Threat Hunting

Amelio Calcara – Etudiant en Consultance en Cybersécurité orientée SecOps
Technobel 2024-2025

Bonjour!

Agenda

01. Introduction

02. Principe

03. Déroulement d'une chasse

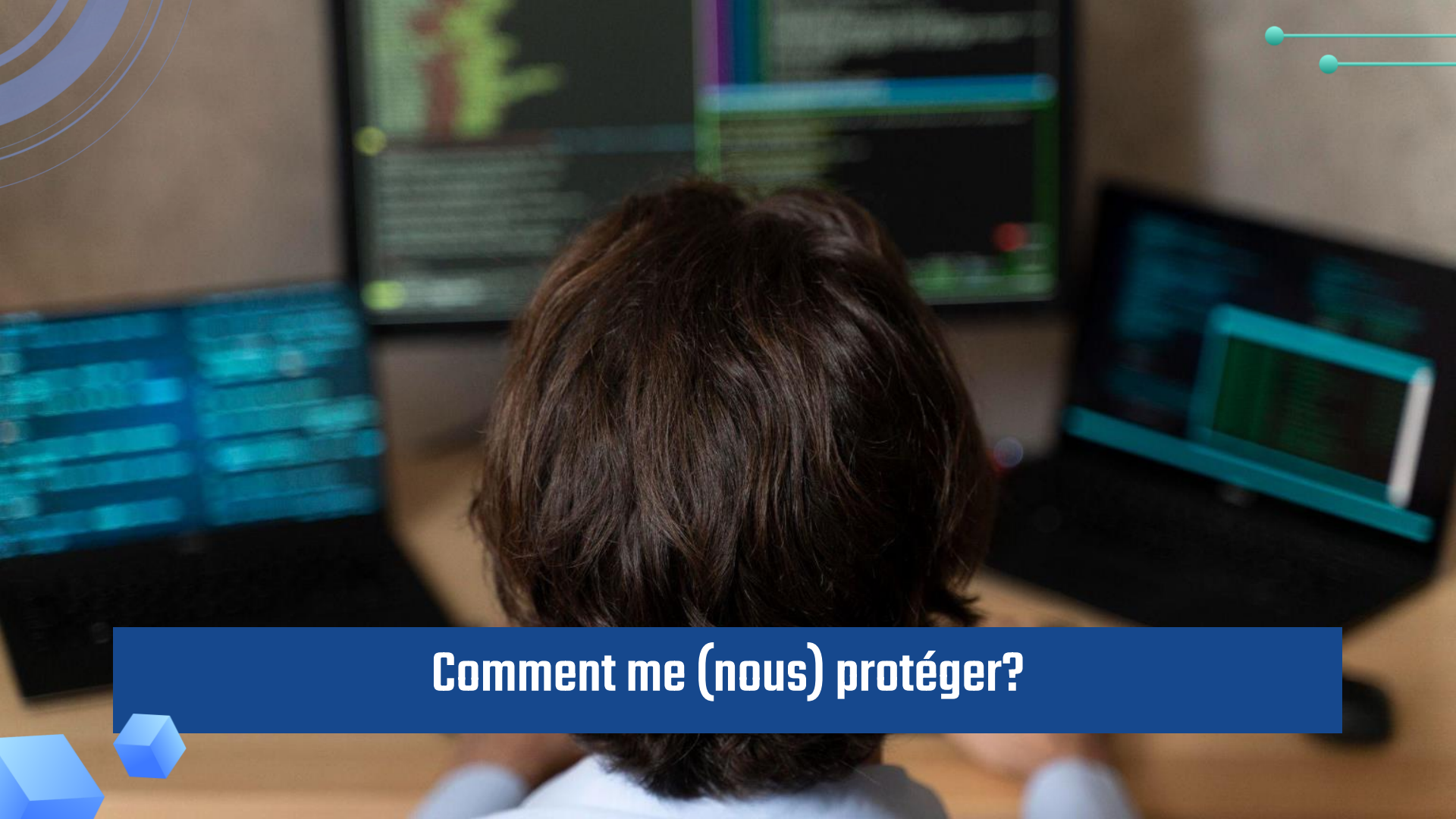
04. Outils

05. Démonstration

06. Conclusion

01.

Introduction



Comment me (nous) protéger?

Les Particuliers

Les solutions de sécurité pour les utilisateurs réguliers, à leur domicile ou ailleurs opteront pour des options **peu coûteuses, accessibles et surtout pertinentes en connaissance des risques et du volume de l'infrastructure :**

- Anti-virus
- Mots de passe robustes
- Prudence envers les techniques de Phishing, cheval de troie ou autre malware

Cohérence dans les ressources investies au profit de la sécurité

Security Operations Center

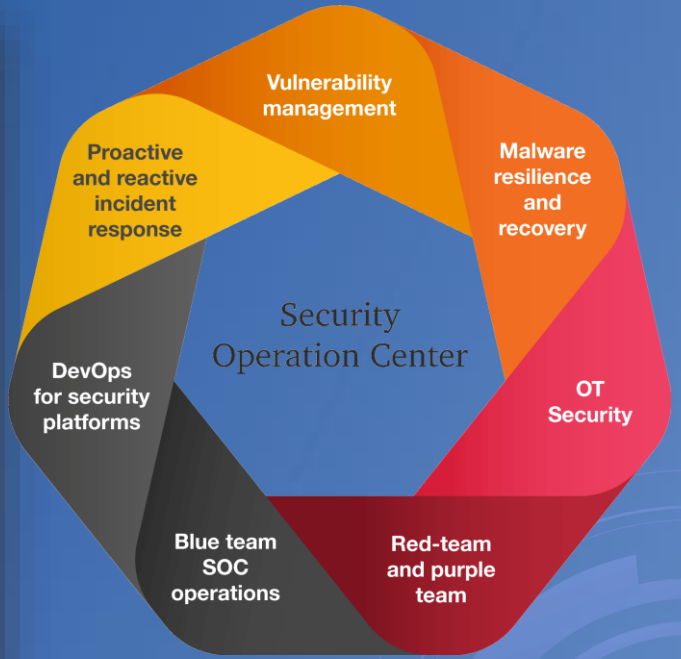
Le **Security Operations center**, **SOC**, désigne dans une entreprise l'équipe en charge d'assurer la sécurité de l'information.
Le SOC est une plateforme permettant la supervision et l'administration de la sécurité du système d'information au travers d'outils de collecte, de corrélation d'événements et d'intervention à distance.

Quel est le rôle d'un SOC?

- ❑ La surveillance proactive
- ❑ Gestion du trafic
- ❑ Analyse approfondie des données des journaux de sécurité provenant de diverses sources
- ❑ Application des politiques et procédures de sécurité
- ❑ Une expertise sur tous les outils de l'organisation
- ❑ Gestion des correctifs et MàJ
- ❑ Etc...

Equipe SOC


Cyber Writes
Roles in Security Operations Center
SOC Manager
Compliance Analyst
Security Analyst
Forensic Analyst
Responsible for the management and monitoring of an organisation's cybersecurity operations
Incident Responder
Vulnerability Analyst
Threat Hunter


Vulnerability management
Malware resilience and recovery
Proactive and reactive incident response
Security Operation Center
DevOps for security platforms
OT Security
Blue team SOC operations
Red-team and purple team

2,365

Nombre de cyberattaques en 2023

72%

Augmentation des fuites de données en 2023

4,880,000$

Coût **moyen** d'une fuite de données en 2023

Source: www.forbes.com

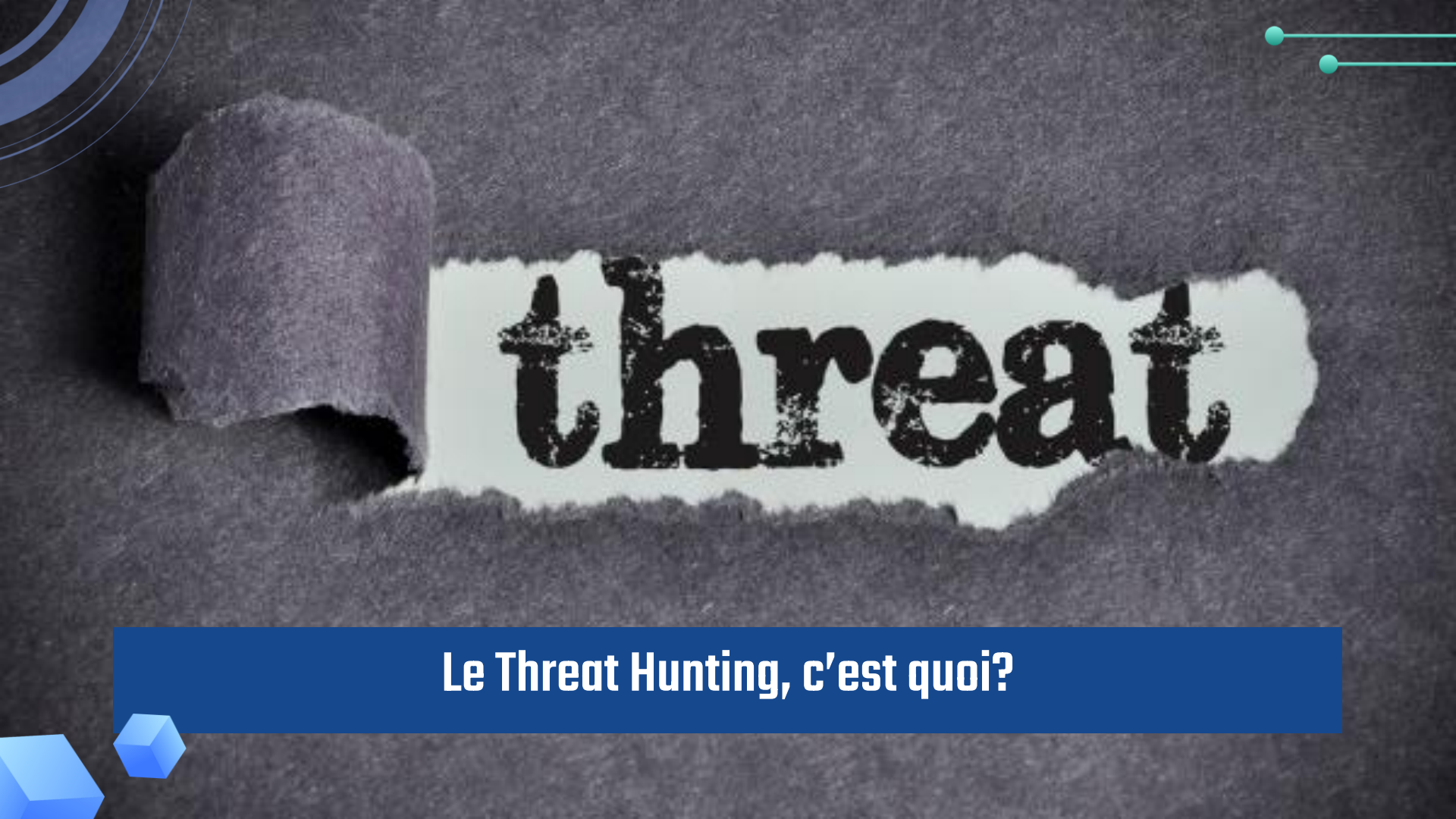
287 JOURS

Période **moyenne** pour identifier et contenir une fuite de données, soit **9,4** mois.

Source: www.forbes.com

02.

Principe



Le Threat Hunting, c'est quoi?

Qu'est ce que le Threat Hunting?

88% des causes de fuites de données sont dues à des erreurs humaines

80% alertes automatiques

Détectés par des SIEM, EDR,...

20% aucune alerte

Intervention humaine requise

Objectifs, rôles

Recherche proactive de menaces et vulnérabilités internes

Le Threat hunting consiste à anticiper les menaces et les vulnérabilités potentiellement déjà présentes au sein de l'organisation.

Etablir une Baseline du comportement normal de l'infrastructure

Avant même de commencer une chasse, le Threat hunting se base surtout ce qui doit être normalisé dans l'infrastructure parmi une quantité importante de données.

Analyse de données récoltées sur base d'hypothèses fondées

Emettre des hypothèses cohérentes en s'appuyant sur des données est l'un des piliers majeurs d'une chasse réussie. Bon nombres d'hypothèses n'aboutissent pas à une menace ou une vulnérabilité, ce qui rend les chasses potentiellement longues et surtout rapidement onéreuses.

03.

Déroulement d'une chasse

Eligibilité

Le Threat Hunting Maturity Model (THMM)

HMM0 (Initial)

- ❑ Alertes uniquement automatisées
- ❑ Collecte minime de données

HMM1 (Minimal)

- ❑ Intègre de la Threat Intelligence
- ❑ Collecte de données modérée

HMM2 (Procedural)

- ❑ Utilisation d'analyses de données créées en externe
- ❑ Collecte de données haute

HMM3 (Innovative)

- ❑ Utilisation de ses propres procedures d'analyse de données
- ❑ Collecte de données de tous types à grande échelle

HMM4 (Leading)

- ❑ La plupart des procedures sont automatisées
- ❑ Collecte de données à grande échelle et variée

Plan de stratégie

Chercher une menace dans un réseau, c’est comme chercher une aiguille dans une botte de foin finalement...

La routine d'une chasse: La Threat Hunting Loop

Threat Hunting Maturity Model Cycle

HUNTING MATURITY LEVEL

HUNTING LOOP STEPS

	HM0 Initial	HM1 Minimal	HM2 Procedural	HM3 Innovative	HM4 Leading
DATA COLLECTION	Little or no data collection	Moderate collection of some types of data from a few key points in the IT environment	High collection of certain types of data throughout the IT environment	High collection of certain types of data throughout the IT environment	High collection of many types of data throughout the IT environment
HYPOTHESIS CREATION	Respond to existing automated alerts from SIEM, IDS, Firewall, etc.	Review threat intelligence to develop new hypotheses	Review threat intelligence and "friendly intelligence" to develop new hypotheses	Review threat intelligence, "friendly intelligence", and manual cyber risk scoring (i.e. "crown jewel analysis") to develop new hypotheses	Review threat intelligence, "friendly intelligence", and automated cyber risk scoring to develop new hypotheses
TOOLS & TECHNIQUES FOR HYPOTHESIS TESTING	Alert consoles, SIEM searches; No proactive investigation	Utilize SIEM or log analysis tools to conduct basic search via full-text or SQL-like queries	Utilize simple tools and histograms to search and analyze data based on existing hunting procedures	Leverage visualizations and graph searches. Develop new hunting procedures	Advanced visualizations and graph searches. Publish, and automate new hunting procedures
PATTERN & TTP DETECTION	None; Only SIEM/ IDS alerts	Identifying IOCs at bottom of PoP like domains, URLs, and hashes	Identification of IOCs at bottom and middle of PoP and mapping trends of those IOCs over time	Able to detect adversary TTPs and other IoCs at the top of the PoP	Automatic complex TTP discovery and campaign tracking; Active sharing of IoCs with information sharing organization
ANALYTICS AUTOMATION	None	Integrates threat intel feeds into automated alerting for basic matching	Build a library of effective hunting procedures and performs them on a regular schedule	Build a library of effective hunting procedures and performs them frequently; basic data science (standard deviation, outlier detection)	Automate effective hunting procedures to continuously improve alerting capabilities; advanced data science (machine learning)

Threat Intelligence

Stratégique

Concerne des informations de haut niveau sur les tendances et les menaces globales. Elle aide à la prise de décision stratégique, souvent destinée aux dirigeants.

Opérationnel

Se concentre sur des menaces spécifiques et des incidents en cours. Elle inclut des informations sur les attaquants, leurs motivations et les vulnérabilités ciblées.

Technique

Fournit des informations sur les techniques, tactiques et procédures (TTP) utilisées par les attaquants. Cela aide les équipes de sécurité à comprendre comment les menaces opèrent.

Tactique

Fournit des informations sur les techniques, tactiques et procédures (TTP) utilisées par les attaquants. Cela aide les équipes de sécurité à comprendre comment les menaces opèrent.

04.

Outils

Analyse réseau

Analyseurs de paquets

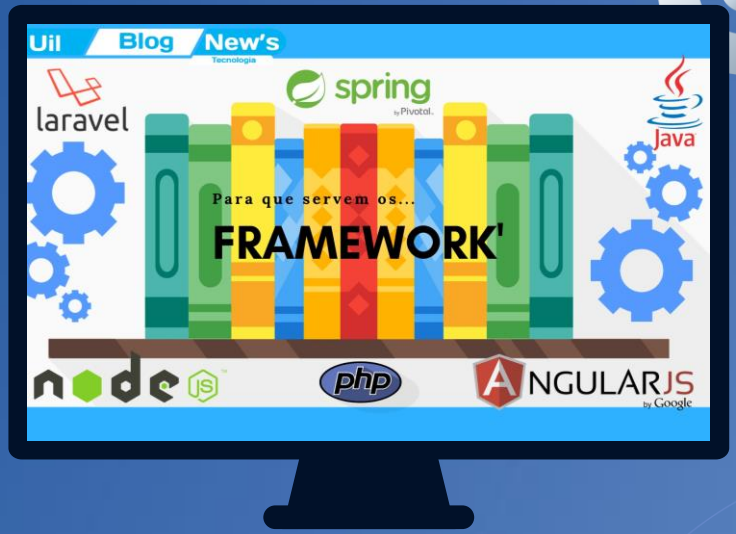
Wireshark

Tcpdump

Ingiénerie Sociale et collecte d'informations

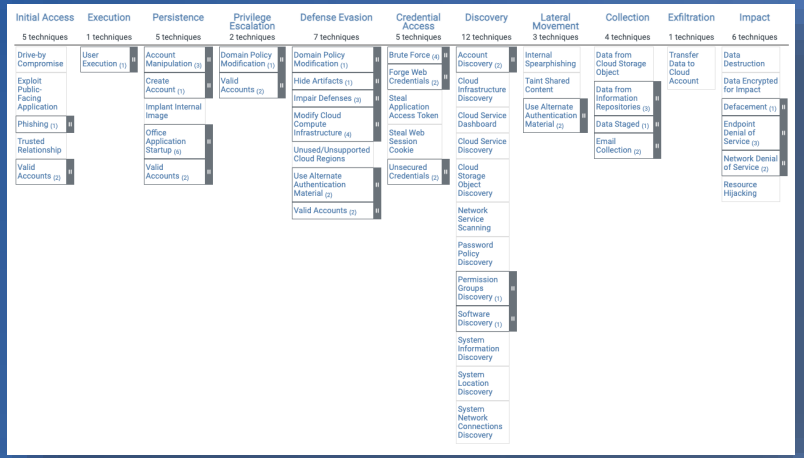
- Investigation sur des potentielles menaces **intérieures**
- Recherche de **correlations** entre les logs d'évènements et les utilisateurs
- Etablir des **baselines** sur lesquelles s'appuyer durant les futures investigations

Frameworks

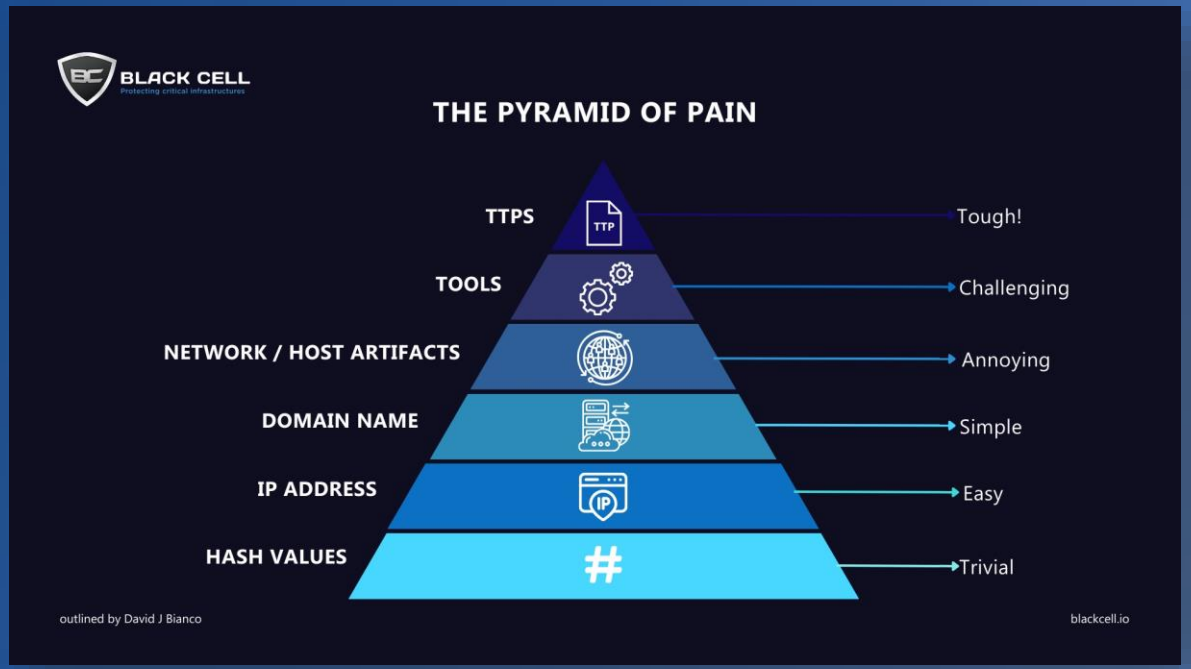

Uil
Blog
New's
Tecnologia
spring
by Pivotal
laravel
Java
Para que servem os...
FRAMEWORK'
node
php
ANGULARJS
by Google

Mitre Att&ck

MITRE | ATT&CK™



“La pyramide de la douleur”



TTP
Tactics
Techniques
Procedures

Les SIEM

SIEM

Splunk

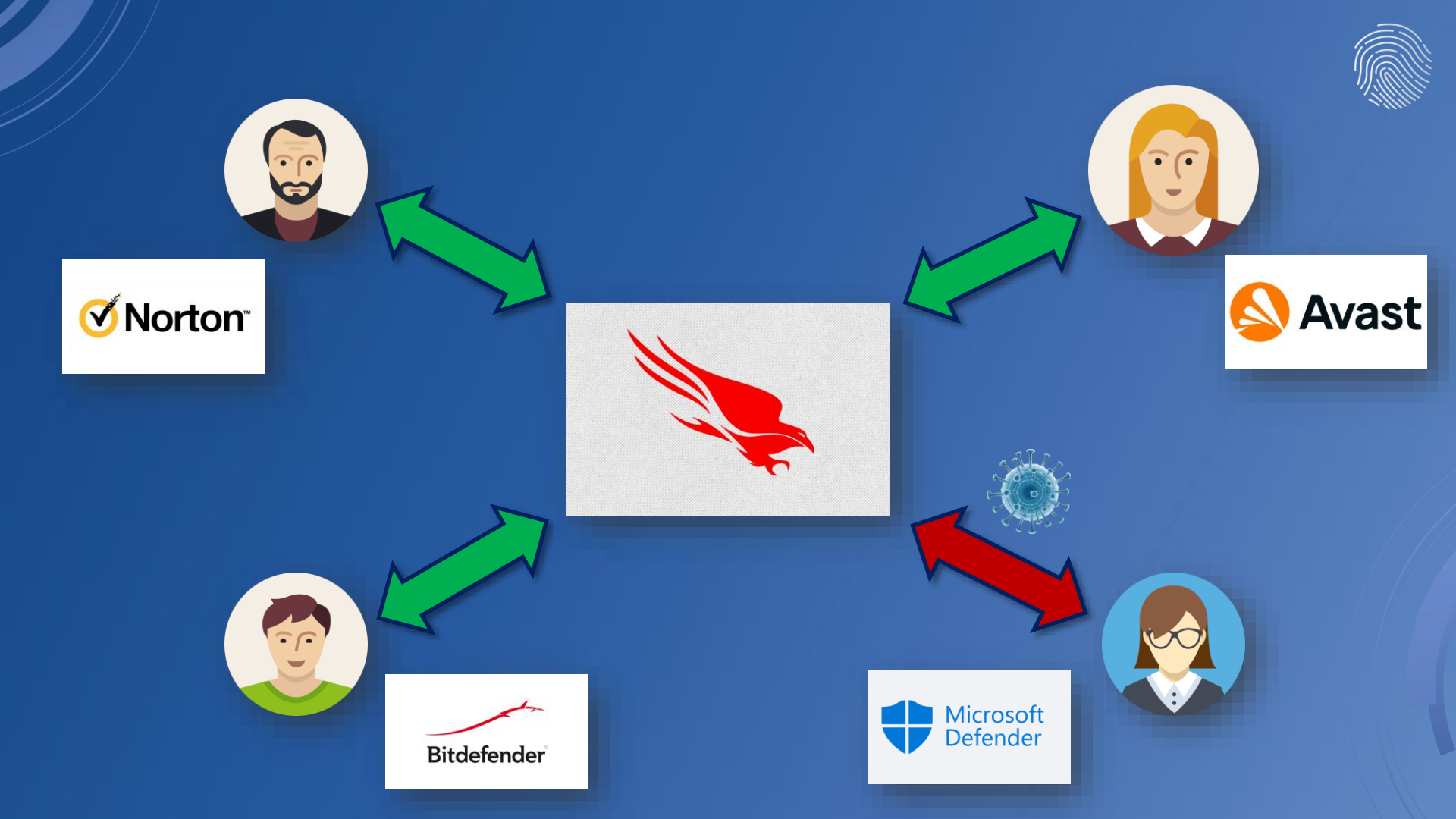
Solarwinds

Elastic Security

IBM Qradar

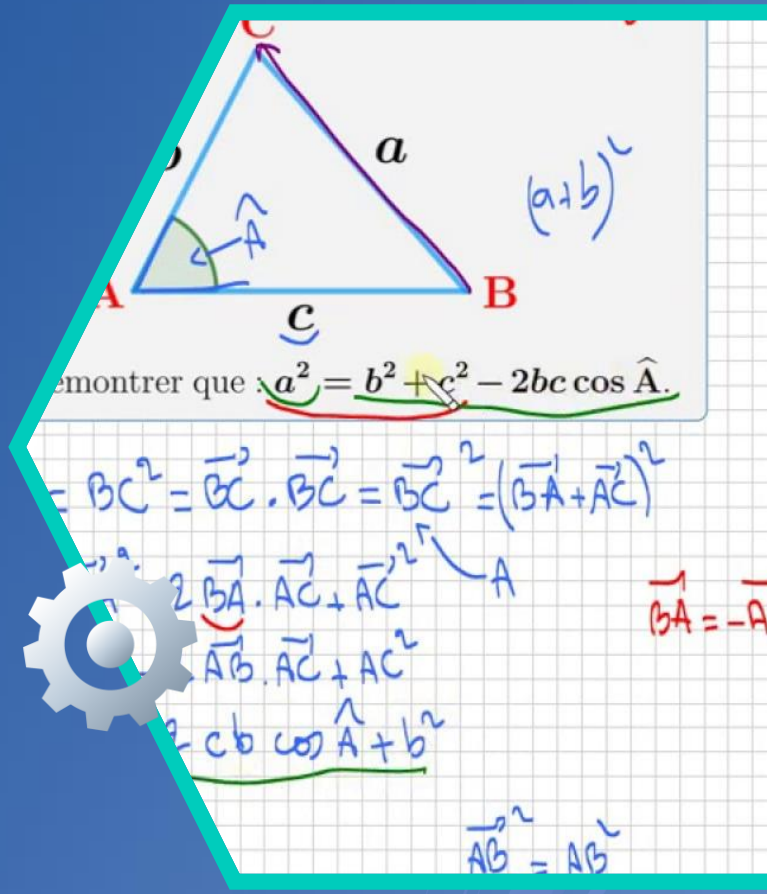
Modules orientés Threat Hunting

Endpoint detection and response (EDR) et Managed detection and response (MDR)


Norton
Avast
Bitdefender
Microsoft Defender

05.

Démonstration



06.

Conclusion

Qu'est ce qui fait d'un chasseur, un **bon** chasseur?

01. Social Engineering

02. Outils SIEM

03. Threat Intelligence

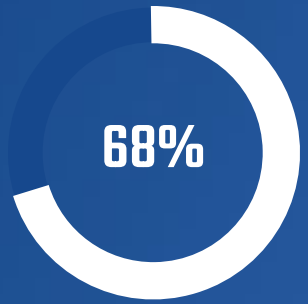
04. EDR, MDR et XDR

05. Analyses, Threat hunting frameworks

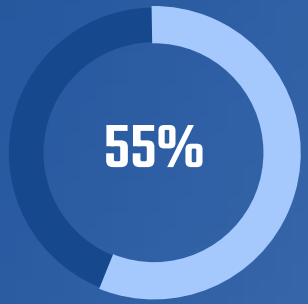
Il n'y a pas de recettes miracles dans le threat hunting, les recherches ne seront jamais suffisantes.

Le Threat Hunter est curieux, ne cesse d'étendre son panel d'outils et de recherches d'informations, il innove dans ses investigations et surtout adopte une approche proactive, avec pour objectifs de prévenir les éventuelles attaques et réduire leurs impacts

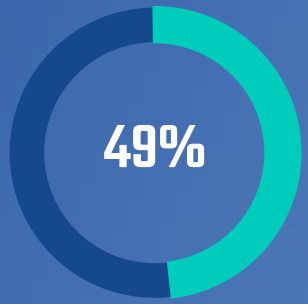
Impact du Threat Hunting



Capacité de détection aux menaces avancées



Réduction du temps d'investigation



Découverte de menaces indétectables sans le threat hunting

Source: Threat Hunting report 2021 (Cybersecurity insiders)

SANS INSTITUTE

Resources

https://www.oracle.com/fr/cloud/soc-security-operations-center/
https://www.cyberuniversity.com/post/security-operations-center-ou-soc-definition-roles-enjeux
https://www.ibm.com/topics/edr
https://www.threathunting.net/files/framework-for-threat-hunting-whitepaper.pdf
https://attack.mitre.org/
http://detect-respond.blogspot.com/2015/10/a-simple-hunting-maturity-model.html
https://www.youtube.com/@BlackPerl
Course Catalog | Splunk
https://www.youtube.com/@Huntress
https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/
https://www.sans.org/emea/

Merci de m’avoir écouté!