Mise en place d’une veille technologique

FOUR Lucas
Conseil départemental de la Drôme

Table des matières

Cahier des charges – Expression des besoins

| Descriptif de l'existant |

Avant la mise en place de ce projet, je ne disposais d'aucun système structuré de veille technologique. Mon suivi de l'actualité en cybersécurité se limitait à des consultations ponctuelles et non organisées de différents sites web, sans agrégation, sans archivage, et sans aucune méthode de classement des informations recueillies. Mon environnement de travail se compose d'un poste personnel sous Windows 11 disposant d'un accès Internet, ainsi que d'une adresse de messagerie Gmail. Aucun outil dédié à la veille n'était installé.

| Besoin(s) |

Ce projet a pour objectif la mise en place d'une veille technologique structurée et durable, centrée sur la détection des nouvelles failles de sécurité informatique (vulnérabilités CVE). Cette veille doit me permettre de :

- Suivre quotidiennement la publication de nouvelles vulnérabilités sur les systèmes d'exploitation, les équipements réseau et les logiciels couramment déployés en entreprise ;
- Identifier rapidement les failles critiques (score CVSS élevé, exploitation active dans la nature) afin de pouvoir réagir avec priorité ;
- Archiver et catégoriser les informations recueillies pour pouvoir les restituer lors de l'épreuve orale du BTS SIO ;
- Disposer d'une démarche professionnelle, reproductible et documentée, transposable en environnement professionnel.

| Contrainte(s) |

La réalisation de cette veille est soumise aux contraintes suivantes :

- **Contrainte de temps** : la mise en place de l'infrastructure de veille doit être réalisée en moins de quatre heures, hors temps de prise en main quotidien.
- **Contrainte budgétaire** : la solution retenue doit être entièrement gratuite et ne nécessiter aucun abonnement payant ni achat de licence.
- **Contrainte juridique** : les sources consultées doivent être publiques et licites, et le traitement des informations doit respecter les conditions d'utilisation des éditeurs (pas de scraping abusif).
- **Contrainte d'organisation** : la veille doit pouvoir être maintenue durablement avec un investissement quotidien réduit (10 minutes maximum), pour rester compatible avec la charge de travail du BTS.
- **Contrainte de validation** : le projet sera considéré comme abouti lorsque les flux d'information seront agrégés automatiquement, classés selon leur criticité, et qu'une seconde couche de notification par mail sera fonctionnelle.

Ressources

| Ressources mises à disposition |

Pour la réalisation de ce projet, je dispose des ressources suivantes :

- Un poste de travail personnel sous Windows 11 disposant des droits d'administration nécessaires à l'installation de logiciels ;
- Un accès Internet stable, indispensable pour la récupération des flux RSS et la consultation des sources ;
- Une adresse de messagerie Gmail personnelle, qui sera utilisée pour la réception des alertes critiques.

| Ressources nécessaires à la mise en place |

Plusieurs éléments logiciels sont nécessaires à la mise en place de la solution :

- **Mozilla Thunderbird** : client de messagerie open source qui sera détourné de son usage classique pour servir d'agrégateur de flux RSS local. Téléchargeable gratuitement sur *https://www.thunderbird.net*
- **Blogtrottr** : service web gratuit permettant la conversion d'un flux RSS en notification par mail. Aucun compte requis. Disponible sur *https://blogtrottr.com*
- **Sources d'information publiques** : flux RSS du CERT-FR (cert.ssi.gouv.fr), de la CISA, ainsi que de plusieurs médias spécialisés en cybersécurité (Bleeping Computer, The Hacker News, Krebs on Security, Dark Reading) et de l'éditeur Microsoft (Security Update Guide).

| Gestion des ressources |

L'ensemble des ressources mobilisées étant gratuit et accessible publiquement, aucune procédure d'approvisionnement n'a été nécessaire. La principale ressource à gérer dans la durée est le temps quotidien consacré à la veille, estimé à dix minutes par jour ouvré, complété par une session hebdomadaire d'environ quarante-cinq minutes consacrée à la rédaction d'une fiche de veille approfondie.

Analyse

| Descriptifs des solutions |

Plusieurs solutions ont été envisagées pour bâtir l'infrastructure de veille. Trois d'entre elles ont été comparées en détail :

- **Feedly** est un agrégateur de flux RSS hébergé dans le cloud. L'utilisateur crée un compte sur le service et accède à son tableau de bord via un navigateur web. La version gratuite permet de suivre jusqu'à cent sources et de les organiser en plusieurs dossiers. L'inscription nécessite un compte Google ou une adresse mail, et les données sont stockées sur les serveurs de l'éditeur.
- **Mozilla Thunderbird** est un client de messagerie open source développé par la fondation Mozilla. Outre la gestion des emails, il intègre un module de lecture de flux RSS qui permet de créer des comptes dédiés à la veille. Toutes les données sont stockées localement sur le poste de l'utilisateur. Le logiciel propose un système d'étiquettes colorées et de filtres automatiques par mots-clés.
- **FreshRSS** est un agrégateur de flux RSS auto-hébergé, écrit en PHP. Il s'installe sur un serveur web (Apache ou Nginx) et propose une interface web personnalisable. Cette solution offre une grande maîtrise des données mais nécessite la mise en place d'une infrastructure de serveur.

| Comparaison des solutions |

Solutions	Thunderbird	Feedly	FreshRSS
Coûts	Gratuit (open source)	Gratuit (version limitée) ou payant	Gratuit (open source)
OS d'installation	Windows, macOS, Linux (client lourd)	Service en ligne (cloud, navigateur web)	Serveur Linux (auto-hébergement, PHP / MySQL)
Points forts	Données 100 % locales Étiquettes colorées Filtres automatiques par mots-clés Aucun compte requis	Très simple à mettre en place Interface moderne et accessible Application mobile disponible Synchronisation multi-appareils	Maîtrise complète des données Hautement personnalisable API et extensions disponibles Adapté à la projection en entreprise
Interface / utilisation	Familière de type messagerie, classique mais efficace	Très intuitive, design moderne et soigné	Interface web sobre, moins léchée que Feedly
Mise en place	Rapide à déployer, configuration accessible	Immédiate, simple inscription par mail	Plus longue, nécessite un serveur web (Apache, Nginx, base MySQL)
Communauté / Support	Communauté active soutenue par Mozilla	Support éditeur, communauté importante	Communauté open source orientée auto-hébergement

Idéal pour	Étudiants, professionnels souhaitant une veille structurée et privée	Utilisateurs cherchant une solution rapide et sans installation	Entreprises et particuliers avancés disposant d'un serveur
Limites	Pas de synchronisation entre appareils, pas d'application mobile	Données stockées chez l'éditeur, fonctionnalités bridées en gratuit	Installation complexe, nécessite des compétences serveur

| Choix d'une solution – Argumentation |

J'ai choisi de retenir **Mozilla Thunderbird** comme solution principale pour la mise en place de cette veille, complétée par **Blogtrottr** pour la couche de notification par mail. Ce choix s'appuie sur plusieurs arguments. Tout d'abord, Thunderbird est entièrement gratuit, open source, et ne nécessite la création d'aucun compte tiers. L'ensemble des données de veille est stocké localement sur mon poste, ce qui garantit la confidentialité de ma démarche et l'absence de dépendance à un service externe pouvant disparaître ou changer ses conditions d'utilisation. Ensuite, Thunderbird propose nativement un système d'étiquettes colorées et un moteur de filtres automatiques très puissant, deux fonctionnalités essentielles pour catégoriser efficacement les vulnérabilités selon leur criticité. La présentation des articles dans une interface familière de type messagerie facilite également la prise en main. Enfin, l'utilisation d'un client lourd installé sur le poste constitue un argument professionnel valorisable lors de l'oral, en démontrant la maîtrise d'un outil open source plutôt que la simple consommation d'un service en ligne. La solution FreshRSS, bien que techniquement plus avancée, a été écartée en raison de la complexité de son installation et de l'absence d'infrastructure serveur disponible dans le cadre de ce projet. **Blogtrottr** est ajouté en complément pour transformer certains flux critiques en notifications par mail. Cette seconde couche garantit qu'aucune alerte critique ne soit manquée, même en cas de longue absence devant le poste, et reproduit le fonctionnement d'un véritable Security Operations Center (SOC) en entreprise.

| Etude de l'impact sur le SI existant |

Étant donné que ce projet s'inscrit dans un cadre personnel et pédagogique, il n'existe aucun système d'information préexistant à impacter. La mise en place de la veille n'a aucune incidence sur d'autres services. Toutefois, la mise en place d'un dispositif équivalent en entreprise présenterait plusieurs intérêts : amélioration de la posture de sécurité grâce à une meilleure réactivité face aux nouvelles vulnérabilités, valorisation du temps des équipes techniques par l'automatisation du tri, et structuration de la connaissance accumulée grâce à l'archivage local et à la classification par étiquettes.

Sécurité :

Aucun risque introduit. Les flux RSS consultés sont publics et lus en mode passif. Aucune authentification n'est utilisée.

Performance :

L'impact sur les ressources du poste est négligeable : Thunderbird consomme moins de 200 Mo de mémoire vive en fonctionnement et l'ensemble des flux représente un volume de données très faible.

Juridique :

Toutes les sources retenues sont publiques et autorisent explicitement la consultation par flux RSS via leurs conditions d'utilisation.

Ergonomie :

L'interface de Thunderbird est familière et la disposition en mode classique permet une lecture fluide. Le système d'étiquettes colorées facilite la priorisation visuelle.

| Phasage de l'intervention |

La mise en place s'organise en six phases successives, chacune étant une étape bloquante pour la suivante :

N°	Phases	Durées	Tests associés
1	Installation et configuration de Thunderbird	15 min	Lancement du logiciel
2	Création du compte Veille SIO et des sous-dossiers	20 min	Vérification de l'arborescence
3	Ajout des flux RSS dans les dossiers thématiques	25 min	Réception d'articles
4	Création des étiquettes colorées	10 min	Étiquetage manuel test
5	Mise en place des filtres automatiques	30 min	Exécution sur l'existant
6	Configuration de Blogtrottr (push mail)	15 min	Réception du premier digest

| Prévision des tests et validation |

Les tests sont prévus à la fin de chaque phase de la procédure, afin de valider chaque brique avant de passer à la suivante :

- **À l'issue de la phase 1** : vérification du lancement de Thunderbird et de l'accès à l'interface principale.
- **À l'issue de la phase 3** : vérification de l'apparition automatique d'articles dans chaque dossier thématique, ce qui valide à la fois la connectivité Internet et le bon paramétrage des flux.
- **À l'issue de la phase 5** : exécution manuelle des trois filtres sur les articles déjà téléchargés, et vérification de l'apparition des étiquettes colorées sur les articles correspondants aux mots-clés.
- **À l'issue de la phase 6** : confirmation des trois abonnements Blogtrottr par retour mail, et attente du premier digest le lendemain matin pour valider la chaîne de bout en bout.

Mise en place

| Installation et configuration de Thunderbird |

La première étape consiste à télécharger Thunderbird depuis le site officiel de la fondation Mozilla.

Téléchargement et installation :

Se rendre sur l'adresse https://www.thunderbird.net puis cliquer sur le bouton « Téléchargement gratuit ». Le fichier d'installation pèse environ 60 Mo. Une fois téléchargé, double-cliquer sur l'exécutable et suivre l'assistant en sélectionnant l'installation de type « Standard ».

Première ouverture :

Au premier lancement, Thunderbird affiche immédiatement une fenêtre de configuration de compte mail. Cette fenêtre n'étant pas pertinente pour notre usage, il faut la fermer en cliquant sur la croix en haut à droite. Si la fenêtre est bloquante, il est possible de saisir une adresse fictive (par exemple test@test.fr) afin de provoquer un échec de connexion permettant la fermeture.

Création du compte de flux :

Cliquer sur l'icône menu (☰) en haut à droite, puis choisir « Paramètres des comptes ». Dans le panneau de gauche, cliquer sur « Gestion des comptes » puis « Ajouter un autre compte… » et choisir le type « Compte Nouvelles & Flux ». Saisir le nom « Veille SIO » et valider.

Configuration des paramètres du compte :

Toujours dans les paramètres du compte, ajuster les options suivantes :

- Régler la fréquence de vérification des flux à 30 minutes ;
- Cocher l'option « Afficher le résumé de l'article plutôt que de télécharger la page web » pour un affichage plus fluide ;
- Vérifier que la case « Activer les mises à jour pour tous les flux » est bien cochée.

| Création des dossiers thématiques |

Les flux RSS doivent être organisés en quatre catégories thématiques, qui structureront l'ensemble de la veille. Pour chaque dossier, faire un clic droit sur le compte « Veille SIO » dans la colonne de gauche, choisir « Nouveau dossier… », saisir le nom et valider.

Les quatre dossiers à créer sont les suivants :

- **Officiel** : sources institutionnelles (CERT-FR, ANSSI, CISA).
- **Presse FR** : presse spécialisée francophone.
- **Presse EN** : presse spécialisée anglophone (réactivité supérieure).
- **Éditeurs** : bulletins de sécurité publiés directement par les éditeurs de logiciels.

| Ajout des flux RSS |

Les flux sont ajoutés via le gestionnaire d'abonnements. Cliquer sur le compte « Veille SIO » puis sur « Gérer les abonnements… ». Pour chaque flux, sélectionner le dossier de destination dans le menu déroulant « Ajouter à », coller l'URL du flux dans le champ correspondant, puis cliquer sur « Ajouter ».

Les huit flux retenus sont les suivants :

Dossiers	Sources	URL du flux
Officiel	CERT-FR Alertes	https://www.cert.ssi.gouv.fr/alerte/feed/
Officiel	CERT-FR Avis	https://www.cert.ssi.gouv.fr/avis/feed/
Officiel	CERT-FR Actualités	https://www.cert.ssi.gouv.fr/actualite/feed/
Presse EN	Bleeping Computer	https://www.bleepingcomputer.com/feed/
Presse EN	The Hacker News	https://feeds.feedburner.com/TheHackersNews
Presse EN	Krebs on Security	https://krebsonsecurity.com/feed/
Presse EN	Dark Reading	https://www.darkreading.com/rss.xml
Editeurs	Microsoft Security Update Guide	https://api.msrc.microsoft.com/update-guide/rss

| Création du système d'étiquettes |

Le système d'étiquettes permet de catégoriser visuellement chaque article reçu selon sa nature et sa criticité. Pour y accéder, cliquer sur le menu (☰) puis « Paramètres ». Dans la section « Général », faire défiler jusqu'à la rubrique « Étiquettes ».

Six étiquettes sont définies, chacune correspondant à un statut précis :

Etiquettes	Couleurs	Significations
Urgente	**ROUGE**	Vulnérabilité critique (CVSS ≥ 9, présence dans le catalogue CISA KEV ou exploitation active observée).
A analyser	**ORANGE**	Faille jugée intéressante à creuser pour la rédaction d'une fiche de veille.
Nouvelle	**JAUNE**	Vulnérabilité récemment publiée, en cours d'évaluation.
Corrigée	**VERT**	Faille pour laquelle un correctif officiel a été publié.
Cas d'étude	**BLEU**	Faille retenue comme cas d'étude approfondi pour la présentation orale.
Hors scope	**VIOLET**	Article lu mais non pertinent pour la veille.

| Mise en place des filtres automatiques |

Les filtres permettent à Thunderbird d'appliquer automatiquement les étiquettes selon le contenu du sujet de chaque article reçu. Cliquer sur le menu (☰), puis « Outils » et « Filtres de messages ».

Trois filtres sont configurés, dans l'ordre suivant (l'ordre est important car les filtres s'exécutent du haut vers le bas) :

Filtre 1 — Nouvelle (avis CERT) :

- Mode : « Valider au moins une des conditions suivantes » ;
- Conditions sur le sujet : contient « AVI- », contient « vulnérabilité », contient « vulnerability », contient « CVE- » ;
- Action : Étiqueter le message avec « Nouvelle ».

Filtre 2 — Corrigée (patch publié) :

- Mode : « Valider au moins une des conditions suivantes » ;
- Conditions sur le sujet : contient « patch », contient « correctif », contient « fix », contient « fixed », contient « resolved » ;
- Action : Étiqueter le message avec « Corrigée ».

Filtre 3 — Urgente (CVSS critique) :

- Mode : « Valider au moins une des conditions suivantes » ;
- Conditions sur le sujet : contient « critique », contient « critical », contient « zero-day », contient « zéro-jour », contient « exploited », contient « exploitée », contient « ALE- » ;
- Action : Étiqueter le message avec « Urgente ».

Le filtre « Urgente » est placé en dernier afin que sa couleur écrase celle des étiquettes précédentes pour les articles correspondant à plusieurs critères. Pour appliquer ces filtres aux articles déjà téléchargés, sélectionner les trois filtres dans la liste, choisir un dossier dans le menu déroulant « Exécuter le(s) filtre(s) sélectionné(s) sur » puis cliquer sur « Exécuter ». Cette opération est répétée pour chacun des quatre dossiers.

| Configuration de Blogtrottr |

Blogtrottr est utilisé pour la seconde couche de notification, par mail. Aucun compte utilisateur n'est nécessaire ; le service envoie un mail de confirmation à chaque abonnement.

Procédure d'abonnement :

Se rendre sur https://blogtrottr.com. Sur la page d'accueil, trois champs apparaissent :

- **Feed URL** : URL du flux RSS à surveiller ;
- **Email address** : adresse de réception des notifications ;
- **Schedule** : fréquence d'envoi. La valeur retenue est **Daily digest**, afin de recevoir un seul mail récapitulatif par jour.

Cliquer sur « Feed me ! » pour valider, puis se rendre dans la boîte mail pour cliquer sur le lien de confirmation.

Trois flux ont été configurés dans Blogtrottr, choisis pour leur niveau de criticité élevé :

Flux	URL	Fréquence
CERT-FR Alertes	https://www.cert.ssi.gouv.fr/alerte/feed/	Daily digest
CERT-FR Avis	https://www.cert.ssi.gouv.fr/avis/feed/	Daily digest
Bleeping Computer	https://www.bleepingcomputer.com/feed/	Daily digest

Le choix de limiter **Blogtrottr** à trois flux a été fait délibérément : recevoir trop de mails quotidiens conduirait inévitablement à les ignorer ou à se désabonner. Les trois sources retenues couvrent l'essentiel des informations critiques, le reste de la veille étant assuré par Thunderbird.

| Rapport de tests |

Conformément au prévisionnel des tests annoncés dans la phase d'analyse, les vérifications suivantes ont été effectuées à l'issue de la mise en place :

Tests réalisés	Résultats attendus	Statuts
Lancement de Thunderbird et accès à l'interface	Interface affichée	**Validé**
Création de l'arborescence des quatre dossiers	Dossiers visibles	**Validé**
Réception des articles dans le dossier Officiel	≥ 100 articles	**Validé (167)**
Réception des articles dans le dossier Presse EN	≥ 50 articles	**Validé (171)**
Réception des articles dans le dossier Éditeurs	≥ 100 articles	**Validé (3369)**
Création des six étiquettes colorées	Six couleurs	**Validé**
Application automatique des filtres aux articles	Étiquetage visible	**Validé**
Tri par étiquette dans la liste des messages	Filtrage fonctionnel	**Validé**
Confirmation des trois abonnements Blogtrottr	Trois mails reçus	**Validé**
Réception du premier digest quotidien	Mail à J+1	**Validé**
Lancement de Thunderbird et accès à l'interface	Interface affichée	**Validé**
Création de l'arborescence des quatre dossiers	Dossiers visibles	**Validé**

L'ensemble des tests prévisionnels a été validé sans réserve. L'infrastructure est opérationnelle et la veille est désormais alimentée automatiquement et structurée selon la criticité des informations.

Conclusion

La mise en place de cette veille technologique m'a permis de créer un dispositif complet de détection des failles de sécurité. Basée sur Thunderbird et Blogtrottr, la solution est gratuite, simple à maintenir, confidentielle et reproductible en milieu professionnel. Elle agrège plus de huit flux RSS, classés en quatre thèmes, avec un tri automatique selon six niveaux de criticité. Les notifications quotidiennes par mail assurent le suivi des alertes CERT-FR même sans accès à Thunderbird. Cette démarche illustre le fonctionnement d'un SOC individuel, mêlant veille quotidienne et alertes en temps réel.

Auto-évaluation

Le projet a été réalisé dans le temps prévu, avec une mise en place en environ deux heures quinze, tests compris. Cette réussite s'explique par une bonne préparation préalable, notamment le choix des sources et la consultation de la documentation Thunderbird. Les principaux points forts sont l'utilisation d'une solution open source, indépendante de services propriétaires, ainsi qu'une architecture à deux niveaux, proche d'un fonctionnement professionnel. Les étiquettes colorées et les filtres automatiques facilitent la priorisation rapide des alertes importantes. Des améliorations restent possibles, comme l'installation de Thunderbird sur un poste dédié, la migration vers une solution auto-hébergée telle que FreshRSS, ou encore la création d'un script Python pour générer automatiquement des fiches de veille à partir des articles à analyser. Au-delà de l'aspect technique, ce projet m'a permis de mieux mesurer le volume d'informations publié chaque jour en cybersécurité. Il m'a aussi amené à structurer un temps de veille régulier, appelé à devenir une habitude durable dans ma pratique professionnelle.