MISE EN PLACE D'UNE VEILLE TECHNOLOGIQUE

Fernandes Sébastien - BTS SIO 2025/2026

1. Introduction

Durant ma formation en BTS SIO option SISR, j'ai mis en place une veille technologique sur la sécurisation des échanges numériques à travers l'évolution des certificats SSL/TLS (Secure Sockets Layer / Transport Layer Security). De plus, durant mon stage de première année des questions technique ce sont posé.
La veille technologique consiste à rechercher, collecter, analyser et partager des informations dans un domaine précis afin d'anticiper les évolutions et d'orienter les décisions techniques.
Dans un contexte où la cybersécurité est une priorité, les certificats SSL/TLS jouent un rôle essentiel dans la protection des communications entre utilisateurs et serveurs. Leur réduction progressive de durée de validité rend désormais l'automatisation de leur gestion indispensable pour les administrateurs réseau et les responsables sécurité.

2. Mon sujet de veille

2.1 SSL/TLS : Réduction de la durée des certificats et automatisation

Depuis 2020, les autorités de certification (CA) réduisent progressivement la durée de validité des certificats SSL/TLS. L'objectif est d'augmenter la sécurité des échanges en limitant la durée d'exploitation d'un certificat compromis.

Les principales évolutions prévues sont :

- 398 jours → 200 jours (2026) → 100 jours (2027) → 47 jours (2029) → 10 jours (2029)
- Adoption du protocole ACME (*Automatic Certificate Management Environment*) pour le renouvellement automatique (ex. : *Let's Encrypt, Sectigo*)
- Intégration de la gestion des certificats dans les outils CI/CD (Continuous Integration / Continuous Deployment) et de supervision réseau
- Préparation à la cryptographie post-quantique et aux certificats à durée ultra-courte

Impacts pour les administrateurs système et réseau :

- L'automatisation devient incontournable pour éviter toute interruption de service.
- La surveillance des expirations doit être intégrée à la supervision centralisée.
- La réduction du risque de compromission améliore la sécurité globale des infrastructures.
- Aujourd'hui, plus de 85 % des certificats gratuits (DV) sont déjà renouvelés automatiquement.

Tarifs observés en 2025 :

- DV (Validation de Domaine) : gratuits (Let's Encrypt) à ~30 €/an

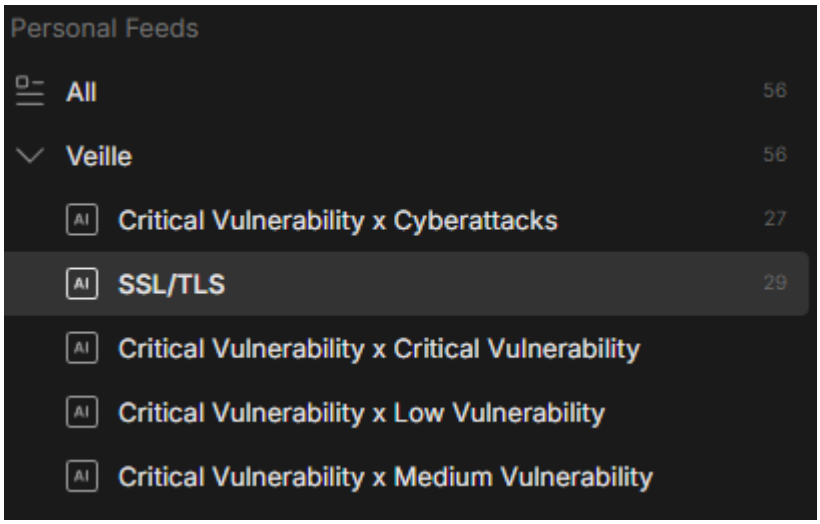
- OV (Validation d'Organisation) : 60 à 150 €/an
- EV (Validation Étendue) : 150 à 400 €/an
- Wildcard : 80 à 300 €/an
- SAN (Multi-domaines) : jusqu'à 800 €/an

Ces changements imposent aux entreprises une gestion proactive, mais renforcent significativement la sécurité et la fiabilité des échanges.

3. Les outils de veille

3.1 Feedly

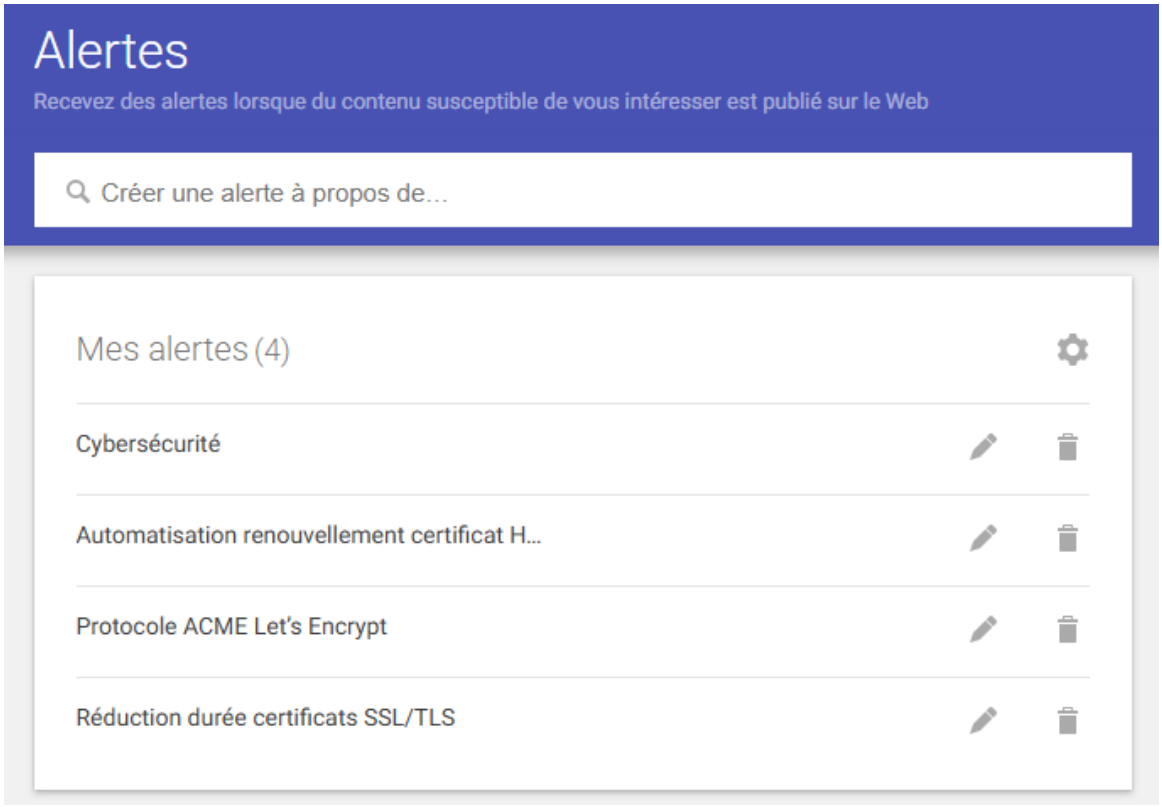
Feedly est un agrégateur de flux RSS permettant de centraliser les publications provenant de différentes sources.
Je l'ai utilisé pour suivre les actualités liées à :



Grâce à ses filtres, Feedly m'a permis de trier les informations pertinentes et d'obtenir une veille automatisée et actualisée sur le thème des certificats numériques.

3.2 Google Alertes

J'ai configuré Google Alertes pour recevoir par e-mail des notifications sur les mots-clés :



Cet outil, complémentaire à Feedly, fonctionne selon la **méthode push** : les informations me sont envoyées automatiquement lorsqu'un nouveau contenu pertinent est publié.

4. Articles consultés

- Nameshield (2025) – *C'est officiel : la durée de vie des certificats SSL/TLS va être réduite à 47 jours* lien

- Let's Encrypt Blog – *The Future of Short-Lived Certificates* lien
- Le Monde Informatique – *Automatisation et supervision : la clé pour la sécurité des certificats TLS* lien

Ces sources fiables m'ont permis de mieux comprendre les enjeux techniques, économiques et réglementaires liés à l'évolution des certificats.

5. Conclusion

Cette veille m'a permis de constater que la sécurité réseau évolue vers une automatisation complète des processus de certification.
En tant que futur administrateur réseau, je serai directement concerné par cette transformation :

- Mise en place de scripts d'auto-renouvellement,
- Intégration dans les chaînes DevOps,
- Surveillance des certificats via des outils de supervision centralisée.

Les certificats à courte durée de vie représentent un progrès majeur en matière de sécurité et de résilience, mais nécessitent une gestion rigoureuse et automatisée.
Cette veille m'a ainsi permis de développer mes compétences en cybersécurité, administration système et automatisation, essentielles dans le domaine SISR.