VEILLE TECHNOLOGIQUE

Thème :

Surveillance des risques et menaces en cybersécurité (incidents de sécurité, vulnérabilités CVE, outils et techniques employées).

Adem RABII

BTS SIO

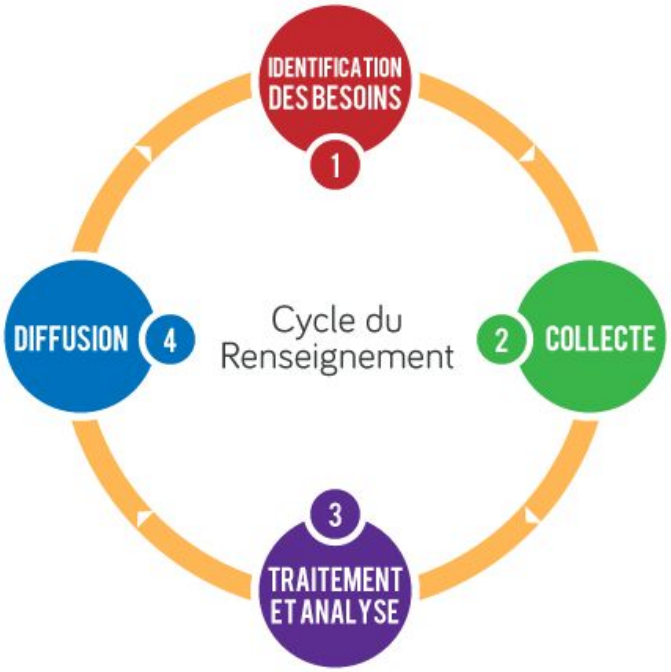
Sommaire

I. Introduction

Chaque professionnel de la cybersécurité octroie une part importante dans la veille.

Elle permet de surveiller en permanence les potentielles menaces qui visent les systèmes d'information. Ce processus doit être continu et cyclique

Il se compose de quatre grandes étapes : l'identification des besoins , la collecte , le traitement et l'analyse et la diffusion de l'information.



Ce processus est unique en cybersécurité en raison de l'immense volume d'informations à traiter et de la vitesse à laquelle les technologies et les menaces évoluent.

La veille doit ainsi être proactive et constamment mise à jour pour assurer une protection efficace des systèmes d'information.

II. Les différents objectifs de la veille en cybersécurité

Les objectifs opérationnels permettent d'identifier des comportements anormaux , détecter des incidents de sécurité et de réagir rapidement aux vulnérabilités exploitées.

Les objectifs tactiques collectent des informations pour identifier les risques cyber, améliorent la compréhension des modes opératoires des attaquants et ajustent les mécanismes de défense.

Les objectifs stratégiques analysent les motivations des attaquants et les tendances émergentes, évaluent les risques et l'impact géopolitique.

Besoins opérationnel, tactique et stratégique

source : OpenClassrooms

III. Les axes de ma veille

Ma veille en cybersécurité est axée sur l'identification des menaces et des risques, avec des objectifs à la fois opérationnels et tactiques.

Concrètement, cela inclut la surveillance des bulletins de vulnérabilités (CVE) et de l'évolution des menaces, telles que les malwares, les cyberattaques et les fuites de données. Je porterai également mon attention sur les outils et techniques utilisés, comme l'ingénierie sociale et l'OSINT, ainsi que sur les méthodes des attaquants, en explorant **leurs outils**, logiciels et environnements de hacking.

1. Les objectifs opérationnels

- Le CTI (Cyber Threat Intelligence), ou renseignement sur les menaces cyber, est une approche qui consiste à collecter, analyser et exploiter des informations sur les menaces. Le **CTI opérationnel** surveille les IOC ,indicateur de compromission, qui sont les traces laissées par une cyberattaque. Ce sont des signaux techniques qui permettent de détecter une toute activité malveillante sur un système (adresses ip suspectes , signatures de malwares , comportement anormaux).
- Surveiller les fuites de données , cela permet de détecter si des informations sensibles ont été compromises et de mieux comprendre les tactiques des attaquants. Grâce à ce travail nous pouvons agir rapidement lorsqu'une fuite de donnée est identifiée avant qu'elle ne soit exploitée .
- Surveiller les vulnérabilités et correctifs , en restant à jour sur les derniers bulletins CVE (identifiant unique donné à une vulnérabilité) on minimise le risque d'attaque en corrigeant rapidement failles critiques (ex : 0 day)

2. Les objectifs tactiques

- Tendances relatives aux risques et menaces cyber : En comprenant les tendances émergentes, nous pouvons anticiper les types d'attaques qui pourraient viser une organisation et prendre des mesures préventives. Par exemple, nous pouvons adapter les systèmes de défense en apprenant qu'un groupe d'attaquants a étendu son champ d'action et cible désormais un nouveau système d'exploitation (OS) qui nous concerne directement.

- Techniques d’attaque adoptées par les acteurs de la menace : En analysant les méthodes utilisées par les attaquants, nous pouvons mieux comprendre leurs intentions et les contrer efficacement.
- L’arsenal des attaquants : En identifiant et en surveillant les éléments clés dans l’arsenal des attaquants (tels que les outils et les logiciels malveillants), nous pouvons perturber leurs opérations et mieux nous défendre.

IV. Sources d’informations en cybersécurité

En cybersécurité, il est essentiel de s'appuyer sur des sources d'information fiables et actualisées pour rester au fait des dernières menaces et des meilleures pratiques. Voici quelques catégories de sources d'information utiles pour effectuer une veille efficace :

• **Agences spécialisées** (nationales, régionales et internationales) - l’ANSSI en France, l’ENISA en Europe, Europol (EC3), Interpol, la CISA aux Etats-Unis, le Centre de la cybersécurité au Canada

• Les **équipes de réponse aux incidents** - CERTs, CSIRTs, InterCERT France - qui publient des avis, des alertes et des recommandations pour faire face aux vulnérabilités et aux menaces.

• **Sources communautaires** et réseaux professionnels

- CESIN, CLUSIF, Cigref, CDSE
- Osint-FR, M82 Project, etc

• **Feeds communautaires** - MalwareBazaar, Tria.ge, MWDB, Feodo Tracker, URLhaus, Red Flag Domains, ThreatFox, PhishTank, VirusTotal, etc.

• **L’OSINT** (Open Source Intelligence), le HUMINT (Human Intelligence)

• **Editeurs** de cybersécurité

• Publications universitaires et de recherche

• **Médias spécialisés**

• Réseaux sociaux - X (anciennement Twitter), Bluesky, Telegram, LinkedIN, Mastodon, Discord, etc.

1. Qualifiez les sources d’informations

Dans la cybersécurité, la qualité des informations collectées est essentielle pour prendre des décisions éclairées et maintenir un environnement numérique sécurisé :

“The Admiralty Code” (également appelé “The Admiralty Scale” ou “The NATO System”) pour classifier les sources et les informations en fonction des critères de fiabilité et de crédibilité.

Fiabilité des sources	Crédibilité de l’information
A - Source entièrement fiable	A - Information entièrement vraie
B - Source a priori fiable	B - Information crédible
C - Source plutôt fiable	C - Information possiblement vraie
D - Source a priori pas fiable	D - Information douteuse
E - Source pas fiable	E - Information peu probable
F - La fiabilité n’est pas garantie	

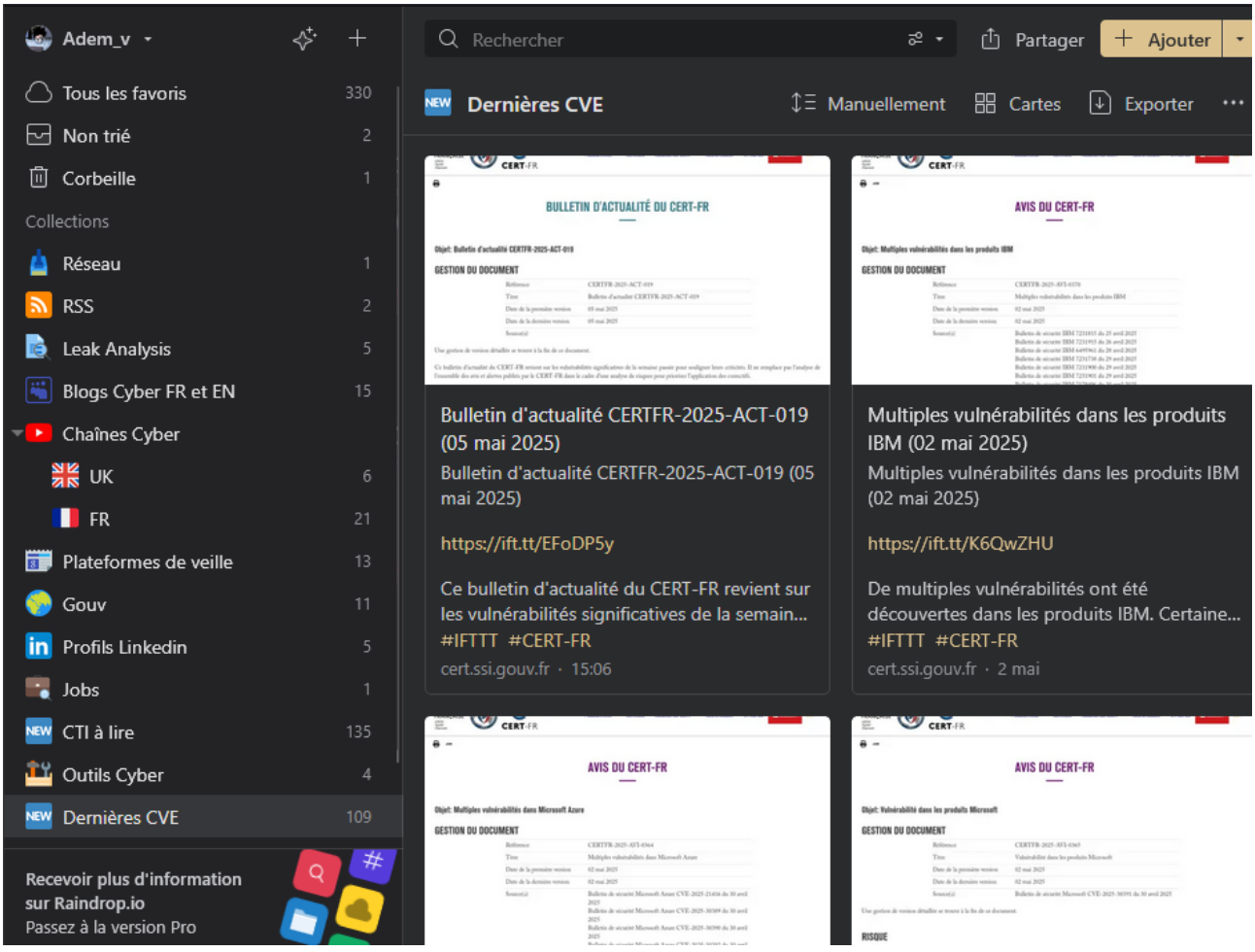
V. Les outils de ma veille

1. Les Gestionnaires de Favoris (ou signets)

Ce sont des outils pratiques pour organiser et stocker des URL, des pages web ou des documents que l'on souhaite consulter ou utiliser plus tard. Ils permettent de regrouper, trier et partager des liens vers des ressources utiles. On peut également les utiliser pour créer des collections de favoris sur des sujets spécifiques.

Raindrop et Zotero sont des exemples de gestionnaires de favoris que l'on peut intégrer à notre processus de veille.

Nous pouvons également utiliser ces gestionnaires de favoris pour enregistrer des liens vers des articles de recherche, des blogs et des outils de sécurité afin de garder une trace organisée de nos références en ligne. Nous pouvons organiser nos favoris par catégories, ce qui nous permet de retrouver rapidement les informations dont nous avons besoin pour notre veille ou nos travaux de recherche. Si nous faisons de la recherche en cybersécurité, cela peut être très utile également.



2. Les agrégateurs de flux RSS

Ce sont des outils essentiels pour centraliser et automatiser la collecte d'informations dans le cadre de notre veille en cybersécurité.

Ils permettent de suivre les mises à jour des sites web et des sources d'information que nous jugeons importantes. Ces outils facilitent également la veille collaborative, car nous pouvons partager les flux avec notre équipe ou d'autres utilisateurs.

Par exemple, si nous travaillons dans une équipe de réponse aux incidents, nous pouvons utiliser un agrégateur de flux RSS pour suivre les dernières vulnérabilités, les alertes de sécurité et les avis de sécurité publiés par différentes organisations. Cela nous permet de rester à jour sur les menaces potentielles et d'agir rapidement en cas d'incident. Il existe plusieurs outils agrégateurs de flux RSS :

• **Feedly** : il permet l'intégration avec la plateforme MISP pour extraire, collecter et

contextualiser des IOCs provenant des articles publiés en sources ouvertes.

• **Start.me :** Sur Start.me, nous pouvons trouver un exemple de **dashboard** "Cyber Threat Intelligence" (créé par Rahmat Nurfauzi).

• **Inoreader**

3. Les plateformes de veille

Ces plateformes offrent souvent des fonctionnalités avancées telles que l'indexation, la catégorisation et la recherche avancée pour faciliter la récupération rapide d'informations pertinentes. Elles vont aussi proposer des critères spécifiques à la cybersécurité tels que la recherche d'informations consacrées à un groupe cybercriminel ou à une technique d'attaque spécifique, le filtrage sur une criticité donnée de vulnérabilités, etc.

- https://lejournalduhack.com/
- https://thehackernews.com/
- https://www.riskintel.fr/actualit%C3%A9s
- https://www.zataz.com/
- https://www.zdnet.fr/actualites/cybersecurite-3900046206q.htm
- https://www.nohackme.com/news.html
- https://cve.nohackme.com/

4. Les blogs

Liste de blogs de sociétés de cybersécurité (liste non exhaustive)

McAfee — https://securingtomorrow.mcafee.com/

Kaspersky Labs — https://securelist.com/

Trend Micro — https://blog.trendmicro.com/trendlabs-security-intelligence/

FireEye — https://www.fireeye.com/blog/threat-research.html

CrowdStrike — https://www.crowdstrike.com/blog/

Dragos — https://dragos.com/blog/

ESET — https://www.welivesecurity.com/

Blogs spécialisés :

Krebs on Security — https://krebsonsecurity.com

Errata Security — https://blog.erratasec.com/

Sites spécialisées anglo-saxons :

(Les médias français ont souvent un jour voire plus de retard par rapport aux anglo-saxons...)

CyberScoop — https://www.cyberscoop.com/

BleepingComputer — https://www.bleepingcomputer.com/

ZDNet — https://www.zdnet.com/

ThreatPost — https://threatpost.com/

Security Affairs — http://securityaffairs.co/wordpress/

Wired — https://www.wired.com/category/security/

5. Les outils d’alerte

Pour une veille en quasi temps réel sur un sujet d’intérêt, nous pouvons exploiter les fonctionnalités d'outils d'alerte comme Google Alerts, que j’utilise personnellement, car il est très facile et rapide à configurer. Cet outil permet de recevoir des notifications chaque fois qu'un mot-clé prédéfini est mentionné dans des sources ouvertes sur Internet.

Nous pouvons utiliser des mots-clés tels que :

vulnérabilités, exploit zero-day, menaces cyber, attaque par ransomware, phishing, vol de données,malware, analyse de sécurité, analyse de malware, patch de sécurité, CVE, alertes de sécurité,incidents de sécurité, cyberattaque, sécurité réseau, sécurité des applications, sécurité des systèmes, risques cyber, bonnes pratiques en cybersécurité, conseils en cybersécurité.

6. Les scripts

Cet outil est précieux pour collecter des données grâce à sa capacité à automatiser des tâches et àintégrer divers services en ligne. Il nous permet de surveiller des sources spécifiques d'informations sur la cybersécurité.Par exemple, nous pouvons créer un applet (une petite application ou un script automatisé) quidéclenche une action chaque fois qu'un mot-clé spécifique lié à la cybersécurité est mentionné sur des plateformes comme Twitter. L'action pourrait consister à envoyer ces informations directement dans notre Raindrop, un outil de gestion de données,

De cette manière, IFTTT peut servir de pont entre diverses sources d'information et nos systèmes

de surveillance, facilitant ainsi la collecte automatisée de données pertinentes en temps réel.