

GUIDE

Suivre les vulnérabilités (CVE) qui vous concernent

Construire une veille CVE filtrée sur votre parc : sources NVD, KEV et EPSS croisées, avec un exemple de pipeline n8n, pour ne recevoir que ce qui compte.

Sedona Radar — audit de sécurité externe automatisé

Sedona AI Lecture ~11 min Édition 2026 sedona-ai.com

Publier 40 000 CVE par an ne rend personne plus sûr : sans filtre, la veille devient du bruit. La méthode qui fonctionne tient en une phrase — ne suivre que les vulnérabilités qui touchent VOS logiciels, puis les trier par probabilité réelle d'exploitation. Ce tutoriel montre comment croiser quatre sources publiques (CVE, NVD, KEV, EPSS) et les orchestrer dans n8n pour ne recevoir, chaque matin, que les alertes qui exigent vraiment une décision.

À retenir

- Le volume est ingérable à la main : plus de 40 000 CVE publiées en 2024 (un record), et le rythme continue de s'accélérer en 2026.
- Une veille utile filtre sur VOTRE inventaire logiciel (produits et versions), pas sur le flux mondial.
- Quatre sources complémentaires : CVE (l'identifiant), NVD (la sévérité CVSS), KEV CISA (l'exploitation confirmée), EPSS (la probabilité d'exploitation).
- Aucun signal seul ne suffit : la priorisation fiable croise inventaire, KEV, EPSS et CVSS.
- n8n, auto-hébergeable et fair-code, orchestre tout le pipeline sans développement lourd.
- Le seuil EPSS de 0,10 est un usage de terrain, pas une norme : calibrez-le sur votre capacité de remédiation.

01 Le vrai problème : trop d'alertes tue l'alerte

Suivre « toutes les CVE » est devenu impossible, et surtout inutile. Le flux mondial n'a cessé de battre des records, tandis que seule une fraction infime concerne réellement votre parc et fait l'objet d'une exploitation active. La bonne question n'est donc pas « quelles vulnérabilités existent ? » mais « lesquelles me concernent, moi, et lesquelles sont réellement exploitées ? ». Tout le reste est du bruit qui épuise vos équipes.

40 009

CVE publiées en 2024, soit +38,8 % vs 2023 — nouveau record annuel

JerryGamblin — 2024 CVE Data Review (données CVE.org / NVD), janvier 2025

35 364

CVE publiées rien qu'au 1er semestre 2026 — le rythme continue de s'accélérer

JerryGamblin — CVE Mid-Year 2026 Check-In, juillet 2026

02 Les quatre sources qui comptent vraiment

Une veille CVE robuste repose sur quatre sources publiques, gratuites et complémentaires. Chacune répond à une question différente — les confondre est l'erreur la plus courante.

Source	Qui la maintient	Ce qu'elle mesure	Rôle dans la veille
CVE	MITRE (depuis 1999)	Identifiant unique de la vulnérabilité	Le langage commun, la clé qui relie toutes les sources
NVD	NIST	Sévérité technique CVSS + produits affectés (CPE)	Enrichit chaque CVE, API REST idéale pour automatiser
KEV	CISA	Exploitation active confirmée (oui / non)	Signal binaire d'urgence maximale
EPSS	FIRST	Probabilité d'exploitation à 30 jours (0 à 1)	Priorise ce qui n'est pas encore au KEV

KEV : un signal binaire, pas un score

Le catalogue KEV de la CISA ne mesure ni sévérité ni probabilité : une CVE y entre uniquement si trois critères sont réunis — identifiant CVE attribué, remédiation documentée disponible, et preuve fiable d'exploitation dans la nature. C'est un « oui / non », pas une note de risque comme CVSS ou EPSS.

03 Prioriser : croiser quatre signaux, jamais un seul

La priorisation fiable ne repose sur aucun indicateur isolé. Elle croise quatre signaux, du plus discriminant au plus fin.

1. Présence dans votre inventaire : la CVE touche-t-elle un produit et une version que vous utilisez réellement ? (filtre n°1)
2. Présence au KEV : exploitation confirmée dans la nature = urgence absolue, quel que soit le score.
3. Score EPSS : probabilité d'exploitation prochaine, pour trier ce qui n'est pas encore au KEV.
4. Score CVSS : sévérité technique de l'impact si la faille est exploitée.

Le seuil EPSS de 0,10 n'est pas une norme

EPSS publie une probabilité entre 0 et 1, mise à jour chaque jour vers 13h30 UTC, mais ne définit AUCUN seuil officiel de priorisation. Le fameux 0,10 (10 %) est un usage de terrain, explicitement présenté sans autorité particulière par la FAQ du FIRST. Calibrez votre propre seuil selon votre capacité réelle de remédiation.

04 Étape par étape : le pipeline dans n8n

n8n est un orchestrateur de workflows fair-code (source-available) : auto-hébergeable gratuitement, il enchaîne des nœuds HTTP, un planificateur et des nœuds de notification sans écrire de code lourd. Voici le squelette d'une veille CVE filtrée.

- 1. Déclencheur planifié**
Nœud Schedule Trigger (Cron) : une exécution automatique chaque matin, par exemple à 8h.
- 2. Récupérer les CVE récentes**
Nœud HTTP Request vers l'API REST de la NVD, filtré sur les CVE publiées ou modifiées depuis la dernière exécution.
- 3. Récupérer le catalogue KEV**
Nœud HTTP Request vers le fichier JSON public du catalogue KEV de la CISA pour connaître les CVE réellement exploitées.
- 4. Récupérer les scores EPSS**
Nœud HTTP Request vers l'API EPSS du FIRST pour attacher à chaque CVE sa probabilité d'exploitation à 30 jours.
- 5. Croiser et filtrer**
Nœud IF / Filter : ne garder que les CVE dont le produit figure dans votre inventaire ET (présente au KEV OU EPSS $\geq$ votre seuil).
- 6. Notifier**
Nœud email, Slack, Teams ou webhook : une alerte claire par vulnérabilité retenue, avec CVE, produit, CVSS, EPSS et statut KEV.

05 Calibrer le filtre à votre parc

- 1 Dresser l'inventaire**
Listez vos logiciels et versions sous forme d'identifiants produits (CPE). C'est le filtre le plus discriminant : sans inventaire, toute veille reste du bruit.
- 2 Choisir un seuil EPSS**
Commencez large, puis resserrez au fil des semaines selon le volume que vos équipes peuvent réellement traiter. Le seuil n'est jamais figé une fois pour toutes.
- 3 Traiter le KEV comme prioritaire absolu**
Toute CVE de votre parc présente au catalogue KEV se corrige sans attendre le score : l'exploitation est déjà confirmée.

Commencez petit, itérez

Un premier workflow qui ne surveille que vos 10 briques logicielles les plus exposées vaut mieux qu'une usine à gaz jamais finie. Ajoutez des sources et des règles une fois le flux quotidien maîtrisé.

06 Router les bonnes alertes aux bonnes personnes

Une alerte utile arrive au bon interlocuteur, au bon niveau d'urgence. Modélisez trois canaux dans votre nœud de notification pour éviter la fatigue d'alerte.

- KEV + présente dans votre parc → alerte immédiate à l'équipe technique et information de la direction.
- EPSS élevé + CVSS critique, sans KEV → ticket priorisé dans votre outil de suivi.
- Le reste → digest hebdomadaire consolidé, sans interruption du travail en cours.

07 Garder la veille valide dans le temps

Attention aux règles périmées

En juin 2026, la CISA a révoqué sa directive BOD 22-01 — qui imposait des délais fixes de remédiation sur le catalogue KEV — pour la remplacer par la BOD 26-04, qui gradue la priorité via une matrice combinant quatre facteurs binaires — exposition publique de l'actif, présence au KEV, potentiel d'automatisation de l'exploit et degré de contrôle obtenu — soit 16 combinaisons qui se ramènent à cinq paliers de délai (le plus court étant de 3 jours). Nombre de tutoriels citent encore les anciens délais : ne les figez pas dans votre process.

La leçon de fond dépasse cette directive : n'ancrez pas votre veille sur un chiffre réglementaire susceptible de changer, mais sur des principes stables — exploitation confirmée = priorité absolue, sévérité et probabilité pour trier le reste. Revoyez vos sources et vos seuils au moins une fois par trimestre.

08 Aller plus loin avec Sedona.AI

Construire le workflow est à votre portée ; le maintenir et l'alimenter d'un inventaire à jour demande du temps. Sedona Radar analyse ce que votre domaine expose sur Internet et classe les vulnérabilités détectées par gravité, à chaque scan : il évalue, il ne certifie pas.

Deux façons de démarrer

Construire votre propre veille avec ce tutoriel, ou recevoir « La Veille Sedona », la lettre gratuite de Sedona.AI : chaque semaine, l'essentiel de la cybersécurité (NIS2, menaces, réglementation) en quelques lignes pour un dirigeant. C'est la même lettre pour tous les abonnés : elle ne remplace pas une veille filtrée sur votre parc. L'inscription se fait en bas de chaque page de sedona-ai.com.

§ Sources

1. NVD (National Vulnerability Database) — NIST — <https://nvd.nist.gov/>
2. CISA — Known Exploited Vulnerabilities Catalog (KEV) — <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
3. FIRST.org — EPSS (Exploit Prediction Scoring System) — <https://www.first.org/epss/>
4. FIRST.org — EPSS FAQ — <https://www.first.org/epss/faq>
5. CISA — BOD 26-04 : Prioritizing Security Updates Based on Risk — <https://www.cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk>
6. MITRE — CVE Program (site officiel CVE.org) — <https://www.cve.org/>
7. n8n — dépôt GitHub officiel (licence fair-code) — <https://github.com/n8n-io/n8n>
8. JerryGamblin — 2024 CVE Data Review — <https://jerrygamblin.com/2025/01/05/2024-cve-data-review/>

Une veille qui ne vous réveille que quand il le faut

Sedona.AI publie « La Veille Sedona », une lettre gratuite : chaque semaine, l'essentiel de la cybersécurité. Sedona Radar, lui, analyse ce que votre domaine expose sur Internet et classe les vulnérabilités détectées par gravité, à chaque scan.

Recevoir La Veille Sedona

sedona-ai.com/