



# BTS SIO

## BTS SERVICES INFORMATIQUES AUX ORGANISATIONS

### FICHE MÉTHODOLOGIQUE DE VEILLE TECHNOLOGIQUE

**Candidat :** Alenzo Wauters

**Spécialité :** SISR (Solutions d'infrastructure, systèmes et réseaux)

**Objectif :** Présentation des outils et processus de surveillance technologique.

---

#### SOMMAIRE

#### Table des matières

1. Introduction : La veille au service de l'expertise SISR.....	2
2. Où et comment je trouve mes informations ? .....	2
3. Comment je trie et j'analyse ce que je trouve ?.....	3
4. Ma boîte à outils : Organisation et archivage.....	3
5. Conclusion : Ma veille me fait progresser .....	3

---

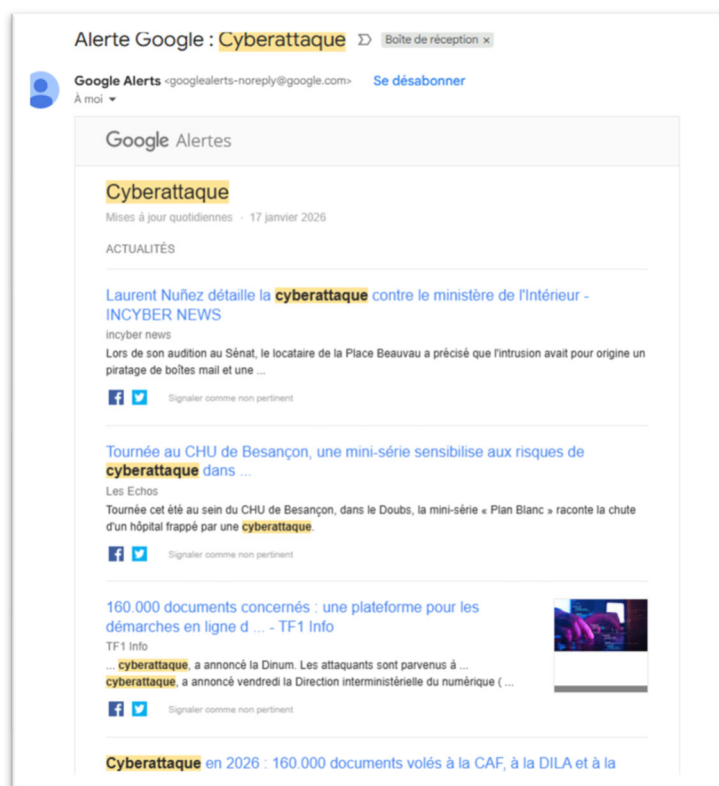
# 1. Introduction : La veille au service de l'expertise SISR

Pour un futur technicien en **cybersécurité**, rester immobile, c'est déjà prendre du retard. Dans mon parcours en **SISR**, j'ai vite compris que les cours ne suffisent pas : je dois surveiller moi-même les nouvelles failles (comme les vulnérabilités **Zero-day**) et comprendre comment les infrastructures évoluent vers le **Cloud** ou le **Zero Trust**. Cette fiche n'est pas qu'une liste de sites, c'est le mode d'emploi de ma méthode personnelle pour faire le tri dans tout ce qu'on lit sur le web et ne garder que ce qui est vraiment utile sur le terrain.

## 2. Où et comment je trouve mes informations ?

J'ai choisi de ne pas dépendre d'un seul outil, mais de croiser les sources pour garantir la fiabilité des informations.

- **Le levier LinkedIn (Veille Active)** : En suivant des experts comme **Damien Bancal (ZATAZ)** et des organismes comme l'**ANSSI**, je bénéficie d'une analyse humaine et immédiate de l'actualité.
- **Les Alertes Automatisées** : Utilisation de **Google Alerts** sur des mots-clés spécifiques ("**Architecture Zero Trust**", "**Cyberattaque**") pour ne rien manquer des publications web.
- **Les Flux Institutionnels** : Consultation directe des bulletins d'alerte du **CERT-FR** pour la partie technique et réglementaire.
- **L'ANSSI (CERT-FR)** : Ma source pour les alertes critiques et les guides officiels de sécurisation des systèmes.



### *Automatisation de la veille via Google Alerts.*

*Mise en place d'alertes automatisées sur le mot-clé 'Cyberattaque'. Ce système me permet de recevoir en temps réel les actualités critiques directement dans ma messagerie. C'est grâce à ce flux que j'ai pu identifier rapidement l'incident des Hauts-de-France, me permettant d'analyser l'impact technique et les mesures de remédiation envisageables en tant que futur administrateur SISR*

### 3. Comment je trie et j'analyse ce que je trouve ?

Récupérer des tonnes d'infos, c'est bien, mais ça ne sert à rien si on ne fait pas de tri. Pour ne pas me laisser déborder, je suis toujours ces trois étapes :

- Le tri sélectif : Je laisse de côté les articles trop "publicitaires" ou les sites qui ne citent pas leurs sources.
- La vérification (Check) : Si je vois passer une info sur un blog, je vais tout de suite voir si l'ANSSI ou le CERT-FR en parlent pour être sûr que c'est du sérieux.
- La mise en situation : C'est le plus important pour mon futur métier. Je me pose toujours la question : *"Si j'étais responsable d'un parc de 200 serveurs demain matin, est-ce que cette info changerait ma façon de travailler ?"*

### 4. Ma boîte à outils : Organisation et archivage

Pour que ma veille serve vraiment à l'examen (et après), je dois être super organisé. L'idée, c'est de retrouver n'importe quelle info en quelques secondes :

- **Mes marque-pages** : J'ai classé mes sites préférés et mes outils dans des dossiers sur mon navigateur pour ne pas avoir à les chercher à chaque fois.
- **Mes notes numériques** : Dès que je vois une astuce technique ou une commande PowerShell utile, je la note pour pouvoir la ressortir plus tard.

### 5. Conclusion : Ma veille me fait progresser

Toute cette organisation me permet d'être super réactif. C'est grâce à cette méthode que j'ai pu repérer et comprendre l'attaque informatique dans les **Hauts-de-France** tout en faisant le lien avec mes cours sur le **Zero Trust**. Pour moi, la veille c'est le moteur qui va me permettre de devenir un bon **Manager en infrastructures** : en étant toujours au courant des dernières menaces, je serai capable de mieux protéger mon futur réseau.