Routine de Veille Cyber
BTS SIO – 1ère année

THEPOT Quentin

Réalisé le 24 nov. 2025

Sommaire

1. Introduction

En tant qu'étudiant en BTS SIO 1ère année, il est essentiel d'apprendre à suivre l'évolution constante des menaces cyber. Même si je ne pratique pas encore de veille régulière, j'ai une sensibilité naturelle pour la sécurité personnelle, la discrétion en ligne et les fuites de données, notamment lorsque de grandes entreprises comme Bouygues subissent des attaques.

2. Objectifs de la veille cyber

- Développer une culture générale en cybersécurité.
- Suivre les vulnérabilités et incidents majeurs.
- Se tenir informé des nouveautés touchant l'administration réseau et système (SISR).
- Protéger mon identité numérique (fuites de données, comptes piratés…).
- S'inspirer du monde professionnel (CERT, ANSSI, chercheurs en sécurité).

3. Routine Matinale de Veille Cyber

3.1. Vérification rapide des alertes

Cette étape repose sur des outils capables d'envoyer des notifications automatiques, ce qui permet de faire une veille même sans y penser.

- HaveIBeenPwned Alerts : notifications email en cas de fuite de données contenant mon adresse email.
- Google Alerts : envoi d'un mail lorsqu'un mot-clé important apparaît (exemple : "vulnérabilité Windows", "CVE critique").
- TheHackerNews – Application mobile : notifications push pour les cyberattaques majeures, mises à jour de sécurité, malwares.
- CERT-FR – Alertes RSS transformées en notifications.
- Action du matin :
    - Vérifier rapidement les mails d'alertes.
    - Consulter les notifications de l'application TheHackerNews si l'une d'elles parle d'une nouvelle attaque.
    - Regarder X (Twitter) car le réseau est souvent le premier endroit où les chercheurs publient des infos.

3.2 Lecture structurée des actualités

Même sans automatisation avancée, je consulte les sources fiables suivantes :

- TheHackerNews (site ou app).
- Reddit : r/cybersecurity / r/netsec.
- CERT-FR : Bulletins d'alerte (CVE, correctifs, attaques).
- ANSSI : Recommandations et guides.

Je me concentre surtout sur :

- les fuites de données,
- les attaques ciblant les entreprises françaises,
- les vulnérabilités critiques du jour.

3.3 Approfondissement ciblé

Si une attaque attire mon attention (ex : un ransomware visant une grande entreprise) :

1. Je cherche une analyse sur TheHackerNews ou BleepingComputer,
2. Je regarde sur GitHub pour voir si un exploit PoC est déjà publié,
3. Je vérifie les discussions techniques sur Reddit,
4. Je regarde les comptes experts sur X (CERT-EU, ANSSI, chercheurs indépendants).

3.4 Synthèse rapide

Chaque matin, je note :

→ Les CVE intéressantes,
→ Les attaques importantes du jour,
→ Les outils ou techniques observées,
→ Ce qui peut me servir dans le cadre du SISR.

4. Automatisations et outils envoyant des notifications

4.1 Flux RSS avec notifications

- Feedly, Inoreader : transforment les flux RSS du CERT-FR, ANSSI, HackerNews en alertes instantanées.

4.2 Notifications via applications

- TheHackerNews : alerts push.
- BleepingComputer app.
- Reddit : notifications pour les posts dans r/cybersecurity.
- GitHub : notifications pour les nouveaux exploits ou repositories suivis.

4.3 Notifications email

- *HaveIBeenPwned* pour fuites de données personnelles.
- Google Alerts pour mots-clés personnalisés.
- *Certains* CERTs *internationaux peuvent envoyer des newsletters.*

4.4 Alertes via réseaux sociaux

- Listes X :

1.1. Chercheurs en cybersécurité,
1.2. CERT-FR / ANSSI,
1.3. Analystes de malware.

- Discord : salons cyber qui envoient des alertes en temps réel.

5. Outils et ressources principaux

- X (Twitter) : informations en temps réel.
- Discord : communautés cyber, partage d'incidents.
- GitHub : PoC liés aux CVE du jour.
- HaveIBeenPwned : surveillance de mon identité numérique.
- Reddit : discussions techniques.
- TheHackerNews App : notifications d'articles importants.
- Feedly / Inoreader : agrégation automatique d'alertes (à mettre en place).
- MOOC ANSSI : base théorique solide.

6. Conclusion

Cette routine simple mais efficace m'aide à construire progressivement des réflexes de veille cyber, tout en restant adaptée à mon niveau de BTS SIO SISR.
Elle inclut :

- des alertes automatiques (emails + notifications),
- la consultation quotidienne de ressources fiables,
- un approfondissement selon les incidents du jour,
- une synthèse pour capitaliser mes connaissances.

Avec le temps, je pourrai automatiser plus largement cette veille, l'adapter à ma future spécialisation et utiliser des outils plus avancés (SIEM, dashboards, scripts Python pour scraper les CVE, etc.).