

GUIDE

Voir votre exposition comme un attaquant

Le guide de la surface d'attaque externe pour PME & ETI

Sedona Radar — audit de sécurité externe automatisé

Sedona AI Lecture 14 min Édition 2026 sedona-ai.com

Un attaquant ne commence jamais par vous attaquer : il commence par vous regarder. Avant le moindre paquet envoyé, il dresse la carte de tout ce que votre organisation expose sur Internet — domaines oubliés, serveurs de préproduction, panneaux d'administration, certificats, identifiants fuités. Cette carte, la plupart des PME et ETI ne l'ont jamais vue elles-mêmes. La gestion de la surface d'attaque externe (EASM, External Attack Surface Management) consiste précisément à découvrir, inventorier et surveiller en continu ces actifs exposés — pour les corriger avant qu'ils ne servent de porte d'entrée. Ce guide vous fait faire le tour de votre propre organisation avec les yeux d'un attaquant, puis vous donne la méthode pour reprendre le contrôle.

À retenir

- Votre surface d'attaque externe grossit en continu — cloud, shadow IT, sous-domaines, IT hérité — souvent sans décision consciente. Fin 2025, plus de 6 200 systèmes exposés en France restaient vulnérables à des failles connues depuis 2023-2024 (ANSSI/CERT-FR).
- Un attaquant commence par la reconnaissance : Certificate Transparency lui livre vos sous-domaines passivement, avant tout paquet envoyé. Tout service HTTPS est déjà répertorié publiquement.
- Les équipements de périmètre exposés (pare-feu, VPN) sont devenus une cible de choix : 22 % des compromissions par exploitation en 2025, environ huit fois plus qu'en 2024 (Verizon DBIR).
- Priorisez avec trois signaux complémentaires : CVSS (gravité), EPSS (probabilité à 30 jours), KEV CISA (exploitation confirmée). Une entrée KEV est une urgence factuelle, pas une hypothèse.
- La cartographie continue de la surface d'attaque devient un prérequis des obligations que prévoit NIS2 (directive non transposée en droit français à mi-2026) — et une première ligne de défense concrète pour les PME/ETI.

01 1. La surface d'attaque externe : ce qu'elle est, et pourquoi elle grossit sans vous

Votre surface d'attaque externe, c'est l'ensemble des actifs numériques que votre organisation expose sur Internet et qu'un tiers peut atteindre sans être déjà chez vous : noms de domaine et sous-domaines, adresses IP, ports et services ouverts, applications web, API, certificats TLS, portails d'accès distant. Chacun de ces points est une porte. Certaines sont verrouillées et à jour ; d'autres ont été ouvertes il y a des années et oubliées.

Le problème n'est pas seulement qu'elle existe : c'est qu'elle grossit en permanence, souvent sans décision consciente. Quatre moteurs l'expliquent.

- Le cloud et le SaaS : chaque nouvel environnement (préproduction, démo, outil métier hébergé) crée un actif exposé, parfois provisionné en quelques minutes par une équipe sans passer par l'IT.

- Le shadow IT : services souscrits directement par un métier, sous-domaines montés pour une campagne ponctuelle, dépôts de code publics — autant d'actifs que la DSI ne connaît pas.
- La prolifération des sous-domaines et des certificats : chaque service exposé génère généralement un certificat TLS public, traçable, qui trahit son existence (voir section 2).
- L'IT hérité : anciens serveurs, VPN d'un prestataire parti, applications non décommissionnées. Ils ne rapportent plus rien, mais restent joignables — et rarement patchés.

Le socle méthodologique : on ne protège pas ce qu'on ignore

Les CIS Controls v8 placent en Contrôle 1 (inventaire des actifs matériels) et Contrôle 2 (inventaire des logiciels) le fondement de toute la sécurité : on ne peut pas défendre des actifs dont on ignore l'existence. Un inventaire précis et tenu à jour est la condition préalable — non négociable — à toute réduction de la surface d'attaque. Source : Center for Internet Security, CIS Controls v8.

Cet angle mort a un coût mesurable. Fin 2025, plus de 6 200 systèmes exposés en France restaient vulnérables à des failles identifiées dès 2023 ou 2024 (ANSSI/CERT-FR, Panorama de la cybermenace 2025). Ce ne sont pas des failles inconnues : ce sont des failles connues, publiées, corrigeables — sur des actifs que personne ne surveillait plus.

02 2. La reconnaissance vue par l'attaquant

Avant toute intrusion, un attaquant investit dans la reconnaissance. L'objectif : cartographier votre exposition sans se faire remarquer, puis choisir la porte la plus faible. Comprendre ces techniques n'a rien d'offensif — c'est ce que fait tout défenseur sérieux pour se regarder de l'extérieur. Voici l'enchaînement typique, du plus passif au plus actif.

1 OSINT et empreinte publique

L'attaquant collecte l'information ouverte : votre site, vos mentions légales, vos offres d'emploi (qui révèlent votre stack technique), vos profils sociaux, vos communiqués. Objectif : comprendre votre organisation et deviner vos technologies. Aucune interaction avec vos systèmes, donc rien à détecter.

2 Énumération des sous-domaines via Certificate Transparency

C'est l'étape la plus sous-estimée. Les registres publics de Certificate Transparency (CT) enregistrent chaque certificat TLS émis, avec tous ses noms alternatifs (SAN). En interrogeant un service comme crt.sh, un attaquant énumère passivement vos sous-domaines — y compris serveurs de dev, staging, outils internes, VPN — souvent avant même d'envoyer le moindre paquet vers vous.

3 Scan de ports et de services

Sur les actifs identifiés, l'attaquant cartographie les ports ouverts et les services actifs : versions de serveurs web, bases de données exposées, VPN, RDP, panneaux d'administration. Chaque bannière de version se compare à des bases de vulnérabilités connues.

4 Recherche d'identifiants et de secrets fuités

L'attaquant croise votre nom de domaine avec les fuites de données publiques et les dépôts de code : mots de passe recyclés, clés d'API, tokens. Les secrets exposés sont une exposition majeure — Verizon a analysé plus de 441 000 secrets trouvés dans des dépôts git publics.

Dernière étape avant l'exploitation : repérer les interfaces d'administration accessibles (panneaux de login, consoles cloud) et les fichiers qui n'auraient jamais dû être servis publiquement — fichiers de configuration .env (contenant souvent des mots de passe de base de données), répertoires .git exposant tout le code source, sauvegardes oubliées.

Pourquoi Certificate Transparency change la donne

La CT a été conçue pour un bon usage : détecter les certificats frauduleux. Mais son effet de bord est qu'aucun service HTTPS n'est réellement « discret ». Créer un sous-domaine dev.exemple.fr avec un certificat, c'est le publier dans un registre mondial consultable par tous. Partez du principe que tout ce qui a un certificat est déjà connu de vos adversaires. Source : synthèses techniques Certificate Transparency (Pentest Factory / ReconShield).

94 jours

Délai médian de remédiation d'un secret ou identifiant fuité sur GitHub — près de trois mois pendant lesquels la porte reste ouverte.

Verizon 2025 DBIR

03 3. Les expositions les plus fréquentes et les plus dangereuses

Toutes les expositions ne se valent pas. Voici celles que l'on retrouve le plus souvent lors d'une découverte de surface d'attaque, avec leur impact concret. La colonne « impact » décrit ce qu'un attaquant peut en faire.

Exposition	Ce que c'est	Impact potentiel
Fichier .env exposé	Fichier de configuration servi publiquement	Fuite de mots de passe de base de données, clés d'API, secrets applicatifs — accès direct au cœur du système
Répertoire .git accessible	Dossier de gestion de version laissé public	Récupération de tout le code source, souvent avec des secrets en clair dans l'historique
Équipement de périmètre non patché	Pare-feu, concentrateur VPN, passerelle d'accès distant	Accès initial au réseau interne — devenu une cible privilégiée (voir stat ci-dessous)
Panneau d'administration exposé	Interface de login accessible depuis Internet	Attaques par force brute, réutilisation d'identifiants fuités, exploitation de failles
Sous-domaine oublié (staging, démo)	Actif de préproduction jamais décommissionné	Souvent moins protégé, code de test, données réelles, versions logicielles obsolètes
Service obsolète / version vulnérable	Serveur web ou composant non mis à jour	Exploitation d'une CVE connue, potentiellement déjà activement exploitée
Identifiants recyclés fuités	Mots de passe réutilisés apparus dans une fuite tierce	Connexion directe sans exploitation technique — l'abus d'identifiants est un vecteur majeur
Configuration email absente (SPF/DKIM/DMARC)	Domaine sans protection anti-usurpation	Usurpation de votre domaine pour du phishing ciblant clients et collaborateurs
Base de données ou stockage cloud ouvert	Bucket ou base sans authentification	Fuite massive de données, exposition directe sans exploitation

22 %

Part des compromissions par exploitation qui ont ciblé des équipements de périmètre exposés (pare-feu, VPN) en 2025 — soit environ huit fois plus que l'année précédente (3 %).

Verizon 2025 DBIR

La bordure du réseau est devenue la ligne de front

Le bond des équipements de périmètre comme cible n'est pas un hasard : ce sont des actifs exposés en permanence, difficiles à patcher rapidement, et qui donnent un accès direct au réseau. C'est exactement le type d'actif qu'un inventaire EASM continu permet de repérer avant l'attaquant.

04 4. Reprendre le contrôle : de l'inventaire à la remédiation priorisée

Reprendre la main sur sa surface d'attaque n'est pas un projet ponctuel : c'est un cycle continu. La surface bouge chaque semaine ; un audit annuel photographie un instant déjà périmé. Quatre étapes structurent la démarche.

- 1

Inventaire continu

Découvrir automatiquement tous les actifs exposés — domaines, sous-domaines, IP, services, certificats — et les tenir à jour. C'est le socle : les CIS Controls v8 en font le Contrôle 1. L'objectif est de ne plus avoir d'angle mort, notamment sur le shadow IT et l'IT hérité.
- 2

Monitoring des changements

Détecter en continu ce qui apparaît, disparaît ou change : nouveau sous-domaine, port qui s'ouvre, certificat émis, service dont la version devient vulnérable. Un nouvel actif non prévu doit déclencher une vérification.
- 3

Priorisation par criticité réelle

Toutes les vulnérabilités ne méritent pas la même urgence. Avec près de 50 000 CVE publiées en 2025 (CVE Program / NVD), corriger « tout » est impossible. La priorisation croise trois signaux complémentaires (voir tableau ci-dessous) pour concentrer l'effort là où le risque est réel.
- 4

Remédiation et suivi

Corriger, décommissionner l'inutile, fermer l'exposition — puis vérifier que la correction tient dans le temps. La remédiation n'est close que lorsque le prochain scan le confirme.

Signal	Ce qu'il mesure	Ce qu'il ne dit pas
CVSS	La sévérité technique de la faille (gravité intrinsèque)	Si elle est réellement exploitée ou exploitable dans votre contexte
EPSS (FIRST)	La probabilité qu'une CVE soit exploitée dans les 30 jours (modèle mis à jour quotidiennement, version 4 depuis mars 2025)	Une certitude : c'est une estimation probabiliste, qui évolue jour après jour
KEV (CISA)	L'exploitation active confirmée et observée sur le terrain (245 entrées ajoutées en 2025, dont 24 liées à des rançongiciels)	La gravité technique ni la probabilité — c'est un constat, pas une prédiction

La bonne lecture : trois signaux complémentaires, jamais interchangeables

CVSS dit la gravité, EPSS la probabilité d'exploitation à 30 jours, KEV l'exploitation confirmée. Une faille présente au catalogue KEV de la CISA est une urgence absolue : son exploitation est un fait, pas une hypothèse. Ne présentez jamais un score EPSS élevé comme une certitude — c'est une probabilité qui aide à trier, pas un verdict.

05 5. EASM et NIS2 : anticiper une directive non transposée

La directive européenne NIS2 impose aux entités concernées des mesures de gestion des risques, incluant explicitement le traitement et la divulgation des vulnérabilités. Or on ne peut pas gérer les vulnérabilités d'actifs qu'on ne connaît pas : la cartographie continue de la surface d'attaque externe devient, de fait, un prérequis.

Point de vigilance juridique : NIS2 n'est pas encore transposée en droit français

À mi-2026, la transposition française n'est pas finalisée. Le projet de loi « résilience » a été adopté par le Sénat le 12 mars 2025, mais il n'est ni adopté définitivement ni promulgué. Il ne s'agit donc pas d'une réglementation déjà en vigueur en France. Vérifiez le statut exact sur Legifrance avant tout engagement. Source : ANSSI — cyber.gouv.fr.

En complément, l'ANSSI a publié (en 2026, selon les sources spécialisées à recouper sur cyber.gouv.fr) le Référentiel Cyber de France (ReCyF), qui liste les mesures recommandées pour atteindre les objectifs de NIS2 — dont la gestion des vulnérabilités et la réduction de l'exposition. Ce référentiel est non contraignant par défaut, mais peut être invoqué par l'ANSSI en cas de contrôle si l'entité a choisi de l'appliquer. À traiter comme un cadre de mesures recommandées, non comme une obligation.

L'enjeu dépasse la conformité. À l'échelle de l'UE, l'ENISA a analysé 4 875 incidents entre juillet 2024 et juin 2025 : l'exploitation de vulnérabilités a représenté 21,3 % des vecteurs d'accès initial, et une large majorité des plus de 42 595 vulnérabilités divulguées sur la période étaient exploitables à distance via le réseau — donc contre des actifs exposés. C'est précisément le périmètre de l'EASM. (Chiffres UE, non spécifiques à la France ni aux PME.)

La cible PME/ETI est directement concernée

En France, 48 % des victimes de rançongiciels traitées par l'ANSSI en 2025 étaient de petites structures (TPE/PME/ETI) — la catégorie la plus touchée. Réduire son exposition externe n'est pas un luxe de grand compte : c'est la première ligne de défense pour une PME. Source : ANSSI/CERT-FR, Panorama de la cybermenace 2025.

06 6. Ce que Sedona Radar automatise

Faire manuellement tout ce que ce guide décrit — énumérer les sous-domaines, scanner les services, chasser les .env et les secrets, rapprocher chaque version des vulnérabilités connues — demande du temps et une expertise rare. Sedona Radar automatise ce travail à intervalles réguliers (mensuels à hebdomadaires selon le plan), pour les PME et ETI françaises.

- Découverte et inventaire de votre surface d'attaque externe : domaines, sous-domaines (Deep Scan, dont via Certificate Transparency), IP, ports, services, certificats.
- Détection des expositions à risque : fichiers sensibles exposés (.env, .git), panneaux d'administration, services obsolètes, absence de protections email.
- Classement des vulnérabilités par gravité, avec des conseils de correction.

- Indicateurs de maturité sur 6 référentiels : NIS2, RGPD, ISO 27001, ANSSI Hygiène, OWASP Top 10 et Cadre Sedona (grille propre à Sedona, qui n'est pas un référentiel de l'ANSSI).
- Scans opérés depuis Gravelines (OVH, France) ; données stockées dans l'Union européenne (Supabase, Irlande).

En toute honnêteté : Radar évalue, il ne certifie pas

Sedona Radar donne des indicateurs de maturité (NIS2, RGPD, ISO 27001, ANSSI Hygiène, OWASP Top 10, Cadre Sedona). Il ne délivre aucune certification : il n'existe aucune certification NIS2. Si un texte ou un client exige un audit par un prestataire qualifié PASSI, adressez-vous à l'un des prestataires de la liste publiée par l'ANSSI. Sedona.AI n'est ni qualifiée PASSI ni certifiée ISO 27001. Le scoring Radar est un outil de pilotage, pas un label réglementaire.

Sedona Radar est disponible dès 79 € HT/mois (plan Starter). Le plan Discovery, gratuit, permet un premier Scan de Contrôle de votre domaine, pour voir concrètement ce qu'un attaquant en voit.

§ Sources

1. Verizon 2025 Data Breach Investigations Report (DBIR) — <https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf>
2. ANSSI/CERT-FR — Panorama de la cybermenace 2025 (CERTFR-2026-CTI-002) — <https://www.cert.ssi.gouv.fr/uploads/CERTFR-2026-CTI-002.pdf>
3. ENISA — Threat Landscape 2025 — <https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025%20Booklet.pdf>
4. FIRST — EPSS (Exploit Prediction Scoring System) — <https://www.first.org/epss/>
5. CISA — Known Exploited Vulnerabilities (KEV) Catalog — <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
6. Center for Internet Security — CIS Controls v8 — <https://www.cisecurity.org/controls/cis-controls-list>
7. ANSSI — cyber.gouv.fr (directive NIS2 et ReCyF) — <https://cyber.gouv.fr/en/regulations/the-nis-2-directive/>
8. Certificate Transparency — synthèse technique (Pentest Factory / ReconShield) — <https://www.pentestfactory.de/en/subdomains-under-the-hood-ssl-transparency-logs/>
9. Cyberwatch — EASM (synthèse marché) — <https://cyberwatch.fr/actualite/easm-external-attack-surface-management/>

Voyez ce qu'un attaquant voit de votre organisation

Sedona Radar analyse ce que votre domaine expose sur Internet et remet un rapport en français, avec un plan de correction. Le plan Discovery est gratuit : un premier Scan de Contrôle de votre domaine, sans exploration des sous-domaines. Le plan Starter, dès 79 € HT/mois, ajoute le détail des failles et un rapport PDF. Données stockées dans l'Union européenne.

Lancer mon scan gratuit

sedona-ai.com/scan-gratuit