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

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.

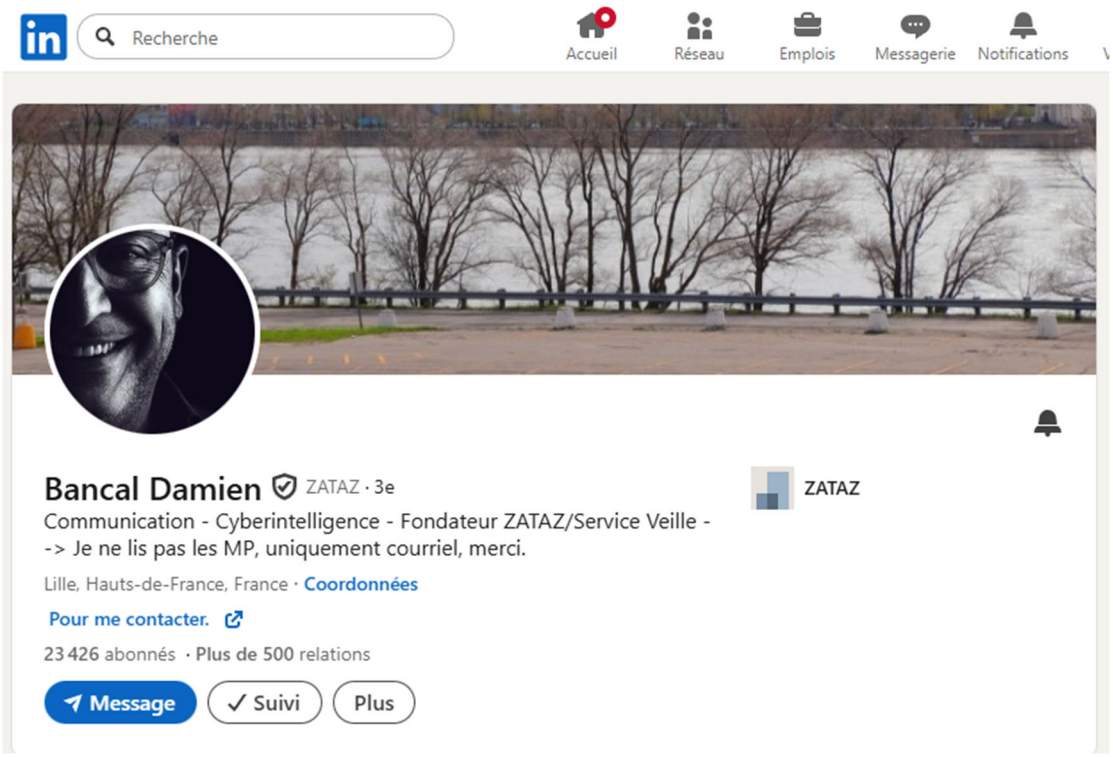
- **L'ANSSI (CERT-FR) :** Ma source pour les alertes critiques et les guides officiels de sécurisation des systèmes.

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.

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

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

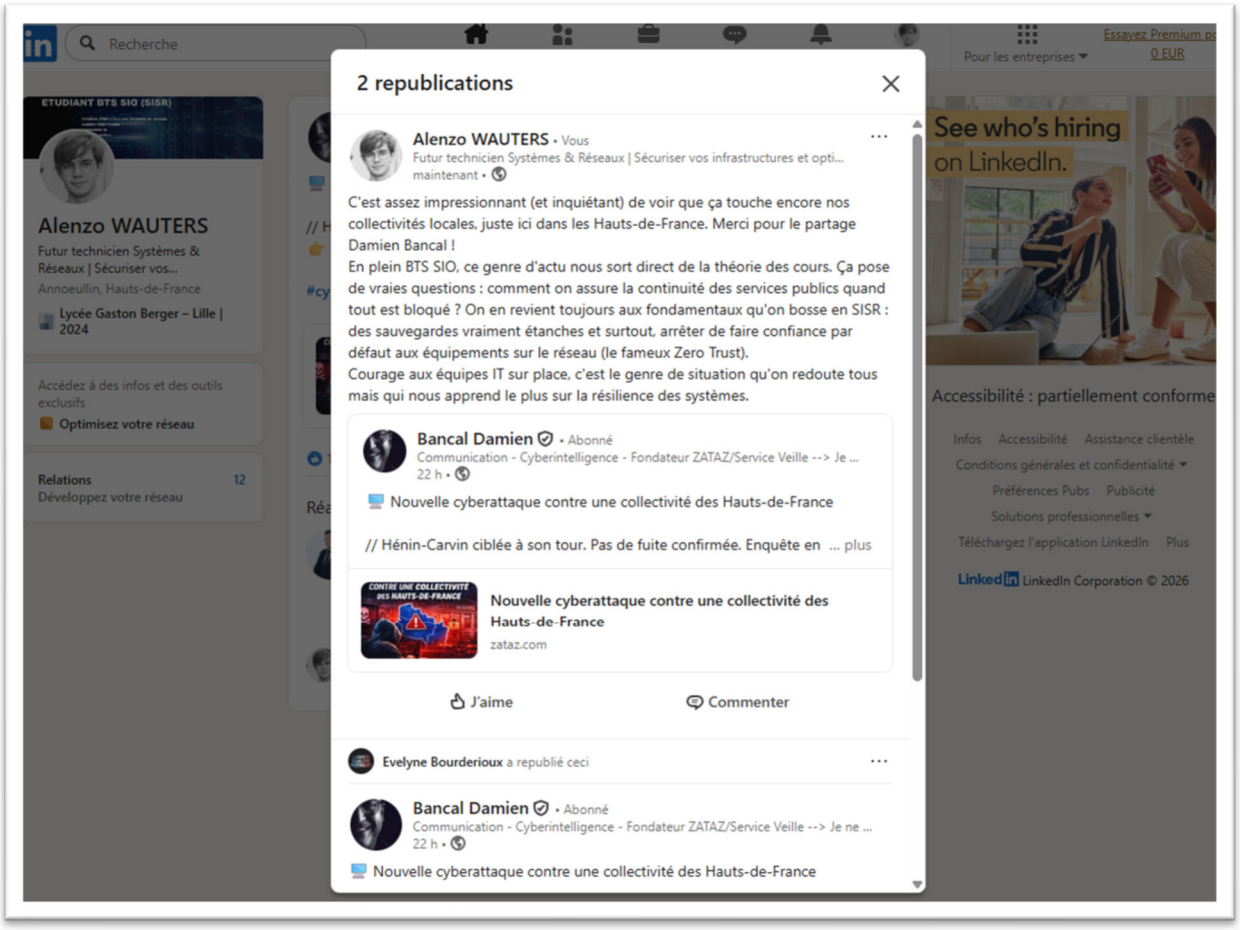


Veille spécialisée en Cyberintelligence et menaces émergentes.

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.

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

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



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.

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

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.