



BTS SIO

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS

FICHE MÉTHODOLOGIQUE DE VEILLE TECHNOLOGIQUE

Candidat : Alenzo Wauters

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

Thème de veille : L'approche Zero Trust et la résilience des infrastructures face aux cybermenaces.

SOMMAIRE

Table des matières

1. Introduction : Ma démarche de veille	2
2. Outils et Méthodologie : LinkedIn comme pivot	2
3. Étude de cas : Analyse d'un incident en région Hauts-de-France	4
4. Synthèse technique : Vers l'architecture Zero Trust	4
5. Conclusion et perspectives professionnelles.....	5

1. Introduction : Ma démarche de veille

Dans le cadre de mon **BTS SIO**, la veille technologique est un pilier de mon apprentissage. L'informatique évoluant plus vite que les programmes, il est vital de rester connecté au terrain. Ma veille se concentre sur la **cybersécurité**, avec un intérêt particulier pour la protection des données et la disponibilité des services informatiques face aux cyberattaques.

2. Outils et Méthodologie : LinkedIn comme pivot

Plutôt que d'utiliser des outils de stockage passif, j'ai choisi une approche de **veille active** sur LinkedIn. Cette méthode me permet d'échanger directement avec des experts et de suivre l'actualité institutionnelle.

- **L'ANSSI (CERT-FR)** : Ma source pour les alertes critiques et les guides officiels de sécurisation des systèmes.



The screenshot shows the LinkedIn profile of the official page of the Agence nationale de la sécurité des systèmes d'information (ANSSI). The page features a banner with a blue and red shield logo, a person working at a computer, and a message about unlocking a new level related to national cyberdefense. Below the banner, the page name 'ANSSI - Agence nationale de la sécurité des systèmes d'information' is displayed with a verified checkmark. A brief description follows: 'Défendre, connaître, partager, accompagner et réguler.' It also lists 'Sécurité informatique et des réseaux · PARIS · 394 K abonnés · 501-1 K employés'. There are 2 other relations following the page. At the bottom, there are buttons for 'Envoyer un message' (Send a message), 'Suivi' (Follow), and a three-dot menu. The navigation bar at the bottom includes 'Accueil', 'À propos', 'Posts' (which is underlined in green), 'Emplois', 'Vie de l'organisation', and 'Personnes'.

Identification de la source institutionnelle de référence.

Abonnement à la page officielle de l'ANSSI pour le suivi des bulletins d'alerte du CERT-FR. Cette source me permet d'anticiper les vulnérabilités critiques et de consulter les guides de bonnes pratiques pour la sécurisation des infrastructures nationales.

- **Damien Bancal (ZATAZ)** : Une source précieuse pour comprendre la psychologie des attaquants et le "cyber-renseignement".

Bancal Damien ZATAZ · 3e
Communication - Cyberintelligence - Fondateur ZATAZ/Service Veille -
-> Je ne lis pas les MP, uniquement courriel, merci.
Lille, Hauts-de-France, France · [Coordonnées](#)
[Pour me contacter.](#)
23 426 abonnés · Plus de 500 relations

[Message](#) [Suivi](#) [Plus](#)

Veille spécialisée en Cyberintelligence et menaces émergentes.

Suivi de l'expert Damien Bancal pour une veille orientée 'terrain' sur les fuites de données et l'actualité du cyber-crime. Cette source complète mon approche institutionnelle par des analyses concrètes sur les modes opératoires des attaquants.

3. Étude de cas : Analyse d'un incident en région Hauts-de-France

The screenshot shows a LinkedIn feed window. At the top, it says "2 publications". The first publication is by "Alenzo WAUTERS" with the text: "C'est assez impressionnant (et inquiétant) de voir que ça touche encore nos collectivités locales, juste ici dans les Hauts-de-France. Merci pour le partage Damien Bancal ! En plein BTS SIO, ce genre d'actu nous sort direct de la théorie des cours. Ça pose de vraies questions : comment on assure la continuité des services publics quand tout est bloqué ? On en revient toujours aux fondamentaux qu'on bosse en SISR : des sauvegardes vraiment étanches et surtout, arrêter de faire confiance par défaut aux équipements sur le réseau (le fameux Zero Trust). Courage aux équipes IT en place, c'est le genre de situation qu'on redoute tous mais qui nous apprend le plus sur la résilience des systèmes." The second publication is by "Bancale Damien" with the text: "Nouvelle cyberattaque contre une collectivité des Hauts-de-France". Below these posts, there is a comment from "Evelyne Bourderiou" and another from "Bancale Damien". The LinkedIn interface includes a sidebar with user information like "ETUDIANT BTS SIO (SISR)", "Alenzo WAUTERS", and "Relations Développez votre réseau". The right side of the screen shows a banner for LinkedIn's hiring feature and some accessibility settings.

Exemple d'interaction et d'analyse d'une actualité cyber régionale (Hauts-de-France) sur mon fil de veille LinkedIn.

Mon analyse de l'incident : En réagissant à l'attaque contre une collectivité locale de ma région, j'ai pu lier la théorie du BTS à la réalité du terrain. Cet incident illustre l'importance de la **continuité de service** et du besoin de **sauvegardes étanches**. Cela confirme que la confiance aveugle au sein d'un réseau est une faille en soi, d'où la nécessité de passer au modèle **Zero Trust**.

4. Synthèse technique : Vers l'architecture Zero Trust

Le concept de "Zéro Confiance" n'est pas qu'un mot à la mode, c'est une nécessité en **SISR**.

- **Vérification systématique** : Chaque utilisateur et appareil doit être authentifié, quel que soit son emplacement.
- **Moindre privilège** : Limiter les accès au strict nécessaire pour réduire la surface d'attaque.
- **Segmentation** : Diviser le réseau en zones isolées pour empêcher la propagation d'un rançongiciel.

5. Conclusion et perspectives professionnelles

Cette veille m'a permis de comprendre que le métier de **Manager en infrastructures et cybersécurité** ne s'arrête jamais aux acquis techniques. Savoir traiter l'information et anticiper les menaces est la compétence la plus précieuse que j'ai développée durant ces deux années. Ma veille continuera d'évoluer en Mastère pour rester à la pointe des stratégies de défense cyber.