d'établir une priorité aux vulnérabilités
- Identifier les cadres ou références à suivre et s'y attacher dans le temps (Ex: CIS Benchmarking pour l'endurcissement)
- Travailler étroitement en collaboration avec les TI afin de trouver un plan d'action raisonnable
- Déterminer le périmètre à protéger et la criticité de celui-ci.

Parlons justement du périmètre ...

PROTECTION DES ACTIFS

Cyber Formation Québec

9 in 10 organizations have embraced zero-trust security globally (CSO Online)

Organisations must make bold decisions to build a robust security position for the future

Qu’est-ce que le « zero-trust » ⟶

PROTECTION DES ACTIFS

Cyber Formation Québec

QU'EST-CE QUE LE ZERO-TRUST?

Il s'agit d'une approche de la cybersécurité qui repose sur le principe de « ne jamais faire confiance, toujours vérifier ». (pas le traditionnel « *Trust, but verify* ») [FR : Confiance nulle]

VÉRIFICATION EXPLICITE

Chaque demande d'accès doit être authentifiée et autorisée en fonction de plusieurs points de données, tels que l'identité de l'utilisateur, la localisation, l'état du dispositif, et la classification des données

MOINDRE PRIVILÈGE

Les utilisateurs ne reçoivent que les permissions nécessaires pour accomplir leurs tâches, limitant ainsi les risques en cas de compromission

SUPPOSITION DE COMPROMISSION

Le modèle part du principe que des menaces existent déjà à l'intérieur du réseau. Il segmente l'accès pour minimiser les impacts potentiels et utilise des analyses pour détecter les anomalies

PROTECTION DES ACTIFS

Cyber Formation Québec

Protection contre les menaces et les tentatives d'exploitation. (AV/EDR)

Analyse du trafic réseau, des plateformes utilisées et protection contre l'exfiltration des données. (SASE/ZTNA/CASB/SWG/DLP)

Identification des vulnérabilités et inventaire des applications. (VAM)

PROTECTION DES ACTIFS

Cyber Formation Québec

Endpoint Detection and Response (EDR)

AV/EDR

- Il s’agit d’une solution de cybersécurité conçue pour détecter et répondre aux menaces sur les actifs tels que les postes de travail, les serveurs et les appareils mobiles. (Capacité encore limité sur les mobiles)
- L’EDR ajoute une capacité qui en fait sa force: la détection de comportements suspicieux. On ne se base plus seulement sur des signatures pour détecter une menace, mais sur un ensemble de critères ou d’évènements.
- La majorité des évènements sur l’actif vont être journalisés permettant une investigation plus efficace. (Bon niveau de granularité, ex: quel processus système à lancé un script, requêtes DNS, etc.)

NOTE ADDITIONELLE

Cet outil vous permettra également d’effectuer des actions de réponse aux cyberincidents telles que : exécuter des commandes, télécharger et téléverser des fichiers, effectuer une copie de la mémoire complète ou de certains processus, lister les processus actifs, etc.

PROTECTION DES ACTIFS

Cyber Formation Québec

ANALYSE DU TRAFIC & ACTIONS

- Détecter les applications infonuagiques utilisées au sein de l'organisation. (Shadow IT)
- Analyse du contenu des requêtes entrantes et sortantes afin d'identifier l'exfiltration de données ou s'il s'agit de contenu malicieux.
- Appliquer des conditions pour l'accès à des ressources infonuagiques où internes à votre organisation. Par exemple : vous devez être au Canada et utiliser Google Chrome à jour pour vous connecter au Jira de votre organisation.
- Des règles d'accès conditionnelles peuvent être appliquées sur votre compte afin d'accéder aux différentes ressources

NOTE ADDITIONELLE

Afin d'être efficace et de remplir leurs rôles, il est important que vos outils soient en mesure de déchiffrer (au minimum) le trafic et les actions effectuées via HTTPS. Le déchiffrement est un défi dans plusieurs organisations considérant l'atteinte potentielle à la vie privée.

PROTECTION DES ACTIFS

Cyber Formation Québec

DÉTECTION DES VULNÉRABILITÉ

L’agent d’évaluation des vulnérabilités est un outil ou une solution utilisée pour identifier, évaluer et gérer les vulnérabilités sur les systèmes informatiques. (Postes de travail ou serveurs)

- Le VAM scanne les systèmes pour détecter les failles de sécurité, les configurations incorrectes et les logiciels obsolètes.
- Il évalue la gravité des vulnérabilités découvertes et leur potentiel impact sur le système.
- Il génère des rapports détaillés sur l'état de sécurité des systèmes, facilitant les audits de sécurité et la conformité réglementaire.

PROTECTION DES ACTIFS

Cyber Formation Québec

Il évalue la gravité des vulnérabilités découvertes et leur potentiel impact sur le système.

Quels sont vos défis quand vient le temps de faire corriger les vulnérabilités?

Pas de contrat de service pour obtenir les mises à jour

Résistance

Trop de changements à apporter

Disponibilité des systèmes

Disponibilité des ressources

PROTECTION DES ACTIFS

Cyber Formation Québec

RISQUE VS OPS

Gérer la balance entre le risque cyber et les opérations dans un programme de gestion des vulnérabilités est un aspect non négligeable pour assurer la sécurité tout en maintenant l'efficacité opérationnelle

- Évaluation des Risques
- Priorisation des Vulnérabilités
- Planification des Correctifs
- Automatisation et Surveillance
- Communication et Collaboration

PROTECTION DES ACTIFS

Cyber Formation Québec

COMMENT DÉMONTRER LE SÉRIEUX DE LA DÉMARCHE À L'ORGANISATION?

- Établir un standard: évaluation selon des critères clairs et constants (Définir un SLA adéquat / Plan d'action avec les équipes TI)
- Être compréhensif du contexte d'affaires. Il faut souvent trouver le juste milieu.

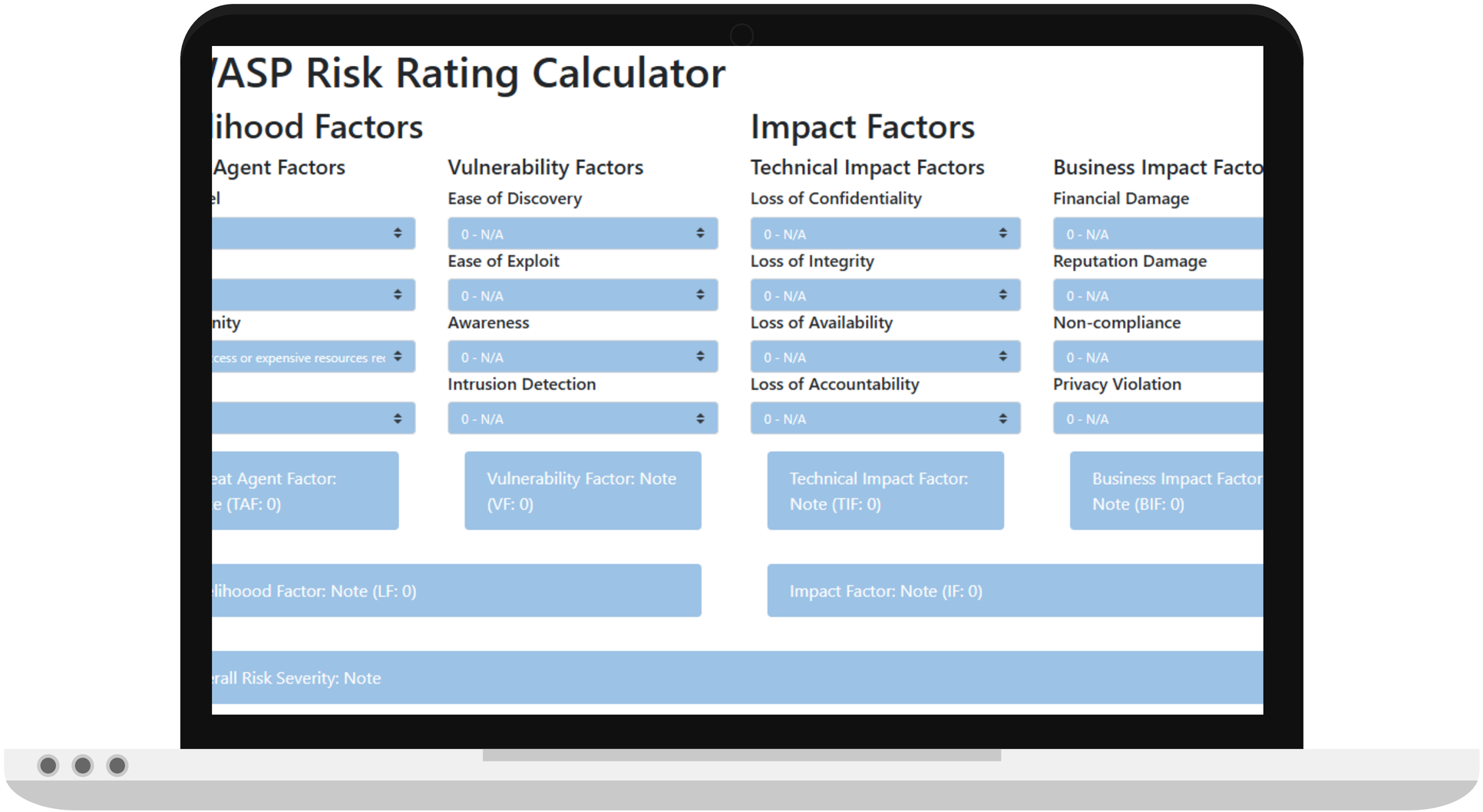
CVSS v3.1 est toujours largement utilisé comme référence aujourd'hui

Formation gratuite sur CVSS v4.0
https://learn.first.org/

Exemple d'un outil d'évaluation granulaire (Second regard) →

PROTECTION DES ACTIFS

Cyber Formation Québec



PROTECTION DES ACTIFS

Cyber Formation Québec

EXERCICE

https://www.owasp-risk-rating.com/

SCÉNARIO

- Une librairie utilisé sur une application hébergée à l'intérieur de votre environnement semble être exploitable selon un article lu récemment. (Bleeping Computer)
- Pour que cette librairie s'exécute, l'utilisateur doit effectuer une action mais celle-ci est seulement permise lorsqu'il est connecté à celle-ci.
- Il n'existe pas d'exploit disponible au grand publique à ce jour pour cette vulnérabilité.
- L'application sert a envoyer des cartes cadeau de 5$ à d'autres employés en guise de remerciement pour leur aide dans divers projets. (Les 20 employés ne peuvent qu'en envoyer une fois par 3 mois)
- L'historique des cartes envoyées est disponible dans l'application.
- Si un attaquant réussi à exploiter cette vulnérabilité, il pourrait communiquer directement avec le service du fournisseur via API pour commander des cartes cadeaux sans aucunes vérifications préalables par contre, les actions seraient journalisées

PROTECTION DES ACTIFS

Cyber Formation Québec

CONFIGURATION SÉCURISÉE

> La configuration sécurisée ou généralement « hardening » en anglais est un ensemble de pratiques visant à renforcer la sécurité des systèmes informatiques en réduisant leur surface d'attaque et en permettant un meilleur audit des activités.

CIS Center for Internet Security®

- Désactivation des services inutiles
- Configuration des paramètres de sécurité
- Contrôle des accès
- Surveillance et audit

PROTECTION DES ACTIFS

Cyber Formation Québec

CENTER FOR INTERNET SECURITY

Les CIS Benchmarks sont des recommandations de configuration de sécurité élaborées par le Center for Internet Security (CIS). Elles fournissent des directives détaillées pour sécuriser divers systèmes et technologies.

RECOMMANDATIONS DE SÉCURITÉ

Les CIS Benchmarks offrent des configurations de sécurité spécifiques pour plus de 25 familles de produits, incluant les systèmes d'exploitation, les appareils mobiles, les réseaux, et les **applications cloud.**

CONFORMITÉ ET RÉGLEMENTATION

Ils aident les organisations à se conformer aux réglementations et aux cadres de sécurité en vigueur, en fournissant des configurations standardisées et éprouvées.

AMÉLIORATION DE LA SÉCURITÉ

En suivant ces recommandations, les organisations peuvent renforcer leurs défenses contre les cybermenaces et réduire les risques de vulnérabilités

CIS Benchmarks™

PROTECTION DES ACTIFS

Cyber Formation Québec

NIVEAUX DE PROTECTION

Les CIS Benchmarks offrent deux niveaux de protection selon la criticité et sécurité requise sur les actifs.

- **Niveau 1 :** recommande des exigences de base en matière de sécurité qui peuvent être configurées sur un système quelconque et qui doivent provoquer peu ou pas d'interruption de service ou de fonctionnement réduit.*
- **Niveau 2 :** recommande des paramètres de sécurité pour les environnements nécessitant une sécurité accrue qui pourraient entraîner un fonctionnement réduit.*

DÉMO

Accès aux CIS Benchmarks

CHASSE À LA MENACE & PROACTIVITÉ

RAPPEL DU RÔLE

Consiste à rechercher activement des menaces potentielles ou inconnues au sein du réseau d'une organisation avant qu'elles ne causent des dommages.

CHASSE À LA MENACE

Cyber Formation Québec

PILLIERS ET CONCEPTS CLÉS

Proactivité

Contrairement aux méthodes traditionnelles qui réagissent aux incidents après leur détection, la chasse à la menace vise à identifier les menaces avant qu'elles ne se manifestent

Réduction des délais de détection

En identifiant les menaces plus rapidement, elle réduit le temps pendant lequel une menace peut rester non détectée et potentiellement causer des dommages

Analyse humaine et automatisée

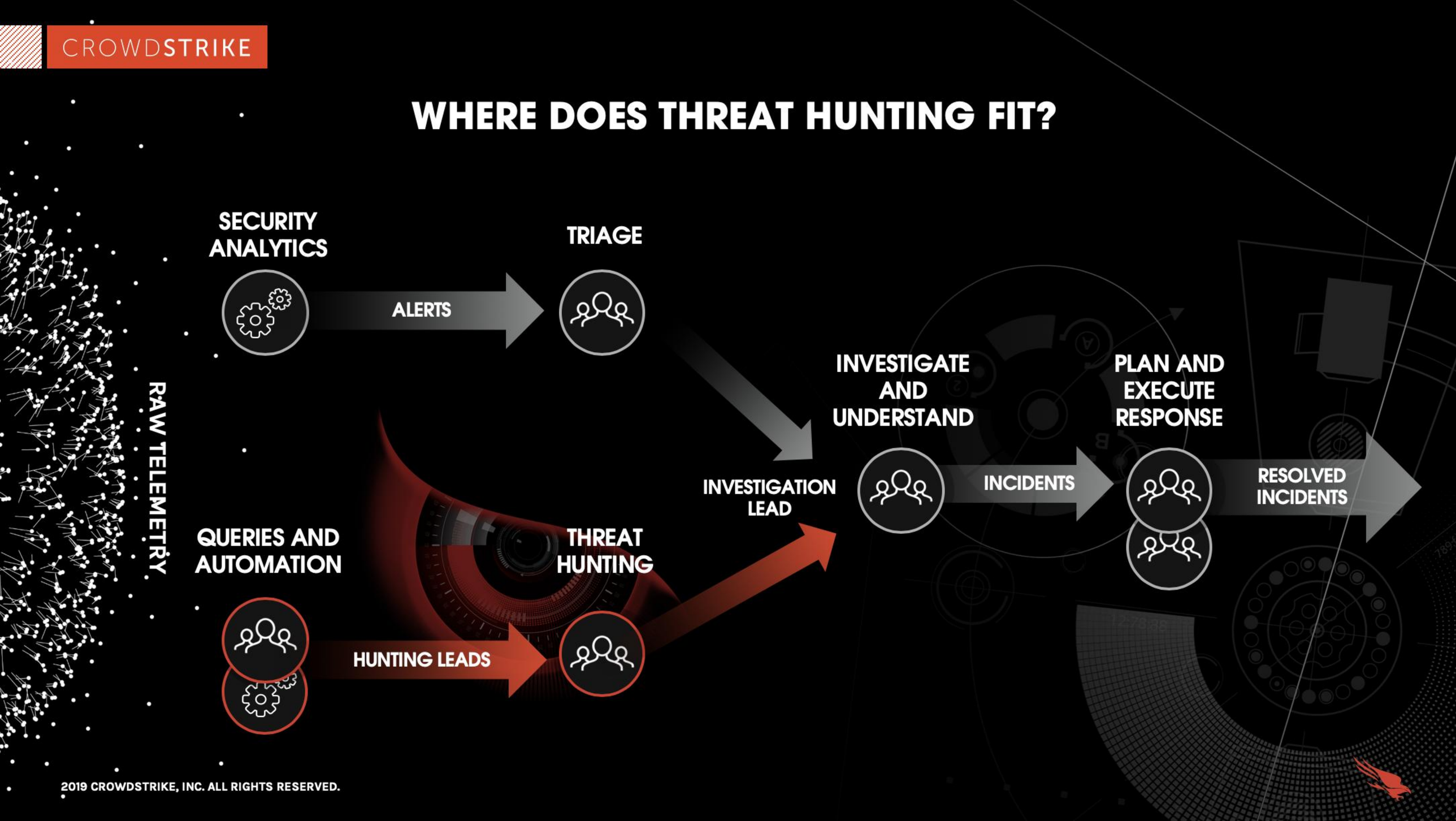
Elle combine l'expertise humaine avec des outils automatisés pour analyser les données et détecter des comportements suspects

Utilisation de données

Les chasseurs de menaces utilisent des données de sécurité collectées à partir de divers systèmes pour repérer des anomalies

CROWDSTRIKE

WHERE DOES THREAT HUNTING FIT?



CHASSE À LA MENACE

Cyber Formation Québec

PRIORISATION DES MENACES

Grâce aux informations de la CTI, les chasseurs de menaces peuvent prioriser les menaces en fonction de leur pertinence et de leur impact potentiel sur l'organisation[3]. Cela permet de concentrer les efforts sur les menaces les plus critiques

CONTEXTE DES MENACES

La CTI offre un contexte détaillé sur les menaces, y compris les tactiques, techniques et procédures (TTP) utilisées par les attaquants

RENSEIGNEMENTS & CYBERMENACES

RAPPEL DU RÔLE

Discipline de la cybersécurité qui consiste à collecter, analyser et interpréter des informations sur les menaces potentielles ou actuelles.

RENSEIGNEMENTS & CYBERMENACE

Cyber Formation Québec

PILLIERS ET ASPECTS CLÉS

COLLECTE DES DONNÉES

Le CTI implique la collecte de données provenant de diverses sources, telles que les réseaux sociaux, les forums de discussion, les bases de données de menaces, et les rapports de sécurité

PRÉPARATION ET RÉPONSE

Les informations obtenues permettent aux entreprises de mieux se préparer et de répondre plus efficacement aux cyberattaques

Intrant aux cyberincidents?

ANALYSE DES MENACES

Les analystes CTI examinent ces données pour identifier des tendances, des tactiques, techniques et procédures (TTP) utilisées par les cybercriminels

PARTAGE D'INFORMATIONS

Le CTI favorise également le partage d'informations entre les organisations pour renforcer la sécurité collective

RETOUR SUR VOS QUESTIONS & DISCUSSIONS