

LIVRE BLANC

Surface d'attaque externe : le guide

Voir votre organisation comme un attaquant : cartographier, prioriser et réduire votre surface d'attaque externe, du premier scan à la remédiation.

Sedona Radar — audit de sécurité externe automatisé

Sedona AI Lecture ~25 min Édition 2026 sedona-ai.com

Sommaire

01	1. Pourquoi ce livre blanc, et pour qui
02	2. La surface d'attaque externe expliquée simplement
03	3. Actifs oubliés, shadow IT et l'angle mort du périmètre
04	4. Sous-domaines, ports, certificats et fuites : le détail des signaux
05	5. Dans la tête de l'attaquant : pourquoi tout commence par la reconnaissance
06	6. Panorama chiffré 2024-2026 : ce que disent les données
07	7. L'argument économique : combien coûte une exposition qui dure
08	8. Le temps qui joue contre vous : Time-to-Exploit et CVE
09	9. Phishing, usurpation et messagerie : la surface humaine et e-mail
10	10. Ancrage France et Europe : ENISA et ANSSI
11	11. Cadre réglementaire : NIS2, RGPD et attentes ANSSI
12	12. EASM : définition, périmètre et différence avec le pentest
13	13. Le cadre CTEM de Gartner en 5 étapes
14	14. Méthode — Étape 1 : Découverte et cartographie
15	15. Méthode — Étape 2 : Inventaire et attribution
16	16. Méthode — Étape 3 : Priorisation par risque et exploitabilité
17	17. Méthode — Étape 4 : Remédiation et réduction de surface
18	18. Méthode — Étape 5 : Surveillance continue et validation
19	19. Hygiène essentielle : SPF/DKIM/DMARC, TLS, CVE, MFA
20	20. Spécificités PME et ETI : faire beaucoup avec peu
21	21. Les 10 erreurs fréquentes qui laissent la porte ouverte
22	22. Checklist opérationnelle et modèles à réutiliser

Ce que votre organisation expose sur Internet est exactement ce que l'attaquant voit en premier — et il commence presque toujours par là. En 2024-2026, les données convergent : l'exploitation de vulnérabilités exposées est devenue le premier ou le deuxième vecteur d'accès initial, le délai d'exploitation des vulnérabilités s'est effondré (médiane de quelques jours, et une majorité de failles désormais exploitées en zero-day, avant tout correctif), et de nombreuses organisations sont attaquées via des actifs qu'elles ne savaient même pas posséder. Ce livre blanc vulgarise la notion de surface d'attaque externe, la documente par des chiffres sourcés, et propose une méthode pas-à-pas actionnable — de la découverte à la remédiation. Objectif : vous faire passer de « on pense être à jour » à « on sait ce qu'on expose, on l'a priorisé et on le réduit en continu ».

À retenir

- La surface d'attaque externe (domaines, IP, ports, mail, TLS, dépôts publics, secrets fuités) est le premier terrain de reconnaissance des attaquants — et le plus mal cartographié.
- L'exploitation de vulnérabilités exposées est le 1er vecteur d'accès initial chez Mandiant (33 %) et en forte hausse chez Verizon (20 %, +34 % sur un an).
- Le temps joue contre vous : le délai médian d'exploitation est tombé à quelques jours et la majorité des failles sont désormais exploitées en zero-day (souvent avant le correctif), alors que la remédiation reste lente.
- La surface bouge en permanence : environ 300 nouveaux services exposés apparaissent chaque mois par organisation ; un scan annuel ne suffit plus.
- La bonne priorisation ne se fait pas au score CVSS seul, mais en tenant compte de l'exploitation constatée (catalogue CISA KEV, EPSS), croisée à la criticité métier de l'actif.
- NIS2 doit étendre l'obligation de maîtrise du risque cyber à environ 15 000 entités en France (estimation de l'étude d'impact du projet de loi, octobre 2024), mais le texte de transposition n'est pas promulgué : gérer sa surface d'attaque aide dès maintenant à s'y préparer.
- Une démarche continue (EASM alimentant le cycle CTEM de Gartner) est associée à un risque de brèche divisé par trois à horizon 2026.

01 1. Pourquoi ce livre blanc, et pour qui

Ce document s'adresse aux dirigeants, DSI et RSSI de PME et d'ETI qui veulent comprendre, mesurer et réduire ce que leur organisation expose sur Internet. Le postulat de départ est simple : un attaquant ne voit pas votre organigramme, vos politiques internes ni vos intentions. Il voit une surface — un ensemble de portes et de fenêtres accessibles depuis le réseau public. Cette surface est la première chose qu'il cartographie, et bien souvent la dernière chose que vous surveillez.

Nous vulgarisons ici deux notions clés du marché : l'EASM (External Attack Surface Management, ou gestion de la surface d'attaque externe) et le cadre CTEM de Gartner (Continuous Threat Exposure Management, gestion continue de l'exposition aux menaces). L'un décrit l'outillage de visibilité, l'autre la démarche de bout en bout. Les deux répondent à la même réalité : la sécurité ne se joue plus à l'audit annuel, mais dans un cycle continu de découverte, priorisation, validation et remédiation.

Posture d'honnêteté

Ce livre blanc parle d'évaluation de l'exposition, jamais de certification de conformité. Aucun outil, y compris Sedona Radar, ne rend une organisation « conforme » à lui seul. La maîtrise de la surface d'attaque aide à répondre aux exigences (NIS2, RGPD, attentes ANSSI), mais la conformité reste une décision d'organisation, documentée et auditée.

02 2. La surface d'attaque externe expliquée simplement

La surface d'attaque externe, c'est l'ensemble des points de contact de votre organisation accessibles depuis Internet sans être un utilisateur interne authentifié. Autrement dit : tout ce qu'un inconnu, depuis n'importe quel navigateur ou outil de scan, peut atteindre, interroger ou tester. Plus cette surface est large et mal connue, plus la probabilité qu'un maillon faible existe augmente.

Une analogie utile : imaginez votre organisation comme un bâtiment vu depuis la rue. La surface d'attaque externe, ce sont les portes d'entrée, les fenêtres du rez-de-chaussée, la porte de service qu'on a oublié de verrouiller, le badge tombé sur le trottoir et le plan du bâtiment affiché sur la vitrine. L'attaquant fait le tour, note tout, et revient par le point le plus faible.

- Domaines et sous-domaines (site principal, campagnes marketing, environnements de test, portails partenaires)
- Adresses IP et plages réseau publiques
- Ports ouverts et services associés (web, mail, accès distant, bases de données)
- Serveurs de messagerie et enregistrements d'authentification e-mail (SPF, DKIM, DMARC)
- Certificats TLS (validité, robustesse, expiration)
- Applications web et API exposées
- Dépôts de code publics et secrets qui y traînent (clés, mots de passe, jetons)
- Espaces de stockage cloud mal configurés (buckets ouverts, partages publics)

La règle mentale à retenir

On ne protège que ce que l'on connaît. Chaque actif exposé et non inventorié est un angle mort : ni patché, ni surveillé, ni attribué à un propriétaire. La première victoire de sécurité n'est pas un pare-feu, c'est une cartographie honnête.

03 3. Actifs oubliés, shadow IT et l'angle mort du périmètre

La surface d'attaque n'est jamais statique et échappe structurellement au contrôle central. Un site de campagne mis en ligne pour un événement puis oublié, un environnement de préproduction laissé accessible, un service SaaS souscrit par une équipe métier sans passer par la DSI, un sous-domaine pointant vers un service désactivé (fenêtre ouverte à un détournement, ou takeover) : autant d'actifs vivants que personne ne surveille.

~300

nouveaux services exposés apparaissent chaque mois sur la surface d'attaque d'une organisation ; plus d'un quart des expositions touchent des infrastructures IT ou de sécurité critiques.

Unit 42 (Palo Alto Networks), Attack Surface Threat Research, 2024

Ce chiffre change la façon de penser la sécurité : si environ 300 services apparaissent chaque mois, la question n'est pas « ai-je terminé mon inventaire ? » mais « à quelle fréquence mon inventaire se re-fait-il tout seul ? ». Le shadow IT n'est pas une faute morale, c'est une conséquence mécanique de la vitesse à laquelle une organisation déploie du numérique.

Le coût de ce qu'on ne voit pas

Un actif inconnu cumule tous les risques : il n'est pas patché, pas monitoré, souvent pas chiffré correctement, et personne ne sait qu'il faut le décommissionner. C'est précisément sur ces actifs fantômes que se concentrent les attaques par actifs mal gérés — l'attaquant, lui, les a trouvés.

04 4. Sous-domaines, ports, certificats et fuites : le détail des signaux

Chaque type d'actif produit des signaux d'exposition qu'un attaquant sait lire — et que vous devez apprendre à lire avant lui. Voici la grille de lecture des principaux signaux, du risque associé et d'un exemple concret.

Signal d'exposition	Risque principal	Exemple concret
Sous-domaine énumérable	Découverte d'actifs oubliés, détournement (takeover)	test.exemple.fr laissé actif après un projet clos
Port / service sensible ouvert	Accès distant ou base de données exposée	RDP, SSH, VNC ou une base de données joignable depuis Internet
Certificat TLS expiré ou faible	Interception, perte de confiance, alerte navigateur	Certificat périmé ou protocole de chiffrement obsolète accepté
Authentification e-mail incomplète	Usurpation de domaine, phishing au nom de l'entreprise	DMARC absent ou en p=none, sans protection réelle
Secret / identifiant fuité	Accès direct, contournement de l'authentification	Clé d'API ou mot de passe dans un dépôt de code public
Stockage cloud ouvert	Fuite de données massive	Bucket ou partage rendu public par erreur de configuration

x8

l'exploitation de failles visant les équipements de périphérie et VPN a été multipliée par près de huit (de 3 % à 22 % des exploitations de vulnérabilités).

Verizon, 2025 Data Breach Investigations Report

Ce dernier chiffre est un signal d'alarme spécifique : les équipements de périphérie (pare-feu, passerelles VPN, concentrateurs d'accès distant) sont par nature exposés et concentrent désormais une part majeure de l'exploitation active. Ce sont souvent des actifs « qu'on installe et qu'on oublie » — exactement le type de brique à surveiller en priorité.

05 5. Dans la tête de l'attaquant : pourquoi tout commence par la reconnaissance

Aucune attaque sérieuse ne démarre par l'exploitation. Elle démarre par la reconnaissance : cartographier la cible, identifier ses actifs, repérer le maillon faible. Le référentiel MITRE ATT&CK formalise cette phase sous la tactique Reconnaissance (TA0043), qui regroupe le scan actif (T1595), la collecte d'informations sur les hôtes (T1592) et la collecte d'informations d'identité. C'est la première case de toute chaîne d'attaque (kill chain).

1 Reconnaissance passive (OSINT)

L'attaquant collecte sans jamais toucher votre infrastructure : moteurs de recherche d'exposition, journaux de certificats, enregistrements DNS, dépôts publics, fuites de données. Silencieux, indétectable de votre côté.

2 Reconnaissance active (scan)

Il interroge directement vos actifs : quels ports sont ouverts, quels services tournent, quelles versions, quels certificats. C'est ici qu'il constitue sa carte des portes et fenêtres.

3 Sélection du maillon faible

Il croise ce qu'il a trouvé avec ce qu'il sait exploiter (vulnérabilités connues, secrets fuités, service mal configuré) et choisit le point d'entrée au meilleur rapport effort/gain.

4 Exploitation

Il n'attaque que ce qu'il a déjà validé comme faisable. La reconnaissance a rentabilisé l'exploitation.

Le renversement de perspective

L'EASM consiste à faire, avant l'attaquant, exactement le travail de reconnaissance qu'il fera contre vous — puis à corriger ce que ce travail révèle. Voir son organisation comme un attaquant n'est pas une posture, c'est une méthode.

06 6. Panorama chiffré 2024-2026 : ce que disent les données

Passons des principes aux faits. Les grands rapports annuels 2024-2026 (Verizon, Mandiant, IBM, ENISA, ANSSI) dressent un tableau cohérent : l'accès initial se joue de plus en plus sur l'exposition et l'identité, moins sur le malware sophistiqué.

33 %

des intrusions démarrent par l'exploitation d'une vulnérabilité — 1er vecteur d'accès initial pour la 5e année consécutive.

Google Cloud / Mandiant, M-Trends 2025

20 %

des brèches impliquent l'exploitation d'une vulnérabilité comme vecteur d'accès initial, en hausse de 34 % sur un an.

Verizon, 2025 Data Breach Investigations Report

22 %

des brèches partent d'un abus d'identifiants et 16 % du phishing — les portes d'entrée dominantes restent l'accès, pas le malware sophistiqué.

Verizon, 2025 Data Breach Investigations Report

~50 %

des accès initiaux se ramènent à une vulnérabilité exploitée (33 %) ou à des identifiants volés (16 %) : l'exposition technique et le vol d'identifiants dominent l'accès initial.

Google Cloud / Mandiant, M-Trends 2025

L'écart apparent entre les 33 % de Mandiant et les 20 % de Verizon tient aux périmètres et méthodologies (Mandiant observe des intrusions gérées en réponse à incident, Verizon un large échantillon de brèches multi-secteurs). Les deux racontent la même histoire : l'exposition technique et le vol d'identifiants dominent l'accès initial.

30 %

des brèches impliquent désormais un tiers ou partenaire, soit le double de l'année précédente — la surface d'attaque s'étend à tout l'écosystème.

Verizon, communiqué 2025 DBIR

07 7. L'argument économique : combien coûte une exposition qui dure

Une surface mal maîtrisée ne coûte pas qu'en risque abstrait : elle coûte en euros et en temps. Plus une exposition dure sans être détectée, plus la facture grimpe.

4,44 M\$

coût moyen mondial d'une violation de données (-9 % vs 2024), la baisse tenant surtout à une détection plus rapide via l'IA et l'automatisation.

IBM, Cost of a Data Breach Report 2025

241 jours

délai moyen pour identifier puis contenir une brèche — chaque jour d'exposition non détectée alourdit la note.

IBM, Cost of a Data Breach Report 2025

Le message de fond du rapport IBM est directement actionnable : la baisse du coût moyen s'explique surtout par une détection et un confinement plus rapides. Autrement dit, ce qui fait baisser la facture, ce n'est pas d'avoir zéro exposition (impossible), c'est de raccourcir le temps entre l'apparition d'une

exposition et sa neutralisation. C'est exactement l'objet de la gestion de la surface d'attaque externe (EASM) : voir son exposition, puis la réduire.

À traduire au comité de direction

L'investissement en visibilité continue ne se justifie pas par la peur, mais par le levier : réduire le délai de détection agit directement sur le coût moyen d'un incident. C'est un argument financier, pas seulement technique.

08 8. Le temps qui joue contre vous : Time-to-Exploit et CVE

La donnée la plus contre-intuitive de la période récente concerne le délai d'exploitation (Time-to-Exploit) : le temps entre la publication d'une vulnérabilité et sa première exploitation observée. Ce délai s'est effondré à quelques jours, et la majorité des vulnérabilités exploitées le sont désormais en zero-day — avant ou au moment de la divulgation, souvent avant tout correctif.

5 jours

délai moyen d'exploitation d'une vulnérabilité en 2023 (contre 63 jours en 2018-2019) ; la majorité des failles exploitées cette année-là l'ont été en zero-day (97 sur 138), avant tout correctif.

Google Cloud / Mandiant, Time-to-Exploit Trends

1 484

vulnérabilités activement exploitées répertoriées au catalogue CISA KEV fin 2025 (+20 % sur l'année) — la vraie file d'attente des correctifs prioritaires.

CISA, Known Exploited Vulnerabilities Catalog, 2025

La conséquence méthodologique est majeure : puisqu'on ne peut plus compter sur une fenêtre confortable entre divulgation et exploitation, la priorisation ne peut plus se faire au seul score de gravité théorique (CVSS). Il faut prioriser en fonction de l'exploitation constatée — une vulnérabilité activement exploitée dans la nature (présente au catalogue CISA KEV, ou avec un score de probabilité d'exploitation EPSS élevé) passe avant une vulnérabilité au CVSS élevé mais jamais exploitée.

Le piège du CVSS seul

Traiter d'abord toutes les vulnérabilités « critiques » au sens CVSS revient à noyer les équipes sous des centaines de tickets sans lien avec la menace réelle. Le catalogue KEV et l'EPSS existent précisément pour recentrer l'effort sur ce qui est exploité aujourd'hui.

09 9. Phishing, usurpation et messagerie : la surface humaine et e-mail

La surface d'attaque n'est pas que technique : votre nom de domaine lui-même est un actif exposé, exploitable pour usurper votre identité. Le phishing reste le premier vecteur d'intrusion, et il s'appuie très souvent sur une faiblesse d'authentification e-mail côté domaine légitime.

60 %

des intrusions réussies en Europe reposent sur le phishing, premier vecteur devant l'exploitation de vulnérabilités (21,3 %).

ENISA, Threat Landscape 2025

Trois enregistrements DNS conditionnent la capacité d'un attaquant à envoyer des e-mails frauduleux au nom de votre domaine : SPF (qui a le droit d'émettre), DKIM (signature cryptographique des messages) et DMARC (politique appliquée en cas d'échec, et rapports). Le point critique est la politique DMARC : publier un enregistrement DMARC en mode `p=none` informe mais ne protège pas — les messages usurpés passent quand même.

L'illusion du DMARC déclaré

Selon le 2026 State of DMARC Report de Valimail, l'adoption de DMARC progresse fortement, mais une majorité de domaines restent bloqués en `p=none` — c'est-à-dire sans protection réelle contre l'usurpation. Déclarer DMARC n'est pas se protéger : il faut passer en quarantaine puis reject, après une phase d'observation des rapports.

10 10. Ancrage France et Europe : ENISA et ANSSI

Les tendances mondiales se déclinent au niveau européen et français, avec des nuances importantes pour une PME ou ETI locale. L'industrialisation du cybercrime, notamment le rançongiciel-as-a-service (RaaS), cible désormais explicitement les organisations de taille intermédiaire, jadis considérées trop petites pour intéresser les attaquants.

4 875

incidents analysés par l'ENISA sur un an (juillet 2024 – juin 2025), l'administration publique étant le secteur le plus ciblé (38,2 %).

ENISA, Threat Landscape 2025

1 366

incidents de sécurité traités par l'ANSSI en 2025, concentrés sur éducation et recherche (34 %), collectivités et ministères (24 %) et santé (10 %).

ANSSI, Panorama de la cybermenace 2025

+51 %

d'incidents d'exfiltration de données signalés en France (196 cas contre 130), signe d'un basculement du chiffrage vers le vol et le chantage de données.

ANSSI / CERT-FR, Panorama de la cybermenace 2025

Ce dernier chiffre marque un tournant stratégique : les attaquants ne se contentent plus de chiffrer pour rançonner, ils exfiltrent pour faire chanter. Or l'exfiltration commence par un accès, et l'accès commence par une exposition. Réduire sa surface externe agit donc en amont d'une menace qui vise désormais directement la donnée.

11. Cadre réglementaire : NIS2, RGPD et attentes ANSSI

La maîtrise de l'exposition n'est plus seulement une bonne pratique : elle devient une attente réglementaire. La directive européenne NIS2 (Directive (UE) 2022/2555) prévoit, pour les entités concernées, des obligations de gestion des risques cyber, des mesures d'hygiène et une notification d'incidents. Elle n'est pas transposée en droit français au 14/10/2026 ; sa transposition doit élargir massivement le périmètre des entités couvertes.

~15 000

entités qui seront concernées par NIS2 en France (estimation), contre environ 500 sous NIS1 ; la loi de transposition n'est pas promulguée.

Étude d'impact du projet de loi de transposition de NIS2, octobre 2024

- Une analyse des risques et une politique de sécurité des systèmes d'information
- Des mesures d'hygiène de base (gestion des vulnérabilités, contrôle d'accès, chiffrage)
- La gestion des incidents et leur notification aux autorités dans des délais courts
- La prise en compte de la sécurité de la chaîne d'approvisionnement (fournisseurs et tiers)
- Une responsabilisation des organes de direction sur le risque cyber

En parallèle, le RGPD impose, en cas de violation de données personnelles, une notification à la CNIL sous 72 heures. Le lien avec la surface d'attaque est direct : une exposition technique non maîtrisée est le point de départ de la plupart des fuites de données personnelles à déclarer.

Précision d'honnêteté

Gérer sa surface d'attaque aide à répondre aux exigences de NIS2 et du RGPD, mais aucun outil ne rend « conforme » à lui seul. La conformité est un dispositif d'organisation, de gouvernance et de preuve, dont l'évaluation continue de l'exposition n'est qu'une brique.

12. EASM : définition, périmètre et différence avec le pentest

L'EASM (External Attack Surface Management) est la découverte et la surveillance continues du périmètre exposé sur Internet, du point de vue de l'attaquant. Son objet propre est la visibilité : trouver tout ce qui est exposé — y compris ce que vous ignoriez posséder — puis suivre l'évolution de cette exposition dans le temps.

Approche	Point de vue	Fréquence	Objet
EASM	Externe, comme l'attaquant	Continue	Découvrir et surveiller tout le périmètre exposé
Scan de vulnérabilités interne	Interne, sur actifs connus	Périodique	Détecter les failles sur un inventaire déjà connu
Pentest / audit ponctuel	Externe ou interne, ciblé	Ponctuel	Éprouver en profondeur un périmètre défini à une date

La distinction est essentielle : un pentest est une plongée profonde sur un périmètre défini à un instant t — précieux, mais photographique. L'EASM est un film : il capte le mouvement permanent de la surface. Les deux sont complémentaires. L'EASM dit « voici tout ce que vous exposez et ce qui a changé cette semaine » ; le pentest dit « voici jusqu'où on peut aller sur ce périmètre précis ».

Le bon réflexe

Ne pas opposer EASM et pentest, mais les enchaîner : l'EASM alimente le pentest en révélant les actifs à éprouver, et le pentest valide en profondeur ce que l'EASM a priorisé.

13. Le cadre CTEM de Gartner en 5 étapes

Gartner a formalisé la démarche continue sous le nom de CTEM (Continuous Threat Exposure Management, gestion continue de l'exposition aux menaces). L'idée directrice : cesser de gérer la sécurité par épisodes (un audit, une alerte, un incident) pour la piloter comme un programme cyclique et permanent. L'EASM alimente naturellement les étapes de découverte et de priorisation.

- 1

1. Scoping (cadrage)
Définir le périmètre qui compte pour le métier : quels actifs, quels services, quels risques sont réellement en jeu.
- 2

2. Discovery (découverte)
Identifier tous les actifs exposés et leurs vulnérabilités — c'est le cœur de l'EASM.
- 3

3. Prioritization (priorisation)
Hiérarchiser selon l'exploitation constatée et la criticité métier, pas par volume ni par CVSS seul.

4. Validation

Vérifier que les expositions prioritaires sont réellement exploitables et que les défenses tiennent.

5. Mobilization (mobilisation)

Mettre l'organisation en mouvement : attribuer, remédier, mesurer, recommencer.

3x

moins de risque de subir une brèche pour les organisations pilotant leurs investissements via un programme CTEM, selon la prédiction Gartner à horizon 2026.

Gartner, Continuous Threat Exposure Management (horizon 2026)

Le cadre méthodologique de fond, côté normatif, est le NIST Cybersecurity Framework 2.0, structuré autour des fonctions Govern, Identify, Protect, Detect, Respond et Recover. La fonction Identify — inventaire des actifs et gestion de l'exposition — est précisément celle que l'EASM outille.

14. Méthode — Étape 1 : Découverte et cartographie

Place à la méthode. La première étape est la découverte : partir de ce que vous savez posséder (vos domaines racines) pour remonter tout ce qui y est rattaché, y compris l'inconnu. L'objectif n'est pas d'être rapide, c'est d'être exhaustif — puis de rendre cette découverte continue.

1. Partir des domaines racines

Lister l'ensemble des noms de domaine détenus par l'organisation, marques et filiales comprises.

2. Énumérer les sous-domaines

Découvrir tous les sous-domaines actifs, y compris ceux issus de campagnes, tests ou projets clos.

3. Cartographier IP, ports et services

Identifier les adresses IP publiques, les ports ouverts et les services qui écoutent derrière.

4. Inventorier certificats et messagerie

Relever les certificats TLS (validité, robustesse) et l'état de l'authentification e-mail (SPF, DKIM, DMARC).

5. Étendre au cloud et aux moteurs d'exposition

Chercher les actifs cloud (stockages, services managés) et la présence sur les moteurs de recherche d'exposition qu'utilisent aussi les attaquants.

L'exhaustivité, pas la vitesse

Une cartographie qui ignore un seul sous-domaine oublié laisse ouverte la porte que l'attaquant cherchait. Et parce que la surface bouge (environ 300 nouveaux services par mois et par organisation), une découverte ponctuelle périclète vite : la découverte doit être répétée en continu.

Livrable de cette étape : une cartographie d'exposition — la liste vivante de tout ce que votre organisation présente à Internet, mise à jour régulièrement.

15. Méthode — Étape 2 : Inventaire et attribution

Une cartographie brute ne suffit pas : il faut la transformer en inventaire exploitable. Chaque actif découvert doit être rattaché à un propriétaire, un usage, une criticité métier et un statut. C'est le pont entre la technique et la gouvernance, et c'est exactement la fonction Identify du NIST CSF 2.0.

Champ du registre	Ce qu'il documente
Actif	Domaine, IP, service ou certificat identifié
Propriétaire	Équipe ou personne responsable de l'actif
Usage	Fonction métier réelle (production, test, marketing, partenaire)
Criticité métier	Impact d'une compromission sur l'activité
Statut	Légitime, shadow IT à régulariser, ou obsolète à décommissionner
Date de découverte	Pour suivre l'apparition et l'âge des actifs

La question qui débloque tout

Pour chaque actif exposé, posez : « qui en est responsable, et doit-il vraiment être exposé ? ». Un actif sans propriétaire clair est soit à attribuer, soit à décommissionner. Il n'y a pas de troisième option acceptable.

16. Méthode — Étape 3 : Priorisation par risque et exploitabilité

Vous ne corrigerez pas tout en même temps — et ce n'est pas nécessaire. La priorisation consiste à croiser trois dimensions : la criticité de l'actif (que se passe-t-il s'il tombe ?), le niveau d'exposition (service sensible ouvert, secret fuité), et la probabilité que la faille soit exploitée.

- Présence de la vulnérabilité au catalogue CISA KEV (exploitée dans la nature)
- Score EPSS élevé (probabilité d'exploitation à court terme)
- Existence publique d'un code d'exploitation
- Secret ou identifiant déjà fuité pour cet actif
- Exposition d'un service d'accès distant ou d'une base de données

Exploitabilité	Actif critique	Actif secondaire
Élevée (KEV / EPSS haut)	Priorité 1 — immédiate	Priorité 2 — rapide
Faible ou théorique	Priorité 2 — planifiée	Priorité 3 — backlog

Pourquoi ne pas trier au CVSS seul

Le CVSS mesure une gravité théorique, pas la probabilité qu'une faille soit exploitée chez vous. Avec un délai d'exploitation tombé à quelques jours et 1 484 vulnérabilités activement exploitées au catalogue KEV, l'exploitation constatée est le meilleur filtre pour concentrer l'effort là où la menace est concrète.

17. Méthode — Étape 4 : Remédiation et réduction de surface

La priorisation débouche sur l'action. La remédiation combine deux logiques : corriger ce qui doit rester exposé, et réduire la surface en supprimant ce qui n'a pas à l'être. Réduire la surface est souvent plus efficace que patcher : un actif décommissionné ne se re-vulnérabilise jamais.

- ☐ Corriger et patcher les vulnérabilités exploitables prioritaires
- ☐ Fermer les ports et services inutiles exposés sur Internet
- ☐ Décommissionner les actifs oubliés, de test ou obsolètes
- ☐ Renforcer TLS et renouveler les certificats faibles ou expirés
- ☐ Passer l'authentification e-mail en enforcement (DMARC en quarantaine puis reject)
- ☐ Généraliser l'authentification multifacteur (MFA), en priorité sur les accès distants
- ☐ Révoquer et tourner (renouveler) tous les secrets et identifiants fuités

Horizon	Objectif de remédiation
30 jours	Traiter les expositions critiques exploitables et les secrets fuités ; fermer les accès distants non protégés
60 jours	Décommissionner les actifs orphelins, renforcer TLS et l'authentification e-mail
90 jours	Généraliser le MFA, régulariser le shadow IT, mettre en place le suivi continu

Commencer par les quick wins

Fermer un port d'administration exposé, révoquer une clé fuitée ou décommissionner un environnement de test abandonné coûte peu et retire immédiatement des cibles de grande valeur à l'attaquant. Ces gains rapides financent la crédibilité du programme auprès de la direction.

18. Méthode — Étape 5 : Surveillance continue et validation

La cinquième étape est celle qui distingue un programme d'un projet. La surface bouge chaque semaine : nouveaux services, nouveaux sous-domaines, nouvelles vulnérabilités publiées. Un scan annuel photographie un état déjà périmé. Il faut donc surveiller en continu et valider que les corrections tiennent dans le temps.

- Alertes sur tout nouvel actif ou service exposé apparaissant sur le périmètre
- Détection des régressions (un port refermé qui se rouvre, un certificat qui expire)
- Veille sur les nouvelles vulnérabilités touchant vos technologies exposées
- Validation périodique que les remédiations passées sont toujours effectives
- Indicateurs de tendance pour piloter au comité (et non chiffres bruts)

Cette boucle referme le cycle CTEM : la surveillance ré-alimente la découverte, qui ré-alimente la priorisation. Le bon indicateur de maturité n'est pas « avons-nous fait un audit ? » mais « à quelle vitesse détectons-nous et neutralisons-nous une nouvelle exposition ? » — le facteur qui, selon IBM, pèse le plus sur le coût final d'un incident.

Boucler la boucle

Découverte, inventaire, priorisation, remédiation, surveillance : ces cinq étapes ne s'exécutent pas une fois, elles tournent en permanence. C'est la définition même d'un programme de gestion continue de l'exposition.

19. Hygiène essentielle : SPF/DKIM/DMARC, TLS, CVE, MFA

Au-delà de la méthode, quelques mesures d'hygiène de base couvrent une part disproportionnée du risque. Pour chacune : pourquoi elle compte, comment la vérifier, l'erreur fréquente à éviter.

Mesure	Pourquoi	Erreur fréquente
SPF / DKIM / DMARC	Empêcher l'usurpation de votre domaine pour le phishing	DMARC laissé en p=none — déclaré mais sans protection réelle
TLS moderne	Protéger les échanges et la confiance des visiteurs	Certificat expiré ou protocole de chiffrement obsolète accepté
Gestion des CVE	Fermer les failles exploitées dans la nature	Prioriser au CVSS seul plutôt qu'à l'exploitabilité (KEV / EPSS)
MFA	Neutraliser le vol d'identifiants (22 % des brèches)	MFA partiel, absent sur les accès distants et comptes à privilèges
Gestion des secrets	Éviter l'accès direct via une clé fuitée	Secrets dans des dépôts publics, jamais tournés après fuite

Le principe de Pareto de l'hygiène

Ces cinq mesures ne couvrent pas tout, mais elles ferment les portes que les attaquants empruntent le plus : usurpation d'e-mail, vol d'identifiants, exploitation de failles connues et secrets exposés. Elles doivent être considérées comme non négociables avant tout projet de sécurité plus avancé.

20. Spécificités PME et ETI : faire beaucoup avec peu

Les PME et ETI n'ont ni SOC dédié, ni équipe sécurité étoffée, et dépendent fortement de prestataires et de SaaS. Leur surface est souvent plus large qu'elles ne le pensent, et désormais explicitement ciblée : l'industrialisation du cybercrime (rançongiciel-as-a-service) a rendu rentable l'attaque de cibles de taille intermédiaire.

- Concentrer l'effort sur la visibilité d'abord : on ne peut pas protéger un inventaire qu'on n'a pas
- Automatiser la découverte et le monitoring plutôt que compter sur des campagnes manuelles ponctuelles
- Traiter en priorité les quick wins (ports d'admin, secrets fuités, MFA sur accès distants)
- Exiger de ses prestataires et fournisseurs SaaS des garanties, car 30 % des brèches impliquent un tiers
- S'appuyer sur les ressources publiques gratuites (ANSSI, CISA KEV, ENISA) pour la priorisation

30 %

des brèches impliquent désormais un tiers ou partenaire, soit le double de l'année précédente — la dépendance aux prestataires est une extension directe de la surface d'attaque.

Verizon, communiqué 2025 DBIR

Le rôle de l'automatisation et de l'IA

Pour une équipe réduite, l'automatisation n'est pas un luxe mais une condition de faisabilité : elle permet de faire tourner le cycle découverte-priorisation-surveillance sans y consacrer un temps humain que la PME n'a pas. C'est là que des outils d'évaluation continue de l'exposition prennent tout leur sens.

21. Les 10 erreurs fréquentes qui laissent la porte ouverte

La plupart des compromissions n'exploitent pas une prouesse technique, mais une négligence répétée. Voici les dix pièges les plus courants — chacun est une porte laissée entrouverte.

- ☐ Inventaire incomplet : on protège ce qu'on connaît, pas ce qu'on expose vraiment

- ☐ Priorisation au CVSS seul, sans tenir compte de l'exploitation constatée (KEV / EPSS)
- ☐ Sous-domaines et environnements de test oubliés, jamais décommissionnés
- ☐ DMARC laissé en p=none : déclaré mais sans protection contre l'usurpation
- ☐ Certificats TLS non renouvelés ou protocoles de chiffrement obsolètes
- ☐ Secrets et clés d'API laissés dans des dépôts de code publics
- ☐ MFA partiel, absent sur les accès distants et les comptes à privilèges
- ☐ Audit ponctuel sans suivi continu, alors que la surface bouge chaque semaine
- ☐ Actifs sans propriétaire identifié : personne pour patcher ni décommissionner
- ☐ Confiance aveugle aux tiers, sans exigence de sécurité contractuelle ni vérification

Le fil rouge de ces erreurs

Neuf de ces dix pièges se ramènent à un manque de visibilité ou de continuité. Réglez d'abord la visibilité (cartographie exhaustive) et la continuité (surveillance permanente), et la majorité de ces portes se referment mécaniquement.

22. Checklist opérationnelle et modèles à réutiliser

Pour passer de la lecture à l'action, voici les livrables à mettre en place. Ils constituent le socle minimal d'un programme de gestion de la surface d'attaque externe.

- ☐ Cartographie d'exposition à jour (domaines, sous-domaines, IP, ports, services, TLS, mail, cloud)
- ☐ Registre d'actifs exposés avec propriétaire, usage, criticité et statut renseignés
- ☐ Matrice de priorisation croisant criticité métier et exploitation constatée
- ☐ Plan de remédiation à 30 / 60 / 90 jours avec responsables et délais cibles
- ☐ Dispositif de surveillance continue avec alertes sur nouveaux actifs et régressions
- ☐ Tableau d'indicateurs de suivi présenté régulièrement à la direction

- Taux d'actifs exposés attribués à un propriétaire (objectif : 100 %)
- Délai moyen de remédiation des expositions critiques (tendance à la baisse)
- Nombre d'expositions critiques ouvertes (tendance à la baisse)
- Nombre de nouveaux actifs découverts par période (pour mesurer la dérive de surface)
- Part des domaines en DMARC enforcement (quarantine ou reject)

Objectif : rendre le programme mesurable

Ces indicateurs transforment la sécurité d'une intuition en un tableau de bord. Ils permettent de prouver la progression, de justifier les moyens et de piloter — trois conditions pour que le programme survive au-delà du premier enthousiasme.

23. Où s'adresser, comment anticiper — et le rôle de Sedona

Vous n'êtes pas seul. Plusieurs ressources publiques fiables permettent de cadrer votre démarche et de prioriser sans budget : l'ANSSI et le CERT-FR pour les alertes et le contexte national, le catalogue CISA KEV pour les vulnérabilités activement exploitées, l'ENISA pour le panorama européen, et cybermalveillance.gouv.fr pour l'accompagnement des plus petites structures.

- ANSSI / CERT-FR — alertes, panorama de la cybermenace, portail Mon Espace NIS2
- CISA KEV — file d'attente officielle des vulnérabilités activement exploitées
- ENISA — Threat Landscape annuel pour le contexte européen
- CNIL — obligations et notification des violations de données personnelles
- cybermalveillance.gouv.fr — accompagnement et réflexes pour les PME

Anticiper, c'est intégrer l'EASM dès les nouveaux projets et les acquisitions : toute nouvelle marque, filiale ou plateforme élargit la surface. Le bon moment pour cartographier une exposition n'est pas après l'incident, c'est avant la mise en ligne. L'écart entre la surface perçue (« notre site et nos e-mails ») et la surface réelle (des dizaines de sous-domaines, services et secrets oubliés) est presque toujours la mauvaise surprise d'un premier scan honnête.

Le positionnement de Sedona — en toute transparence

Sedona Radar est un audit de sécurité externe automatisé : il analyse ce que votre domaine expose sur Internet, à intervalles réguliers selon le plan, et remet un rapport en français où les constats sont classés par gravité. Il donne des indicateurs de maturité sur six référentiels ; il ne certifie rien, ne garantit aucune conformité et ne remplace ni un test d'intrusion, ni un audit réglementaire, ni une réponse à incident. Sedona n'est ni qualifiée PASSI, ni certifiée ISO 27001, ni prestataire de réponse à incident ou de forensic. En complément : audit OSINT des dirigeants, audit de surface manuel, simulation de phishing et sensibilisation.

§ Sources

1. Verizon — 2025 Data Breach Investigations Report (DBIR), rapport complet PDF — <https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf>
2. Verizon — Communiqué officiel 2025 DBIR (surge attaques via tiers) — <https://www.verizon.com/about/news/2025-data-breach-investigations-report>
3. IBM — Cost of a Data Breach Report 2025 (analyse X-Force) — <https://www.ibm.com/think/x-force/2025-cost-of-a-data-breach-navigating-ai>
4. ENISA — Threat Landscape 2025 (page de publication officielle) — <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>
5. ENISA — Threat Landscape 2025 (rapport PDF v1.2) — https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf
6. ANSSI / CERT-FR — Panorama de la cybermenace 2025 (PDF CERTFR-2026-CTI-002) — <https://www.cert.ssi.gouv.fr/uploads/CERTFR-2026-CTI-002.pdf>
7. ANSSI (cyber.gouv.fr) — Actualité Panorama de la cybermenace 2025 — <https://cyber.gouv.fr/actualites/panorama-de-la-cybermenace-2025/>
8. CISA — Known Exploited Vulnerabilities (KEV) Catalog — <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
9. MITRE ATT&CK — Tactique Reconnaissance (TA0043) — <https://attack.mitre.org/tactics/TA0043/>
10. Google Cloud / Mandiant — M-Trends 2025 — <https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2025/>
11. Google Cloud / Mandiant — Time-to-Exploit Trends — <https://cloud.google.com/blog/topics/threat-intelligence/time-to-exploit-trends-2023>
12. Unit 42 (Palo Alto Networks) — Attack Surface Threat Research 2024 — <https://unit42.paloaltonetworks.com/2024-unit-42-attack-surface-threat-research-internet-connected-exposures/>
13. Gartner — Continuous Threat Exposure Management (CTEM) — <https://www.gartner.com/en/articles/how-to-manage-cybersecurity-threats-not-episodes>
14. Valimail — 2026 State of DMARC Report — <https://www.valimail.com/dmarc-report-2026/>
15. Directive (UE) 2022/2555 (NIS2) — texte consolidé EUR-Lex — <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>
16. ANSSI — Mon Espace NIS2 (portail officiel de transposition) — <https://monespacenis2.cyber.gouv.fr/>
17. NIST — Cybersecurity Framework (CSF) 2.0 — <https://www.nist.gov/cyberframework>
18. CNIL — Notifier une violation de données personnelles — <https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles>

Voyez votre exposition avant qu'un attaquant ne la voie

Sedona Radar analyse ce que votre domaine expose sur Internet, à intervalles réguliers selon le plan, et remet un rapport en français où les constats sont classés par gravité. Il ne certifie rien et ne garantit aucune conformité : il vous donne la visibilité pour agir. Commencez par un scan gratuit pour mesurer l'écart entre ce que vous pensez exposer et ce que vous exposez réellement.

Lancer mon scan gratuit

sedona-ai.com/scan-gratuit