Veille Technologique

Veille Technologique – Cybersécurité

Introduction

Dans le cadre de ma formation en BTS SIO (Services Informatiques aux Organisations), j'ai choisi de réaliser une veille technologique sur le thème de la cybersécurité. Ce domaine est en constante évolution et représente un enjeu crucial tant pour les entreprises que pour les particuliers. La maîtrise de ces enjeux est essentielle pour tout futur professionnel de l'informatique, notamment dans les contextes de sécurisation des systèmes, d'identification des vulnérabilités ou encore de protection des données personnelles.

Pour mener cette veille, j'ai utilisé différents outils et sources fiables afin de me tenir informé des dernières actualités, innovations, menaces et bonnes pratiques liées à la cybersécurité.

Les Méthodes de Veille Technologique

La veille technologique repose sur deux grandes approches complémentaires : la méthode **Pull** (recherche active) et la méthode **Push** (réception passive). Les deux sont essentielles pour une veille efficace et exhaustive.

Méthode Pull – Veille active et ciblée

La méthode **Pull** consiste à aller chercher l'information par soi-même, en fonction de ses besoins. Elle repose sur une **démarche proactive** : l'utilisateur définit des mots-clés précis, sélectionne ses sources, puis explore activement les nouveautés dans son domaine.

Outils et supports utilisés :

- Agrégateurs de flux RSS comme **Feedly**
- Moteurs de recherche spécialisés (Google Scholar, blogs techniques…)
- Forums, communautés professionnelles (Stack Overflow, Reddit /r/netsec…)

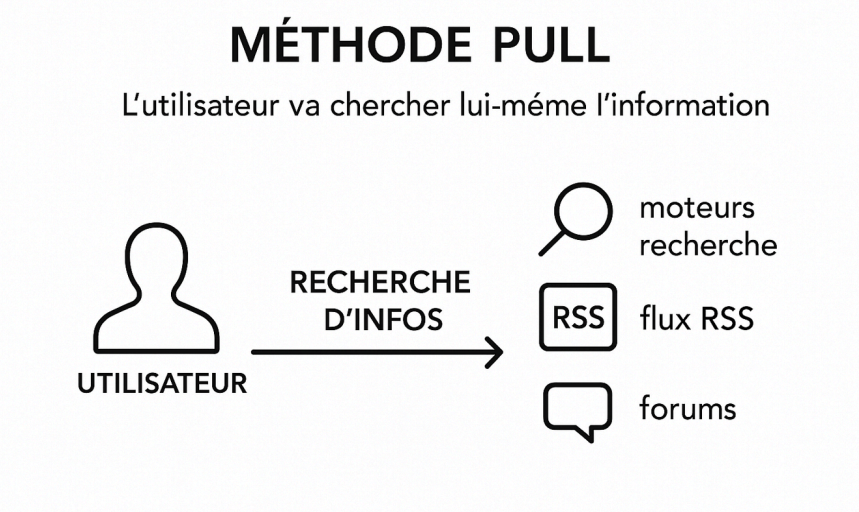
Avantages :

- Contrôle total sur les sources et sujets traités
- Adapté à des besoins ponctuels ou spécialisés
- Permet une veille très personnalisée

Limites :

- Chronophage si non organisé
- Risque de rater des informations périphériques mais importantes

Exemple concret :
Via Feedly, je suis les flux de Zataz, The Hacker News ou LeMagIT, ce qui me permet d'identifier rapidement les failles critiques et les nouveaux outils de sécurité.



Méthode Push – Veille automatisée et régulière

À l'inverse, la méthode **Push** permet de recevoir automatiquement de l'information sans recherche manuelle. Elle repose sur une logique de **diffusion planifiée** : l'utilisateur s'abonne à des flux, newsletters, ou alertes qui l'informent en temps réel.

Outils et supports utilisés :

- Newsletters de la **CNIL**, **ANSSI**, **CERT-FR**
- Alertes Google sur des mots-clés : "cyberattaque", "zero day", "RGPD"
- Chaînes YouTube, podcasts techniques, notifications Twitter/X

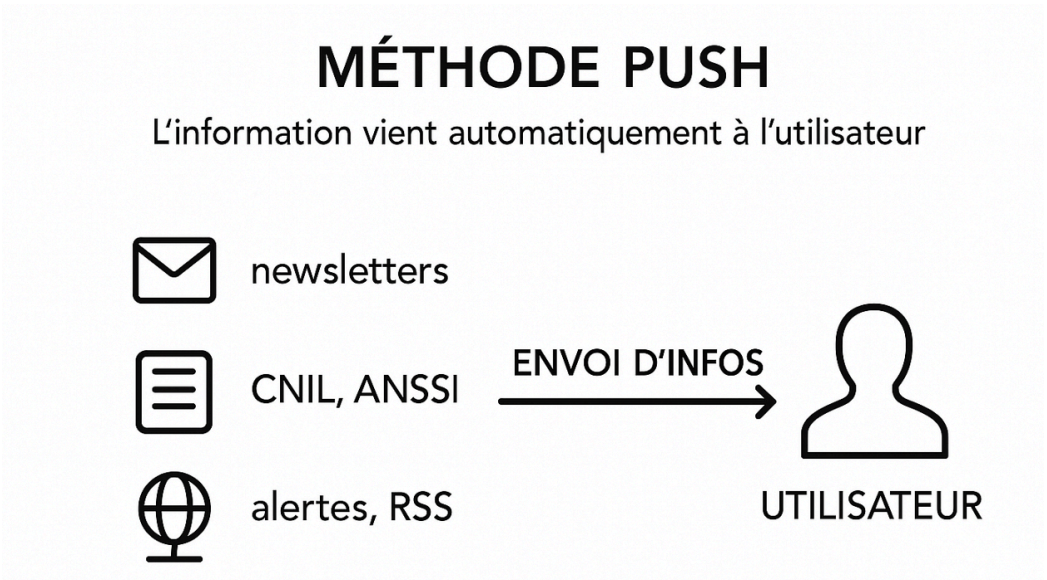
Avantages :

- Gain de temps : les informations viennent à soi
- Mise à jour continue sans effort
- Idéal pour le suivi des tendances générales

Limites :

- Moins personnalisée que la méthode Pull
- Risque de surcharge d'informations si les sources ne sont pas bien filtrées

Exemple concret :
Grâce à la newsletter de l'ANSSI, je reçois directement les alertes du **CERT-FR** sur les vulnérabilités actives et les recommandations de sécurité à suivre.



Outils utilisés pour la veille

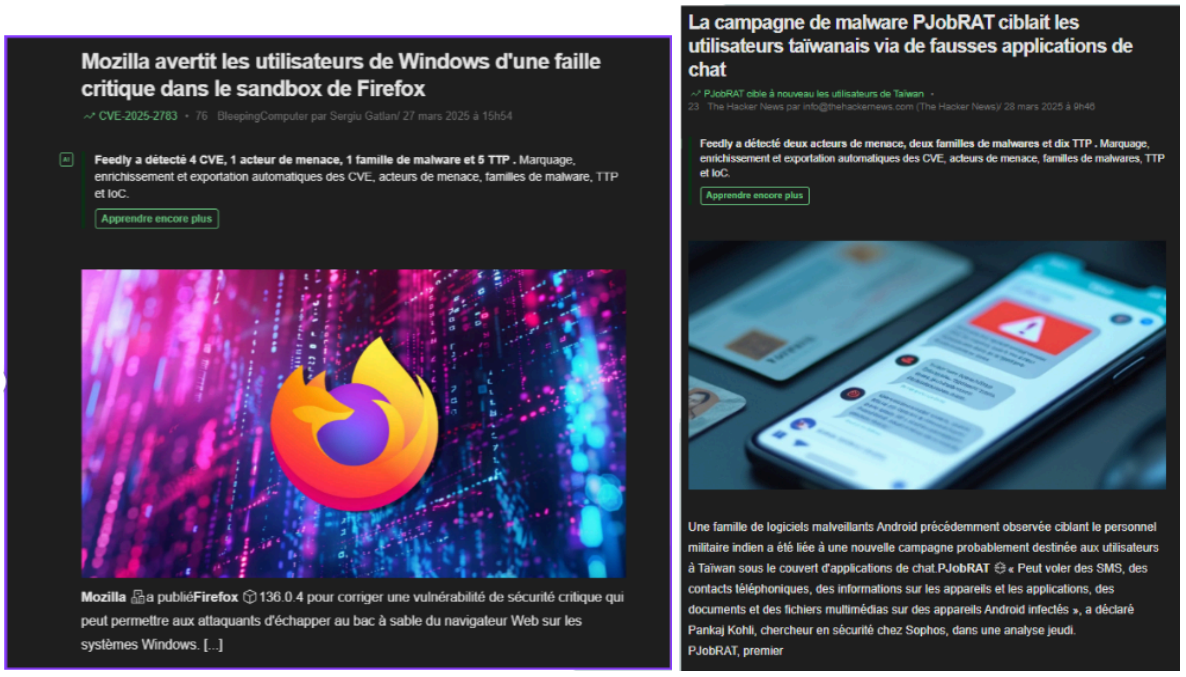
Feedly

Feedly est une plateforme d'agrégation de contenu qui permet de centraliser les flux RSS provenant de divers sites web spécialisés (blogs tech, presse numérique, chaînes YouTube, etc.). J'y ai organisé mes sources en catégories : cybersécurité, cloud, intelligence artificielle…

Avantages :

- Interface claire et personnalisable ;
- Gain de temps grâce au regroupement des actualités ;
- Ajout de sources comme Zataz, LeMagIT, The Hacker News.

Exemple :



J'utilise Feedly quotidiennement pour consulter les dernières actualités du secteur. Par exemple, j'y ai appris en mars 2025 l'existence d'une faille critique dans plusieurs VPN open-source, découverte par des chercheurs en sécurité.

X

La CNIL

La CNIL (Commission Nationale de l'Informatique et des Libertés) est une autorité administrative indépendante française chargée de la protection des données personnelles. Son site web fournit des ressources précieuses sur le RGPD, les droits des usagers, et les sanctions en cours.

Rôle dans ma veille :

- Comprendre l'aspect juridique de la cybersécurité ;
- Suivre les actualités sur les sanctions ou les failles critiques de sécurité déclarées ;
- Accéder à des guides de bonnes pratiques pour les développeurs.

L'ANSSI

L'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) est un acteur clé en France pour la cybersécurité des institutions publiques et privées.

Utilité pour ma veille :

- Guides techniques pour la sécurité des mots de passe, réseaux, télétravail… ;
- Alertes de sécurité via le CERT-FR ;
- Outils open source et supports de formation.

Je consulte régulièrement leur site pour être au fait des recommandations et bonnes pratiques.

Créateurs de contenu spécialisés

- **Micode** : vulgarisateur français reconnu dans le domaine de la cybersécurité et du hacking éthique. Ses vidéos pédagogiques m'ont permis de mieux comprendre des concepts comme le pentesting, les failles XSS ou encore les enjeux liés au darknet.
- **The Cyber Mentor** : expert anglophone du hacking éthique, ses tutoriels techniques sont très utiles pour acquérir une culture offensive de la cybersécurité. J'ai notamment découvert des outils comme Burp Suite, Metasploit ou TryHackMe grâce à ses vidéos.

Sources complémentaires et actions personnelles

Participation à une conférence sur l'intelligence artificielle

Dans le cadre de ma démarche de veille technologique, j'ai également assisté à une conférence intitulée "IA : quels impacts actuels et futurs ?", organisée par le Rotary Club d'Annecy le 1er octobre 2024.

Cette conférence m'a permis :

- D'enrichir ma compréhension des enjeux actuels et futurs de l'intelligence artificielle, notamment dans les domaines de la cybersécurité et de la protection des données ;
- De mieux cerner l'évolution des technologies d'IA dans le traitement automatisé des menaces ;
- De prendre conscience des limites éthiques et juridiques liées à l'IA dans l'univers numérique.

IT-Connect : plateforme de formation continue

En complément de mes sources d'actualités, je consulte régulièrement le site **IT-Connect.fr**, qui propose :

- Des **tutoriels techniques** (Linux, Windows, scripts, sécurité…) ;
- Des **cours détaillés** sur l'administration réseau et la cybersécurité ;
- Des **actualités et tests** d'outils utiles en entreprise.

Cette plateforme m'aide à approfondir mes compétences pratiques, notamment grâce à des **guides sur la configuration sécurisée de systèmes** ou des tests de **solutions antivirus et firewall**.

Tendances actuelles observées

Grâce à cette veille technologique continue, plusieurs tendances clés se dégagent :

- Cybersécurité et Intelligence Artificielle : l'IA est de plus en plus utilisée pour détecter les anomalies réseau, mais elle est aussi exploitée par les cybercriminels.
- Bug Bounty et hacking éthique : de plus en plus d'entreprises ont recours à des programmes de récompense pour identifier leurs failles.
- Sécurité du cloud : enjeu majeur avec la généralisation du télétravail et des services SaaS.
- Phishing et ingénierie sociale : des attaques de plus en plus ciblées nécessitent des stratégies de sensibilisation renforcées.

L'importance de la veille technologique

La veille technologique me permet d'acquérir des compétences à jour et stratégiques, essentielles dans un contexte où les menaces évoluent constamment. Elle est aussi un levier d'apprentissage autonome et continu.

Bénéfices concrets :

- Anticipation des menaces et évolutions du secteur ;
- Meilleure compréhension des enjeux juridiques et techniques ;
- Adaptation aux exigences du marché numérique ;
- Développement d'un esprit critique et d'analyse.

Cette veille s'inscrit pleinement dans le référentiel du BTS SIO, notamment sur les compétences liées à la sécurisation des infrastructures, la gestion des incidents et la mise en œuvre de solutions techniques adaptées.

Conclusion

La cybersécurité étant un domaine prioritaire dans les métiers de l'IT, cette veille m'a permis d'approfondir mes connaissances, de découvrir des outils professionnels, et d'adopter des réflexes de veille continue. C'est une démarche que je compte poursuivre dans le cadre de mes futures missions professionnelles, afin de rester constamment à la page dans un univers numérique en perpétuelle mutation.