Veille informatique

Mathias SINGH – Le 05/10/2026

Concevoir et mettre en place un dispositif de veille

Bac+5 Expert en sécurité des développements informatiques

Cinq questions pour la journée

1. Qu'est-ce que la veille numérique ?
2. Comment concevoir une veille numérique ?
3. Comment mettre en place une veille sur Internet ?
4. Comment intégrer le suivi concurrentiel dans sa veille ?
5. Comment intégrer le community management dans sa veille ?

Le livrable attendu en fin de journée

3

sources de veille au minimum, dont une consacrée à la sécurité

- Un axe de veille formulé : Sujet, question, destinataire, fréquence
- Trois sources au minimum, chacune décrite dans une fiche de source
- Au moins une source primaire consacrée à la sécurité
- Un outil de collecte paramétré et fonctionnel
- Une restitution orale de 2 minutes par personne ou binôme

1

Comprendre la veille numérique

Définition, familles de veille, enjeux pour un développeur en 2026

Une définition de travail

La veille est une activité continue et organisée de surveillance de son environnement, destinée à anticiper les évolutions et à éclairer des décisions.

Ce que c'est

Un processus répété, cadré par un besoin, qui produit une information exploitable pour quelqu'un.

Ce que ce n'est pas

Une recherche ponctuelle, une lecture au hasard de l'actualité, ou une accumulation de liens jamais relus.

Ce qui la distingue

Un destinataire identifié, une fréquence, des sources choisies et une trace écrite de ce qui a été retenu.

Cinq familles de veille

1 Technologique

Langages, frameworks, versions, fin de support des composants utilisés.

2 Vulnérabilités

Failles affectant la pile logicielle et les dépendances, exploitation en cours.

3 Réglementaire

Textes et obligations applicables : RGPD, NIS 2, règlement sur la cyberrésilience.

4 Concurrentielle

Produits, prix, fonctionnalités et choix techniques des acteurs comparables.

5 Image et communauté

Ce qui se dit du produit et de l'organisation, signalements des utilisateurs.

Pourquoi la veille pèse davantage en 2026

+263 %

de soumissions de CVE entre 2020 et 2025

Le volume dépasse la capacité d'analyse de la base nationale américaine.

15 avril

2026 : La NVD n'enrichit plus toutes les CVE

Priorité aux CVE jugées les plus critiques. S'appuyer sur une seule base ne suffit plus.

24 h

pour l'alerte précoce imposée par le CRA

Depuis le 11 septembre 2026, le fabricant signale toute vulnérabilité activement exploitée.

Source : NIST, NIST Updates NVD Operations to Address Record CVE Growth, 15 avril 2026 ; ENISA, fiche plateforme unique de signalement CRA, septembre 2026

2

Concevoir une stratégie de veille

Domaines, axes, périmètre, types de contenus, sources

Le processus de veille en cinq étapes

1

Cadrer

Domaines, axes, destinataires

›

2

Sourcer

Périmètre, types de contenus, sources

›

3

Collecter

Flux, alertes, requêtes, tri

›

4

Analyser

Recouper, qualifier, synthétiser

›

5

Diffuser

Publier, alerter, archiver

Boucle de retour : Les destinataires disent ce qui leur a servi, et le cadrage est ajusté

Identifier les domaines à couvrir

Domaine	Question à laquelle la veille répond	Point de départ concret
Pile technique	Quelles versions arrivent, lesquelles ne sont plus maintenues ?	Inventaire des langages, frameworks, images de base
Vulnérabilités	Un composant que j'utilise est-il vulnérable ou exploité ?	Liste des dépendances, nomenclature logicielle
Réglementation	Quelle obligation nouvelle s'applique à mon produit ?	Secteur, pays de mise sur le marché, données traitées
Concurrence	Que proposent les acteurs comparables, à quel rythme ?	Liste de 3 à 5 produits de référence
Communauté	Que disent les utilisateurs et les chercheurs de mon produit ?	Nom du produit, dépôts, canaux officiels

Formuler un axe de veille

Un axe se formule en quatre éléments

1 Sujet

Ce qui est surveillé, nommé précisément.

2 Question

La décision que l'information doit éclairer.

3 Destinataire

La personne ou l'équipe qui agira.

4 Fréquence

Temps réel, quotidien, hebdomadaire.

Trop large

Suivre la cybersécurité.

Exploitable

Vulnérabilités exploitées touchant nos dépendances Node.js, pour décider d'un correctif urgent, à destination de l'équipe backend, chaque matin.

Délimiter le périmètre et les contenus

Le périmètre : Ce que l'on exclut

- Langues : Français, anglais, autres
- Zone : France, Union européenne, monde
- Période : Nouveautés seulement, ou historique
- Niveau : Technique, décisionnel, grand public
- Volume acceptable : Nombre d'items lus par jour

Les contenus : Ce que l'on collecte

- Avis et alertes de sécurité
- Notes de version et journaux de modifications
- Textes officiels et guides d'autorités
- Articles techniques et rapports d'analyse
- Discussions : Tickets, forums, réseaux sociaux

Quatre familles de sources

1 Institutionnelles

Autorités et centres de réponse : CERT-FR, ANSSI, ENISA, CISA, NIST. Information primaire, validée, parfois plus lente.

2 Éditeurs et projets

Bulletins de sécurité, notes de version, dépôts de code. Source primaire sur le produit concerné.

3 Communauté

Chercheurs, conférences, listes de diffusion, réseaux sociaux. Signal précoce, à recouper.

4 Médias spécialisés

Presse et blogs techniques. Mise en contexte utile, source secondaire à vérifier.

3

Les sources de référence en sécurité

CERT-FR, CVE, NVD, EUVD, KEV, OWASP

CERT-FR : La source française de premier rang

Publication	Usage pour la veille
Alertes de sécurité	Danger immédiat, à traiter en priorité
Avis de sécurité	Vulnérabilités corrigées par les éditeurs, flux quotidien
Rapports menaces et incidents	Analyse des attaquants et des modes opératoires
Indicateurs de compromission	Éléments techniques pour la détection
Durcissement et recommandations	Mesures de configuration et de protection
Bulletins d'actualité	Synthèse périodique des vulnérabilités marquantes
Fiches réflexes	Conduite à tenir face à un incident

Source : CERT-FR, page À propos et menu Publications, cert.ssi.gouv.fr, consultée le 4 octobre 2026

Vulnérabilités : Qui publie quoi

Référentiel	Porté par	Ce qu'il apporte	Limite à connaître
CVE	Programme CVE (MITRE)	Un identifiant unique par vulnérabilité	Description parfois minimale
NVD	NIST, États-Unis	Enrichissement : Score, produits affectés	N'enrichit plus toutes les CVE depuis avril 2026
EUVD	ENISA, Union européenne	Agrège CVE, avis des CSIRT, marquage d'exploitation	Base récente, lancée en 2025
KEV	CISA, États-Unis	Liste des vulnérabilités exploitées dans la nature	Ne couvre que l'exploitation connue de la CISA

Source : CISA, Known Exploited Vulnerabilities Catalog ; ENISA, European Vulnerability Database ; NIST, communiqué du 15 avril 2026

Prioriser : Gravité, probabilité, exploitation

1 CVSS : La gravité

Score de 0 à 10 publié par le FIRST. Répond à la question : Quel serait l'impact si la faille était exploitée ?

2 EPSS : La probabilité

Score de 0 à 1 publié par le FIRST. Estime la probabilité d'exploitation dans les 30 jours. Mis à jour chaque jour.

3 KEV : Le constat

Catalogue de la CISA. La vulnérabilité est déjà exploitée. Signal le plus fort pour agir vite.

Aucun score ne connaît votre contexte : Le composant est-il réellement utilisé, exposé, atteignable ?

Source : FIRST, EPSS version 4, 17 mars 2025, first.org/epss ; CISA, catalogue KEV

OWASP Top 10:2025, la référence du développeur

- A01 Broken Access Control
- A02 Security Misconfiguration
- A03 Software Supply Chain Failures
- A04 Cryptographic Failures
- A05 Injection
- A06 Insecure Design
- A07 Authentication Failures
- A08 Software or Data Integrity Failures
- A09 Security Logging and Alerting Failures
- A10 Mishandling of Exceptional Conditions

Source : OWASP Foundation, OWASP Top 10:2025, owasp.org/Top10/2025

Évaluer une source avant de s'y fier

Critère	Question à se poser
Auteur	Qui publie, avec quelle compétence et quel intérêt ?
Origine	Source primaire, ou reprise d'une autre publication ?
Date	Date de publication et de mise à jour visibles ?
Preuve	Références, identifiants CVE, éléments vérifiables ?
Recoupement	L'information est-elle confirmée par une autre source indépendante ?

Deux jugements distincts : La fiabilité de la source, et la crédibilité de l'information

4

Outiller et faire vivre la veille

Outils, collecte, suivi concurrentiel, community management, diffusion

Choisir un outil de veille : Les critères

1 Licence

Open source, code visible sous conditions, ou propriétaire.

2 Hébergement

Auto-hébergé, ou service en ligne chez un tiers.

3 Filtrage

Mots-clés, étiquettes, règles, recherche plein texte.

4 Interopérabilité

Import et export OPML, API, webhooks.

5 Collaboration

Comptes multiples, partage, annotations.

6 Coût réel

Abonnement, mais aussi temps d'administration.

Panorama d'outils par besoin

Besoin	Outil	Licence	Remarque
Agréger des flux RSS	FreshRSS	AGPL 3.0	Auto-hébergé, multi-utilisateur
Agréger des flux RSS	Miniflux	Apache 2.0	Minimaliste, léger
Alertes sur les CVE	OpenCVE	À vérifier sur le dépôt	Abonnement par éditeur ou produit
Automatiser	Huginn	MIT	Agents de surveillance auto-hébergés
Automatiser	n8n	Fair-code, non open source	Auto-hébergement possible
Capitaliser	Logseq	AGPL 3.0	Notes locales en Markdown
Capitaliser	Obsidian	Propriétaire	Notes locales en Markdown

Source : Dépôts et sites des projets ; FreshRSS, github.com/FreshRSS/FreshRSS ; OpenCVE, opencve.io

Collecter sans se noyer

Mode poussé

L'information arrive seule : Flux RSS et Atom, listes de diffusion, alertes par produit, notifications de dépôt.

Mode tiré

On va la chercher : Requêtes enregistrées, consultation programmée d'un site, lecture d'un rapport périodique.

Trois règles de sélection

- Un item est gardé seulement s'il répond à la question de l'axe
- Une information importante se vérifie à la source primaire
- Une source qui ne donne rien d'utile en un mois est retirée

Intégrer le suivi concurrentiel

Ce que l'on observe	Où le trouver	Ce que cela apprend
Notes de version	Dépôts publics, pages de nouveautés	Rythme et priorités de développement
Bulletins de sécurité	Pages sécurité des éditeurs	Types de failles, délai de correction
Offres d'emploi	Sites carrières	Technologies adoptées, projets à venir
Tarifs et documentation	Sites officiels	Positionnement, fonctionnalités
Conférences et publications	Programmes, enregistrements	Orientations techniques annoncées

Cadre : Uniquement des informations publiques, obtenues loyalement

Intégrer le community management

1 Écouter

Suivre les mentions du produit, de l'organisation et de ses dépendances sur les canaux où la communauté s'exprime.

2 Détecter

Repérer un signalement de faille, une fuite de données annoncée, une rumeur, avant qu'ils ne s'amplifient.

3 Répondre

Disposer d'un canal de signalement connu et d'une personne désignée pour répondre.

4 Remonter

Transmettre à l'équipe technique ce qui relève d'un incident ou d'une vulnérabilité.

Analyser, organiser, diffuser

1 Automatiser

Filtres par mots-clés, étiquettes automatiques, alertes sur les produits suivis. L'automate trie, l'humain décide.

2 Centraliser

Un seul lieu de référence : Base de notes ou wiki, avec date, source, axe concerné et action décidée.

3 Diffuser

Alerte immédiate pour l'urgent, synthèse hebdomadaire pour le reste, dans le canal que l'équipe lit déjà.

Une note de veille tient en quatre lignes : Le fait, la source, l'impact pour nous, l'action proposée

5

Atelier et retour d'expérience

Mettre en place sa veille, présenter ses sources, partager

Atelier : Mettre en place sa veille

1	10 min	Choisir un contexte réel : Projet d'alternance, application, pile technique
2	10 min	Formuler un axe de veille complet
3	20 min	Trouver au moins 3 sources adaptées, dont une sur la sécurité
4	15 min	Paramétrer l'outil : Flux, filtres, alerte
5	15 min	Remplir les fiches de source et rédiger une note de veille

La fiche de source à remplir

Rubrique	Exemple rempli
Nom et adresse	CERT-FR, alertes de sécurité, cert.ssi.gouv.fr/alerte/
Type de source	Institutionnelle, primaire
Axe de veille servi	Vulnérabilités exploitées touchant notre pile technique
Mode de collecte	Flux RSS dans l'agrégateur, consultation chaque matin
Types de contenus	Alertes sur des vulnérabilités à traiter en priorité
Évaluation	Auteur identifié, publications datées, références fournies
Limite	Ne couvre pas tous les produits ni toutes les vulnérabilités

Restitution et retour d'expérience

Chaque restitution, en 2 minutes

- Mon axe de veille en une phrase
- Mes trois sources et pourquoi elles sont adaptées
- La source sécurité et ce qu'elle m'a appris aujourd'hui
- Ce que je garde demain, ce que j'abandonne

Questions pour le partage d'expérience

- Combien de temps par semaine la veille prend-elle réellement ?
- Quelle information de veille a déjà changé une décision ?
- Quelle source a été abandonnée, et pourquoi ?
- Comment la veille est-elle partagée dans l'équipe ?

À retenir

1. Une veille part d'une question et d'un destinataire, pas d'un outil
2. Peu de sources, choisies et évaluées, valent mieux qu'un flux illisible
3. En sécurité, croiser plusieurs référentiels : Aucune base ne couvre tout
4. Une information compte quand elle est vérifiée, diffusée et suivie d'une action
5. Une veille se révise : Sources et axes sont réexaminés régulièrement