ITSec
SOMMET DE LA SÉCURITÉ INFORMATIQUE
PRÉSENTÉ PAR DEVOLUTIONS ET SHERWEB

JOURNÉE DE FORMATION

Cyber Threat Intelligence en Action

Analyses des Cybermenaces

Téléchargez votre application *Whova*

Connectez-vous à votre profil en entrant l'adresse courriel utilisée lors de votre inscription.

Whova vous permet de :

Vous mettre présent dans la formation suivie

Recevoir votre **badge de certification!**

Télécharger dans l'App Store

DISPONIBLE SUR Google Play

Devolutions

Ordre du jour

- Présentation
- Introduction au Cyber Threat intelligence
- Cycle de vie du CTI
- Comment commencer une activité de CTI
- Pyramid of pain
- Processus
- Communiquer le CTI au cadre
- Démo
- Exercice Pratique
- Conclusion et période de questions

À propos de nous

Martin Lemay

- Chez Devolutions depuis 6 ans
- Fondateur de *CyberSpective*
- *Certification : CGEIT, CISM, CRISC, CISA*

William Matos

- Spécialiste SecOPS & CTI chez Devolutions
- Chargé de cours au Cégep de Lanaudière
- 4 ans d'expérience en Cyber Sécurité
- B.Sc en Cybersécurité

Introduction au Cyber Threat Intelligence

Définition et objectifs du CTI

Une pratique visant à collecter, produire, analyser et distribuer de l'information pertinente sur les menaces et les acteurs malveillants.

L'objectif :

Contextualiser les cybermenaces au sein de l'organisation pour améliorer continuellement la stratégie de défense proactive, efficace et efficiente.

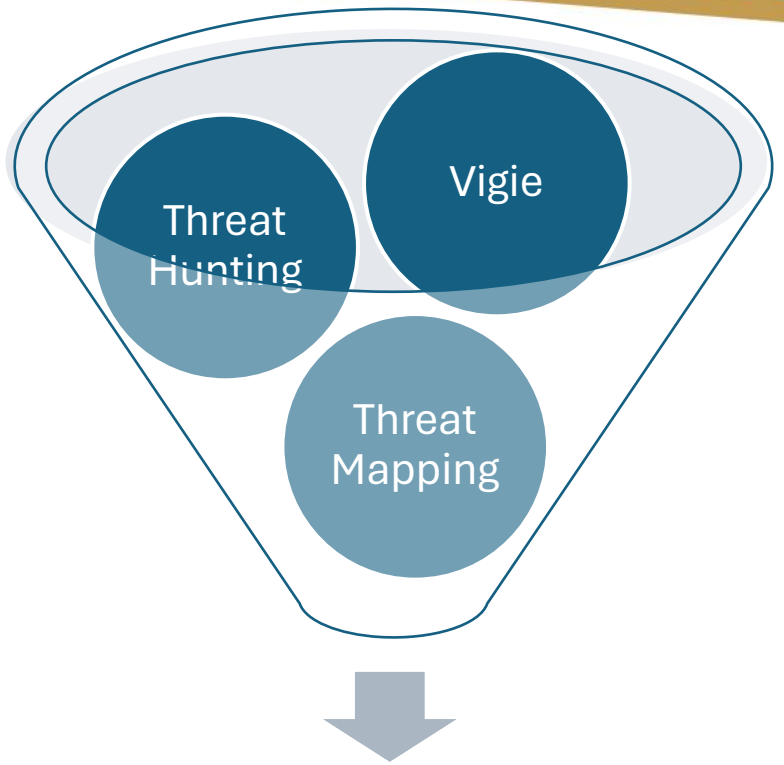
Le CTI n'est pas une fin en soi, mais une pratique essentielle qui renforce la gestion des risques, améliore la posture de cyberdéfense et accroît l'efficacité des opérations.

不知彼　不知己　每戰必殆
不知彼而知己　一勝一負
故曰　知彼知己　百戰不殆

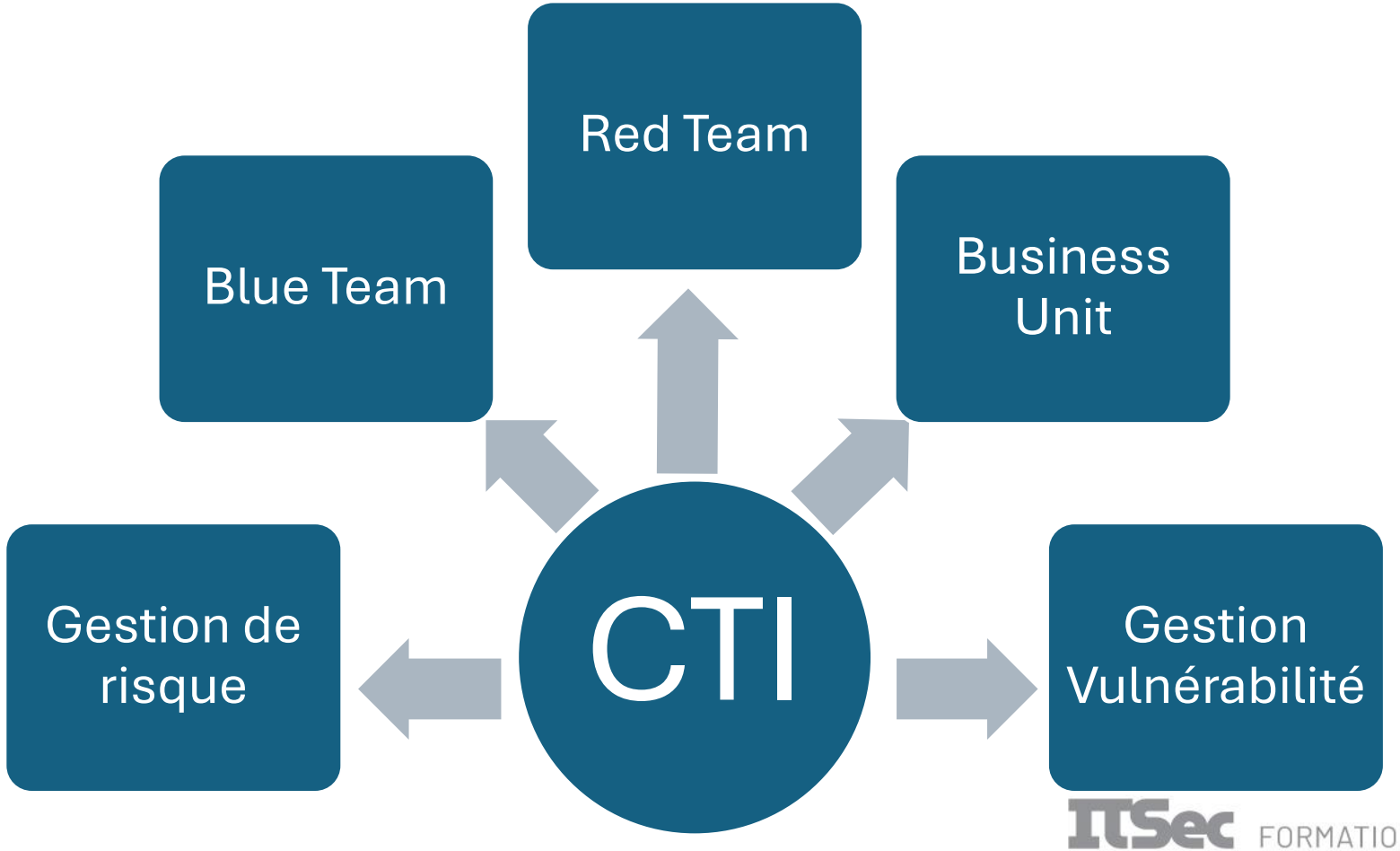
« Know The Enemy and Know Yourself » - Sun Tzu

ITSec FORMATION

Introduction au Cyber Threat Intelligence

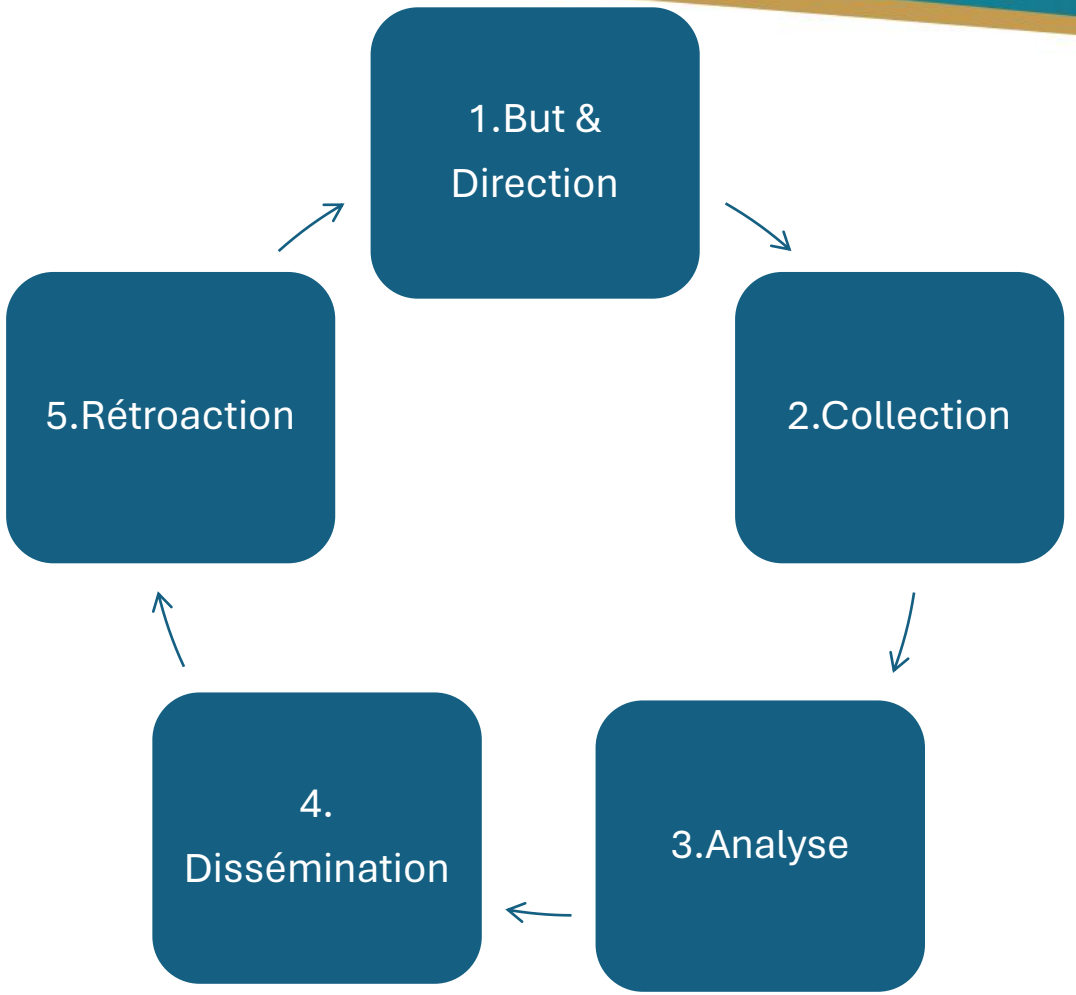


Intelligence Actionnable



ITSec FORMATION

Cycle de vie du CTI



1. **Rédiger un objectif clair**, en identifiant les actifs nécessitant protection et les menaces à traiter. Nous établirons également des priorités concernant les exigences des renseignements requis.
2. **Identifier nos sources de collection**, interne, externe, blog, etc.
3. **Analyser et transformé les données** en informations concrète.
4. **Comprendre notre audience** pour présentation l'information en intelligence actionnable au niveau stratégique, tactique, opérationnel.
5. **Évaluer en continue** le succès du programme et suivre son évolution.

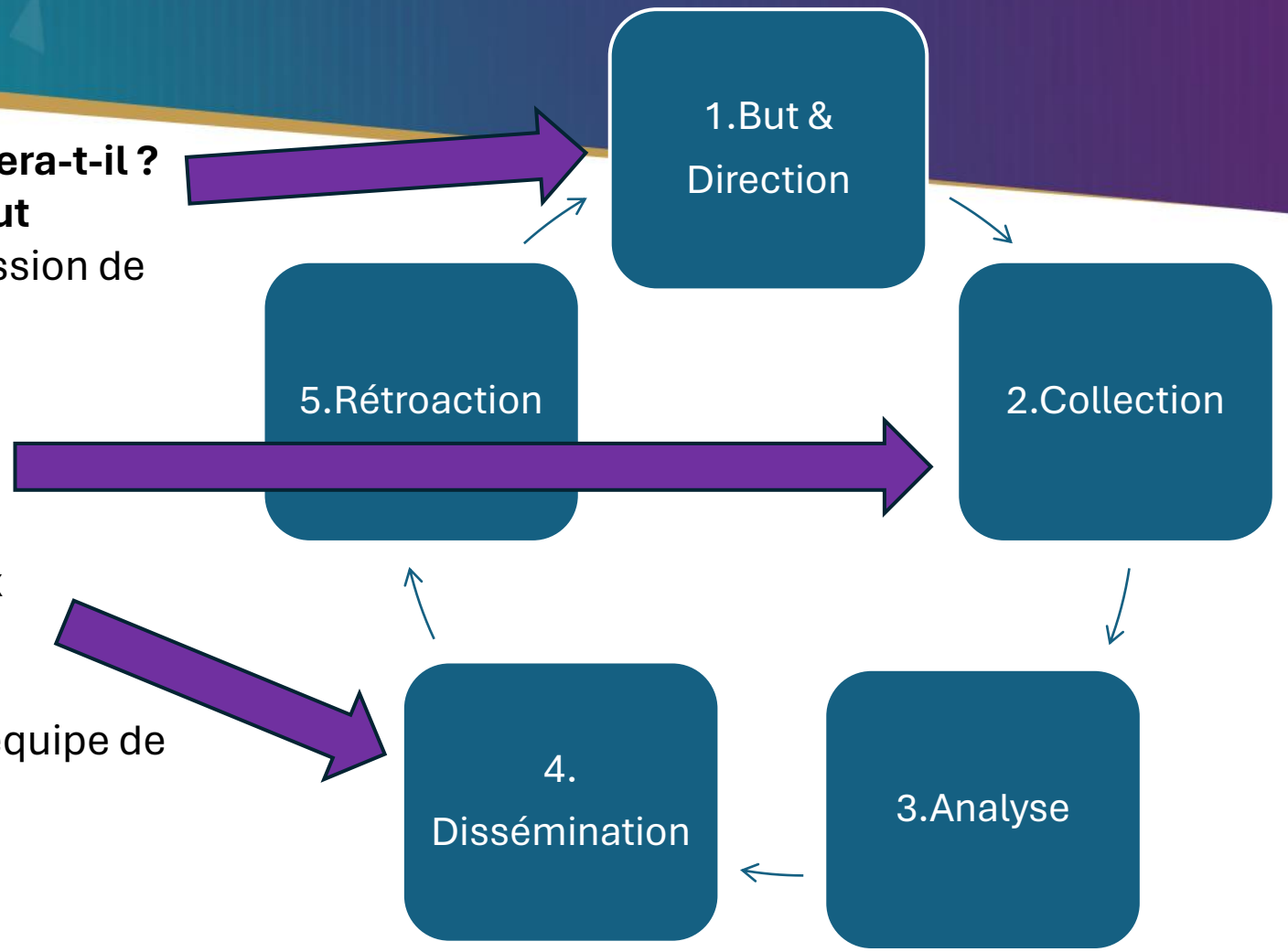
Cycle de vie du CTI - Exemple

- **À quel endroit du périmètre l'adversaire attaquera-t-il ?**
- **Quelles sont les menaces sur lesquelles on veut s'informer davantage** ; Ransomware, compromission de la chaîne d'approvisionnement ?

Outils qui serviront de renseignement : Un SIEM, un honeypot, une plateforme de CTI ou des blogs.

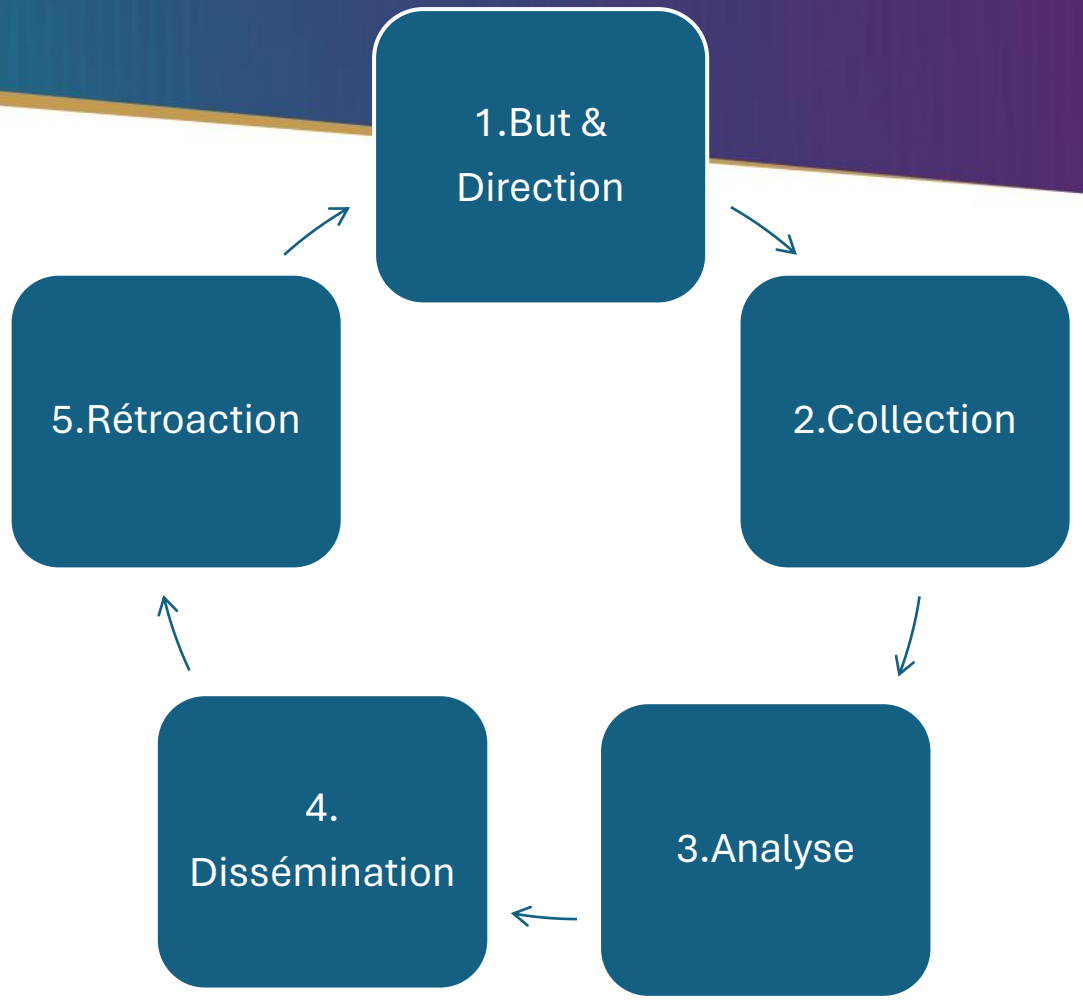
Rendre notre analyse actionnable pour répondre aux questionnements de notre organisation.

1. Stratégique : Coût d'une fuite de données.
2. Tactique : Fournir des techniques d'attaques à l'équipe de défense.
3. Opérationnel : Fournir des indicateurs de compromissions à intégrer dans nos outils.



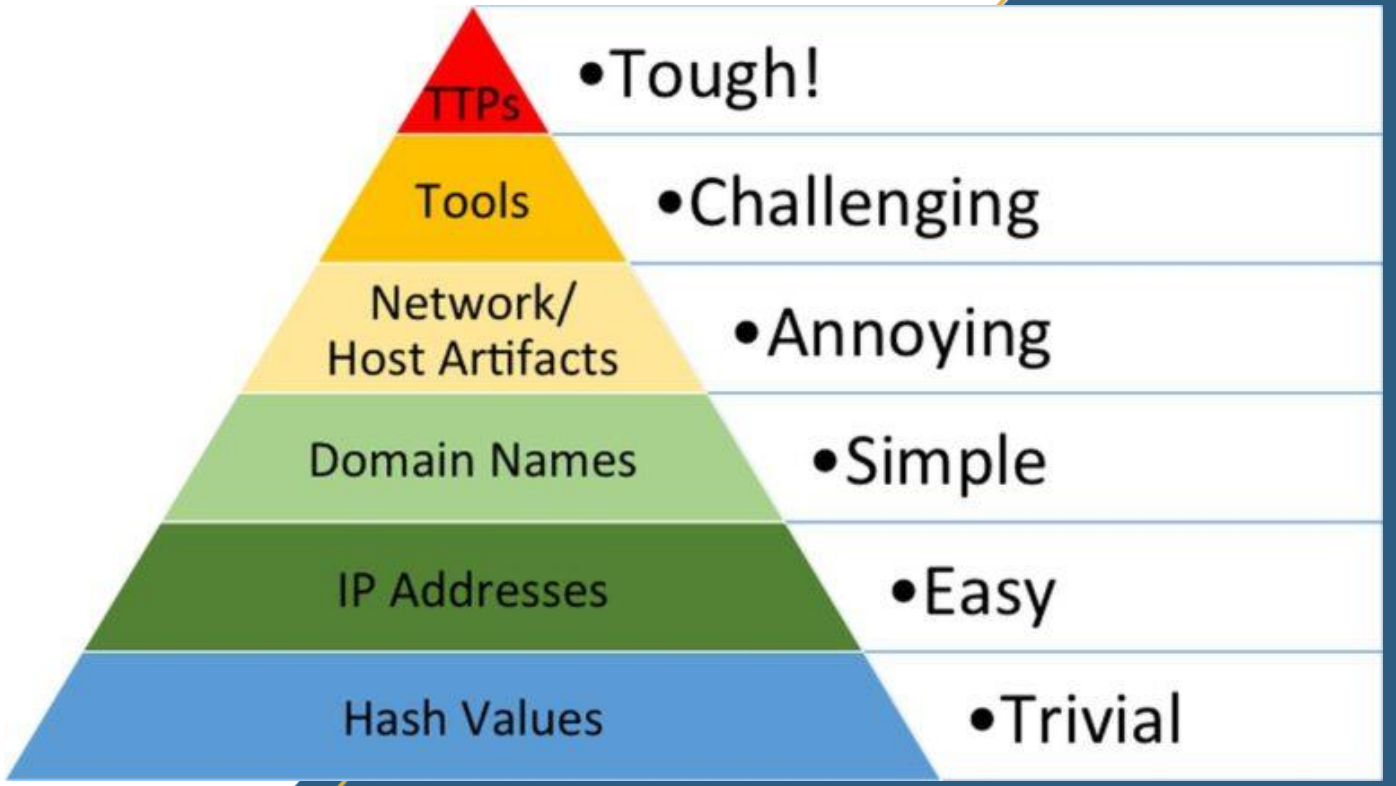
Comment commencer une activité de CTI

- Rédiger un profile de votre organisation
  - Identification de vos joyaux de la couronne « Actif critique et essentiel pour l'entreprise ».
  - Identifié les vecteurs d'attaques de l'entreprises.
- Identifier des « threats actors » selon les priorités d'intelligence établit.
- Collecter des renseignements avec un niveau de confiance acceptable.
- Analyser et documenter vos informations
- Rédiger de l'intelligence actionnable
  - Tendances des menaces, nouvelle technique à détecter, indicateur de compromission à ingéré.



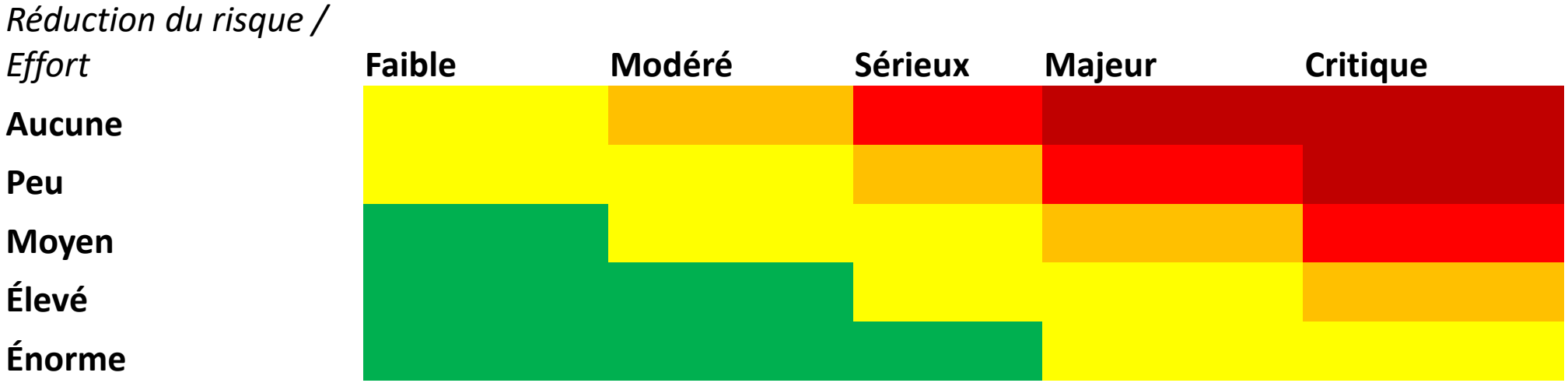
Introduction TTP et « pyramid of pain » - ML

- ❑ Introduction au Mitre
- ❑ TTP, Tactique, Technique et procédure.



Processus - ML

Intelligence → SOC Assessment → Gap analysis → Red Team → Priorisation → Remédiation



Communiquer le CTI aux Cadres - ML

Stratégies et conseils pour communiquer efficacement avec les cadres exécutifs.

- ❑ Connaître son audience.
- ❑ Mettre de l'avant les résultats et non l'analyse !
- ❑ Mesurer les impacts sur les décisions, et non le contenu des rapports.
- ❑ Rapporter sur une base régulière.

Démo

Profile de notre organisation

- Qui suis-je ? Service Conseil Juridique
- Géolocalisation : Canada
- Joyaux de la couronne: Base de données, document secret, PII.
- Vecteur d'attaque: Plateforme web, VPN

- Menace : Ransomware
- Groupe choisi : Alphv

But :
Concentrez nos efforts de détection et de contrôle sur les menaces réelles pesant sur notre entreprise.

Profile Alphv
Un groupe très actif au Canada et populaire dans le Darkweb (Gros joueur). Ce groupe est un *Ransomeware As A Service*.

Victime: Secteur de l'énergie, finance, service legal et Technologie.

Compatibilité: MAC/Windows/Linux.
Années d'expérience : Novembre 2021 et considéré un des plus gros groupes de ransomware en 2023.

Alias : Alphv, Blackcat, Noberus, AlphaVM, and AphaV

Motivation: Monétaire
Collaboration: DarkSide
Origine: Russe

Exercice pratique

Contexte

Vous travaillez pour le système de la santé du Québec. Votre Directeur sécurité est inquiet de l'incident de sécurité de OIIQ. Il vous demande donc d'investiguer sur l'auteur du groupe.

1. *Effectuer le profil sur votre organisation*
2. *Effectuer le profil sur le groupe en question: MEDUSA*
3. *Effectuer le « Threat mapping » du groupe MEDUSA sur MITRE ATT&CK*
4. *Effectuer un « Heatmap » entre le « SOC assessment » et le « Threat Mapping »*

Période de questions !!

Références

Podcast

https://darknetdiaries.com/
https://therecord.media/podcast
https://www.modemmischief.com/

News Blog

OSINTer - Your feeds
Dark Reading | Security | Protect The Business
Threat intelligence | Microsoft Security Blog

Plateforme d'échange

IBM X-Force Exchange
Dashboard - AlienVault - Open Threat Exchange
ThreatQ | Overview

Malware

Malpedia - for research
CrackedCantil: Malware Work Together
https://www.misp-project.org/

Livres

Operationalizing Threat Intelligence
Visual Threat Intelligence
Mastering Cyber Intelligence