Sedona.AI

# SEDONA RADAR

Rapport Essentiel

**AUDIENCE : DIRIGEANT DE PME / TPE**

Vue synthétique non-technique adaptée aux décideurs sans équipe IT dédiée

## demo.testfire.net


**Référence :** SR-98819F7E-20260729

Date du scan : 2026-07-29 15:59 UTC

Plateforme : Sedona Radar v3

CONFIDENTIEL — Diffusion restreinte

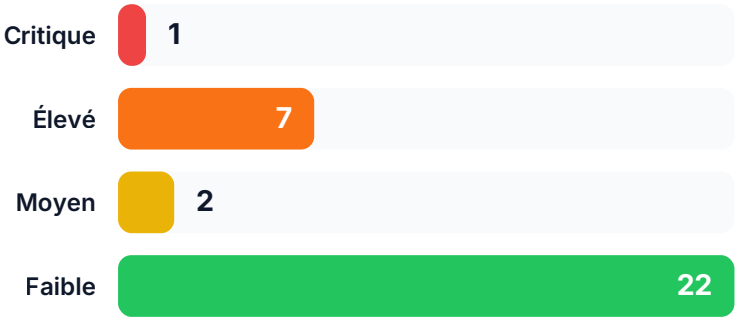
# Table des matières

# Vue d'ensemble

Votre score d'exposition est de **92/100** sur une échelle où 0 = aucune faille externe et 100 = très exposé. Un score supérieur à 70 signifie qu'un attaquant disposant d'outils standards peut compromettre votre périmètre en quelques heures. Les vulnérabilités se répartissent comme suit (graphique ci-dessous) — les **1 critique(s)** en rouge nécessitent une action sous 7 jours.

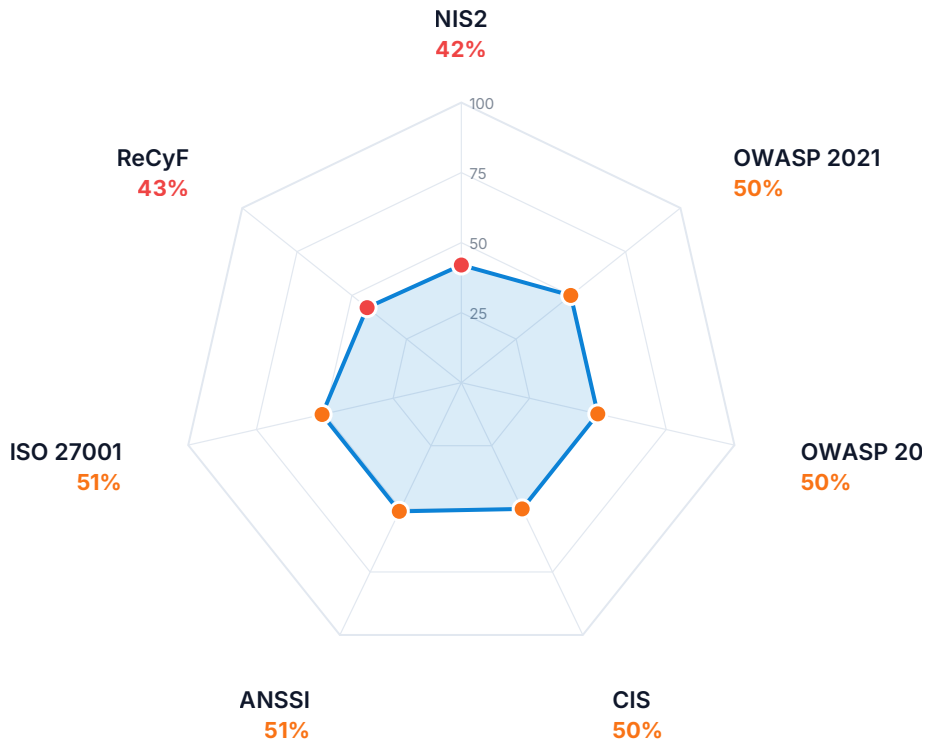
## Score d'exposition global


## Répartition des vulnérabilités

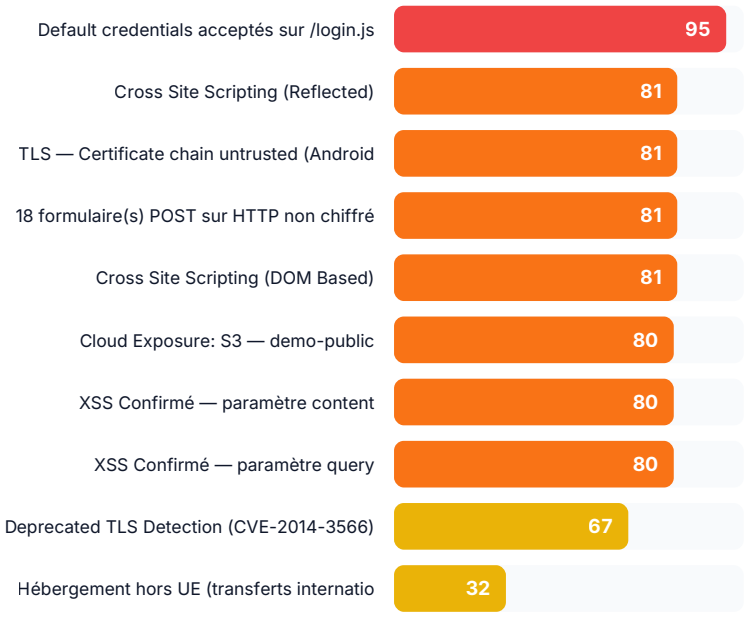



Cette page croise deux lectures de votre exposition. **À gauche** : votre niveau de conformité face aux principaux référentiels cyber (rouge = sanctions possibles, orange = écarts à combler, vert = conforme). **À droite** : vos **5 vulnérabilité(s) les plus dangereuses**, classées par score composite. Les findings en tête sont exploitables par n'importe quel attaquant depuis Internet.

# Conformité réglementaire




# Vulnérabilités les plus critiques



## Surface d'attaque

Votre périmètre expose **1 sous-domaine(s)** accessibles depuis Internet. Chaque sous-domaine est une porte d'entrée potentielle : un seul mal configuré (oublié, en développement, sans mise à jour) suffit à un attaquant pour pénétrer. Les **3 port(s) ouvert(s)** détecté(s) constituent la surface technique principale.


**1** sous-domaine(s) · HTTPS actif (port 443) · **1** avec finding

**Ports ouverts :** 80, 443, 8080

# 1. Synthèse exécutive

Votre système d'information présente un niveau d'exposition alarmant, évalué à 92 sur 100, ce qui place votre organisation en zone critique. L'analyse a révélé 61 failles de sécurité, dont 1 classée critique et 7 à risque élevé. Ces vulnérabilités constituent autant de portes d'entrée potentielles pour des attaquants, mettant en péril vos données clients, votre activité commerciale et votre conformité réglementaire. Le risque financier associé à une exploitation malveillante de ces failles pourrait atteindre plusieurs centaines de milliers d'euros en coûts directs et indirects (estimation IBM CODB 2024, à valider par le commanditaire).

Trois problèmes majeurs requièrent une action immédiate. Premièrement, votre page de connexion accepte des identifiants par défaut (score de criticité 95/100), une négligence grave qui équivaut à laisser la clé sous le paillasson. Deuxièmement, un mécanisme d'injection de code malveillant via les formulaires web a été identifié (score 81/100), permettant potentiellement de voler les sessions de vos utilisateurs. Troisièmement, votre certificat de sécurité pour les connexions chiffrées présente une configuration défaillante (score 81/100), dégradant la confiance accordée par les appareils mobiles et exposant partiellement les données en transit. Votre note globale de chiffrement se situe au niveau B, insuffisante pour une activité traitant des données sensibles.

Ces constats nécessitent un plan de remédiation urgent. La correction des identifiants par défaut doit intervenir dans les 48 heures, celle des deux autres vulnérabilités majeures sous 7 jours. Un accompagnement technique spécialisé est fortement recommandé pour éviter toute interruption de service pendant les opérations de correction et pour établir un programme de surveillance continue.



# 2. Vos données ont-elles fuité ?

**Aucune fuite de données détectée pour vos comptes**

Bonne nouvelle : nous n'avons identifié aucune compromission publique connue liée aux adresses email de votre domaine dans la base Have I Been Pwned. C'est un point positif fort — restez vigilant en cas de réutilisation de mots de passe.

Source : Have I Been Pwned — base de fuites publiques agrégées par Troy Hunt.

# 3. Vulnérabilités identifiées — 61 findings

1 critique, 7 élevées, 2 moyennes, 22 faibles, 29 informationnelles.

Cette section présente l'ensemble des 61 vulnérabilités identifiées lors de l'audit, classées par niveau de sévérité. Chaque finding élevé fait l'objet d'une fiche détaillée comprenant la description technique, une vulgarisation pour les décideurs, la remédiation concrète et le mapping vers les référentiels de conformité applicables.

Le score composite (0-100) de chaque vulnérabilité est calculé ainsi : Base CVSS (v4.0 si disponible, sinon v3.1) pondérée à 50 % (60 % pour les vulnérabilités critiques CVSS ≥ 9), plus la probabilité d'exploitation EPSS (jusqu'à 30 points), plus des bonus d'exploitabilité (CISA KEV +25, module Metasploit +15, exploit public/PoC +10, sans double comptage KEV+PoC), le tout ajusté par des multiplicateurs temporel et contextuel puis borné par des planchers de score par niveau de sévérité. Un score composite élevé traduit une exploitabilité avérée nécessitant une action prioritaire.

## Points positifs identifiés

- Le transfert de zone DNS (AXFR) est correctement protégé sur tous les hostnames.

- La configuration SSL/TLS obtient un grade B, conforme aux bonnes pratiques.
- Aucun secret (clé API, mot de passe) n'a été détecté dans le code source public.
- Aucun service interne (base de données, cache) n'est exposé directement sur Internet.
- Aucune fuite de données connue n'a été identifiée pour ce domaine (Have I Been Pwned).

# Findings de sévérité élevée — 8 vulnérabilités

Les vulnérabilités suivantes présentent la sévérité la plus élevée (critique ou élevée) et nécessitent une attention prioritaire.

**Default credentials acceptés sur /login.jsp** — web **95**

Correction : **Complexe** **Impact estimé :** 50 k€ — 1 M€ Critique Débloquer la remédiation →

**Script malveillant injecté (Script malveillant injecté (XSS)) (Reflected)** (Cross Site Scripting (Reflected)) — http **81**

Correction : **Facile** **Impact estimé :** 10 k€ — 100 k€ Élevé Débloquer la remédiation →

**TLS — Certificate chain untrusted (Android) (demo.testfire.net)** — https://demo.testfire.net:443 **81**

Correction : **Facile** **Impact estimé :** 10 k€ — 100 k€ Élevé Débloquer la remédiation →

… et 5 autres vulnérabilités élevées. Fiches détaillées avec remédiation pas-à-pas **à partir du plan Starter**.

Estimations indicatives basées sur la sévérité technique (CVSS) croisée aux statistiques ENISA Threat Landscape 2024 et CESIN Baromètre 2024. Fourchettes à valider par le commanditaire selon son contexte métier.

### Scénario d'attaque chaîné identifié

**Étape 1 — Reconnaissance** : L'attaquant identifie **Default credentials acceptés sur /login.jsp** (score 95/100) comme point d'entrée.

**Étape 2 — Exploitation** : Il exploite cette vulnérabilité pour obtenir un premier accès au système.

**Étape 3 — Pivot** : Depuis ce point, il pivote via **Cross Site Scripting (Reflected)** pour escalader ses privilèges.

**Étape 4 — Exfiltration et persistance :** l'attaquant copie les données sensibles vers un serveur sous son contrôle et installe une porte dérobée pour revenir plus tard. Le détail technique complet de cette chaîne et les contre-mesures associées sont disponibles à partir du plan Starter.



## Autres vulnérabilités — 53 findings

2 moyennes et 51 faibles. Le détail complet est disponible à partir du plan Starter.

| Risque | Impact estimé |
|---|---|
| MOY 67 | 100 € — 8 k€ |
| MOY 32 | 100 € — 5 k€ |
| FAI 32 | 100 € — 5 k€ |
| FAI 32 | 100 € — 10 k€ |
| FAI 32 | 100 € — 5 k€ |
| FAI 32 | 100 € — 5 k€ |
| FAI 32 | 100 € — 5 k€ |

... et 46 autres vulnérabilités (voir rapport complet).

# 4. Conformité — résumé

Votre posture est évaluée sur 6 référentiels de cybersécurité reconnus. La toile de la vue d'ensemble en donne la lecture visuelle ; le tableau ci-dessous précise, pour chacun, votre verdict, la sanction encourue et pourquoi il vous concerne.

**OWASP Top 10 (2021)** 50 % — Partiellement conforme

l'OWASP Top 10 recense les 10 familles de failles applicatives web les plus courantes — le standard attendu par vos clients et cyber-assureurs.

**CIS Controls v8** 50 % — Partiellement conforme

les CIS Controls sont les 18 gestes techniques qui bloquent l'essentiel des attaques courantes.

**Guide d'hygiène ANSSI** 51 % — Partiellement conforme

le guide d'hygiène de l'ANSSI définit les 42 mesures de base, notamment attendues sur les marchés publics.

**ISO/IEC 27001:2022 (Annexe A)** 51 % — Partiellement conforme

la norme ISO 27001 est la certification internationale de sécurité, souvent exigée par les grands comptes et les banques.

**ReCyF (cadre Sedona)** **43 % — Non conforme**

ReCyF est le cadre d'auto-évaluation Sedona (inspiré de l'hygiène ANSSI v2.0 et de la transposition NIS2 française).

# Verdict par référentiel et sanctions encourues

Synthèse exécutive de votre posture vis-à-vis des principaux référentiels — ce qu'impose la loi, ce qui peut vous coûter, pourquoi ça compte pour votre activité.

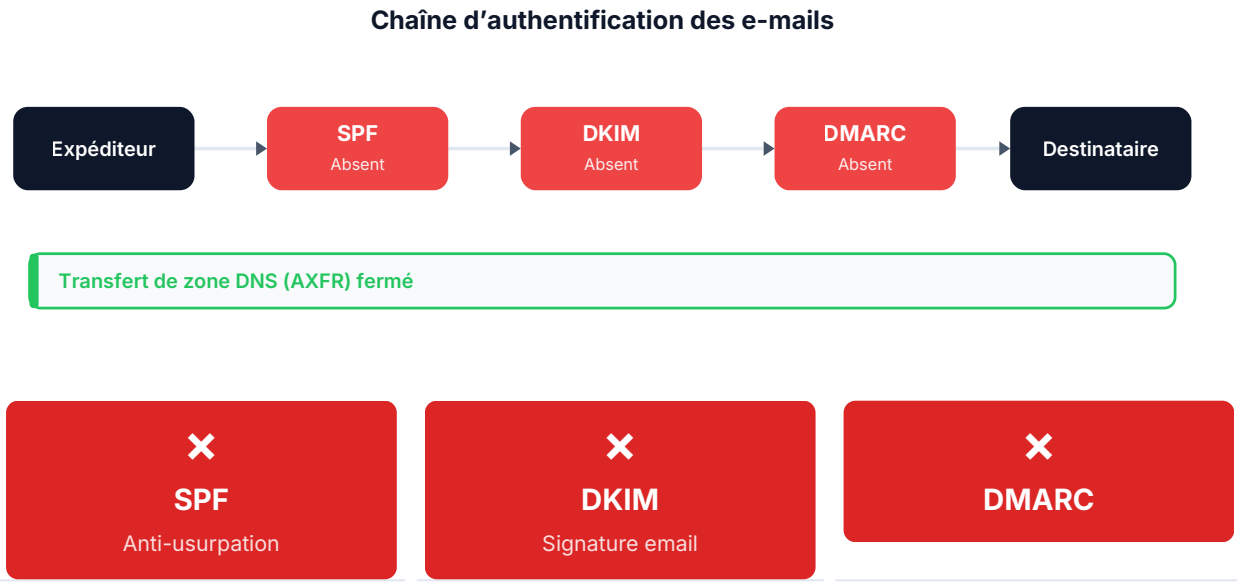
| Référentiel | Verdict | Risque encouru |
|---|---|---|
| **NIS2**<br>Directive européenne d'application obligatoire depuis octobre 2024 pour les entités essentielles et importantes. | Non conforme<br>Score : 42% | **Sanction max :**<br>jusqu'à 10 M€ / 2% du CA (entités essentielles) ou 7 M€ / 1,4% (entités importantes), si assujettie |
| **OWASP 2021**<br>Référence mondiale pour la sécurité applicative — exigée par la majorité des assureurs cyber et auditeurs. | Partiellement conforme<br>Score : 50% | **Sanction max :**<br>Aucune sanction directe — référentiel technique |
| **OWASP 2025**<br>Nouvelle édition intégrant les risques IA et supply chain — anticipez pour 2026. | Partiellement conforme<br>Score : 50% | **Sanction max :**<br>Aucune sanction directe — référentiel technique |
| **CIS**<br>Cadre opérationnel reconnu — réduit de 85% le risque cyber selon études CIS / SANS. | Partiellement conforme<br>Score : 50% | **Sanction max :**<br>Aucune sanction directe — best practice |
| **ANSSI**<br>Indispensable pour les marchés publics et les opérateurs d'importance vitale français. | Partiellement conforme<br>Score : 51% | **Sanction max :**<br>Exclusion des marchés publics + recommandations contractuelles |
| **ISO 27001**<br>Certification reconnue mondialement — souvent exigée par les grands comptes et secteur financier. | Partiellement conforme<br>Score : 51% | **Sanction max :**<br>Perte de certification + audit non-conformité |
| **ReCyF**<br>Cadre Sedona d'auto-évaluation inspiré du Guide d'hygiène ANSSI v2.0 et de la transposition NIS2 française — utile pour préparer un contrôle ANSSI ou un appel d'offres public. | Non conforme<br>Score : 43% | **Sanction max :**<br>Aucune sanction directe — cadre Sedona d'auto-évaluation inspiré ANSSI |

**Lecture business :** ces référentiels structurent les attentes de vos clients, assureurs et régulateurs. Un bon niveau ANSSI / ISO 27001 renforce votre crédibilité lors d'appels d'offres et de due diligence ; la directive NIS2, si votre entité y est soumise, impose des obligations de sécurité dont le non-respect peut entraîner des sanctions administratives. Faites qualifier votre situation exacte par un juriste spécialisé.

# 5. Infrastructure — résumé

## Sécurité email — demo.testfire.net

Trois protections empilées empêchent les pirates d'envoyer des emails au nom de votre organisation (phishing, fraude au président).




**Aucune protection email détectée — usurpation triviale**

Vos emails peuvent être facilement usurpés. Risque BEC (fraude au président) : coût moyen **125 000 €** par incident (source FBI IC3 2024). Action requise sous 7 jours.

## Analyse SSL/TLS

L'analyse SSL/TLS évalue la configuration cryptographique du serveur web : protocoles supportés, suites de chiffrement, configuration du certificat, et vulnérabilités connues (Heartbleed, POODLE, BEAST, etc.). Le grade reflète la robustesse globale.

**B**

Grade SSL/TLS

**Pourquoi ce grade :** Le grade B est attribué en raison de : configuration partiellement non conforme aux meilleures pratiques (CAA record absent, session tickets). L'analyse protocolaire détaillée n'a pas pu être collectée sur ce périmètre ; le grade global reste indicatif et devrait être confirmé par un scan TLS complet.

**Ce que cela signifie concrètement :** Chiffrement conforme — grade B. La configuration cryptographique observée protège correctement les communications entre vos utilisateurs et vos services (protocoles modernes TLS 1.2/1.3, suites de chiffrement robustes).
**Conformité :** Ce niveau de chiffrement répond aux exigences de l'article 32 du RGPD, de l'article 21.2(h) de NIS2 et de PCI-DSS concernant la protection des données en transit.

**3 portes numériques ouvertes** sur Internet — aucune ne mène directement à une base de données ou un cache interne exposé.

## Services détectés — 3 ports exposés

Chaque port ouvert sur Internet constitue un point d'entrée potentiel. L'analyse détaillée des risques par service est disponible à partir du plan Starter.

| Port | Service | Produit |
|---|---|---|
| 80 | http | **Apache-Coyote/1.1** |
| 443 | https | **Apache-Coyote/1.1** |
| 8080 | http | **Apache-Coyote/1.1** |

## Configuration DNS — demo.testfire.net

| | |
|---|---|
| **SPF** | ABSENT |
| **DMARC** | ABSENT |
| **DKIM** | ABSENT |

**Risque concret :** L'absence de SPF et DMARC et DKIM permet à n'importe qui d'envoyer des emails en se faisant passer pour votre organisation. C'est le vecteur principal des attaques de phishing ciblé et des fraudes au président (BEC) — coût moyen par incident : 125 000 € (source FBI IC3 2024). Vos clients, fournisseurs et partenaires bancaires sont directement exposés.

L'analyse détaillée (protocoles SSL par hostname, intelligence Shodan/AbuseIPDB/GreyNoise, findings testssl, résultats des scanners) est disponible à partir du plan Starter.

# 6. Actions prioritaires et conclusion

## Estimation de l'effort

La remédiation de l'ensemble des 61 vulnérabilités identifiées représente un effort de **plusieurs dizaines de jours-homme**. Le chiffrage détaillé par vulnérabilité, les priorités et les étapes concrètes sont disponibles dans le **rapport complet (à partir du plan Starter)**.

## Synthèse des actions — 61 groupes d'actions

Les 61 vulnérabilités sont regroupées par type d'action corrective.

| | | |
|---|---|---|
| **Urgentes (sous 7 jours)** | **20** | actions de configuration (headers HTTP, DNS email, disclosure) |
| **Moyen terme (sous 30 jours)** | **8** | corrections de sévérité élevée nécessitant planification |
| **Long terme (3+ mois)** | **33** | transformations structurelles (WAF, architecture, patch management) |



Avec un score de 92 sur 100 et 61 failles détectées, votre infrastructure numérique nécessite une intervention rapide. Voici ce que vous devez faire maintenant.

Premièrement, faites corriger les identifiants par défaut sur votre page de connexion cette semaine, c'est la porte d'entrée la plus dangereuse. Deuxièmement, planifiez la correction des sept autres problèmes majeurs dans les quinze jours par un prestataire qualifié. Troisièmement, mettez à niveau votre certificat de sécurité pour atteindre au minimum une note A.

Programmez un nouveau contrôle dans 30 jours pour vérifier l'efficacité des corrections. Entretemps, surveillez quotidiennement vos journaux de connexion pour détecter toute tentative d'intrusion.

Pour une protection durable, notre offre Business vous apporte un accompagnement continu avec des scans mensuels automatiques, une surveillance permanente et un support prioritaire. Cet investissement vous protège contre des pertes financières estimées à plusieurs centaines de milliers d'euros en cas d'incident majeur (estimation IBM CODB 2024, à valider par le commanditaire).

Chaque jour sans action augmente votre exposition. Contactez-nous pour démarrer les corrections prioritaires.

# Glossaire — 20 termes cyber essentiels

Les termes cybersécurité les plus utiles, expliqués avec des analogies du quotidien. Pensé pour un dirigeant PME sans équipe IT dédiée.

**CVE** — Numéro mondial d'une faille connue. Comme une plaque d'immatriculation pour les vulnérabilités.

**CVSS** — Note de gravité sur 10. 0 = inoffensif, 10 = catastrophique.

**Vulnérabilité** — Un cadenas défectueux sur votre porte numérique : tant qu'on ne pousse pas, ça tient ; quand on pousse, ça cède.

**Port (ouvert)** — Une porte d'entrée numérique vers vos serveurs. Une porte ouverte non nécessaire = une porte non verrouillée.

**Phishing** — Email frauduleux qui imite votre banque ou un fournisseur pour piéger vos équipes. 80% des attaques commencent là.

**Ransomware** — Logiciel qui chiffre tous vos fichiers et réclame une rançon. Coût moyen PME : 250 000 € et 22 jours d'arrêt.

**Sauvegarde** — Copie de vos données stockée ailleurs. Sans sauvegarde testée : un ransomware = entreprise à l'arrêt définitif.

**DNS** — L'annuaire d'Internet : il traduit votresite.fr en adresse numérique. Mal configuré = visiteurs détournés.

**SSL / HTTPS** — Le cadenas dans la barre du navigateur. Chiffre les échanges entre vos visiteurs et votre site. Sans lui : mots de passe en clair.

**Certificat** — Pièce d'identité numérique de votre site. Périmé = alerte rouge sur Chrome, visiteurs en fuite.

**Patch (mise à jour)** — Correctif publié par l'éditeur. Ne pas l'installer = laisser la porte ouverte après avoir été prévenu.

**Mot de passe fort** — Au moins 12 caractères, mélange chiffres / lettres / symboles, jamais réutilisé. Sans ça : compte piratable en quelques minutes.

**MFA (double authentification)** — Code reçu sur téléphone en plus du mot de passe. Réduit le risque de piratage de 99,9% (chiffres Microsoft).

**Sous-domaine** — Adresse satellite (boutique.votresite.fr). Un sous-domaine oublié reste une porte d'entrée.

**Fuite de données** — Vos informations confidentielles deviennent publiques. Sanction RGPD : jusqu'à 4% du chiffre d'affaires + notification CNIL sous 72h.

**Antivirus / EDR** — Gardien installé sur vos postes qui détecte les programmes malveillants. L'EDR est sa version moderne, plus intelligente.

**Pare-feu (firewall)** — Filtre à l'entrée de votre réseau qui bloque le trafic suspect. Comme un videur à l'entrée d'un magasin.

**VPN** — Tunnel sécurisé entre vos collaborateurs en télétravail et l'entreprise. Sans VPN : connexion exposée.

**Hameçonnage / fraude au président** — Email piégé qui imite votre dirigeant pour déclencher un virement. Coût moyen victime : 125 000 €.

**Audit / Scan** — **Scan** = automatisé, large (Sedona Radar). **Audit** complet = revue documents + entretiens + tests par un expert.

# Prochaines étapes

> **Trois chiffres à garder en tête avant de décider du plan d'action :**

**1 sur 2**
PME touchée par une cyberattaque majeure rencontre des difficultés durables (ordre de grandeur indicatif, sources sectorielles variables)

**20j**
durée moyenne d'arrêt après ransomware (Sophos 2024)

**7 mois**
temps moyen pour détecter une intrusion (IBM Cost of a Data Breach 2024)

## Nos plans Sedona Radar

| Plan | Prix | Scans de Contrôle / Deep Scans | Domaines | Fonctionnalités clés |
|---|---|---|---|---|
| Discovery | Gratuit | 1 à vie | 1 | Aperçu du score & top 3 vulnérabilités |
| Starter | 79 €/mois HT | 5 + 2 / mois | 1 | Audit externe complet, rapport Essentiel, monitoring mensuel |
| **Business** | **229 €/mois HT** | 10 + 5 / mois | 5 | **Rapports Stratégique + Opérationnel, monitoring bi-mensuel, Slack/ Teams (bientôt disponibles)** |
| Scale | 590 €/mois HT | 30 + 10 / mois | 10 | Monitoring hebdomadaire, SLA, API publique (bientôt disponible) |
| Enterprise | bientôt disponible | illimité | illimité | Rapport PASSI, monitoring continu, account manager dédié |

**Recommandation pour votre périmètre :** le plan **Starter (79 €/mois)**. Le plan Starter débloque le rapport complet avec remédiation pas-à-pas, 5 Scans de Contrôle et 2 Deep Scans par mois et le monitoring mensuel. Les plans supérieurs (Business 229 €, Scale 590 €) ajoutent davantage de domaines, le monitoring bi-mensuel/hebdomadaire et le support prioritaire.

## Parlons-en

Nous vous proposons un **échange de 30 minutes** pour parcourir ce rapport ensemble et définir un plan d'action adapté.

| | |
|---|---|
| **Email** | vincent.coderch@sedona-ai.com |
| **Téléphone** | +33 (0)6 03 39 43 98 |
| **Plateforme** | app.sedona-ai.com |

# À propos de Sedona AI

**Pour les PME — Sedona Radar rend la cybersécurité accessible aux entreprises sans équipe IT dédiée.** 10× moins cher qu'un audit traditionnel, 10× plus rapide : un audit complet en quelques heures, livré en français, lisible par un dirigeant.

Sedona AI est un cabinet français fondé en 2025 et incubé à l'Université de Perpignan Via Domitia (UPVD InCube). Notre conviction : la cybersécurité ne doit pas être réservée aux grands comptes.

## Équipe fondatrice

- **Vincent Coderch** — CEO. 10 ans de conseil en stratégie IA et transformation numérique.
- **Angel Venzac** — CTO. Architecte systèmes et sécurité.

## Contact

| | |
|---|---|
| **Email** | vincent.coderch@sedona-ai.com |
| **Téléphone** | +33 (0)6 03 39 43 98 |
| **Adresse** | UPVD InCube, 52 avenue Paul Alduy, 66100 Perpignan, France |
| **Site web** | https://sedona-ai.com |
| **Plateforme** | https://app.sedona-ai.com |

# Annexe E — Mentions légales (synthèse)

Cette annexe présente une **synthèse en deux pages** des clauses encadrant le présent rapport. La version intégrale (20 clauses E.1 à E.20) est accessible en ligne (voir encart en fin d'annexe).

## E.1 — Nature de la prestation

Le présent rapport est le livrable d'une **analyse automatisée de la surface d'attaque externe** réalisée par la plateforme Sedona Radar (éditée par Sedona AI) : reconnaissance passive, analyse des services exposés, scan de vulnérabilités, corrélation avec des bases de threat intelligence publiques. Il ne constitue ni un test d'intrusion complet, ni un audit de code, ni un audit organisationnel, ni un audit physique, ni un avis juridique, ni un avis d'expert humain certifié PASSI.

## E.4 — Absence de garantie d'exhaustivité

Le rapport identifie les vulnérabilités détectables par les outils et méthodologies utilisés à la date du scan. Il **ne garantit pas l'absence d'autres vulnérabilités** : logiques métier spécifiques, zero-day non publiés, configurations accessibles uniquement depuis le réseau interne, vulnérabilités nécessitant un contexte d'authentification (IDOR, BOLA, post-login), éléments derrière un WAF/CDN filtrant le scan, ou composants en cours de déploiement / hors périmètre déclaré. Sedona Radar effectue exclusivement une analyse non authentifiée.

## E.7 — Responsabilité du commanditaire

Le commanditaire déclare détenir les droits sur le périmètre audité et avoir fourni un périmètre exact. Il prend la **responsabilité de la mise en œuvre des recommandations** (test en pré-production avant production, relance d'un nouveau scan après chaque correction pour vérifier la remédiation, association de son RSSI / DPO / juriste / auditeur PASSI selon les besoins, maintien à jour de la configuration). Une vulnérabilité signalée comme corrigée sans nouveau scan reste considérée comme ouverte par Sedona AI.

## E.8 — Limitation de responsabilité de Sedona AI

Dans les limites autorisées par la loi, la responsabilité de Sedona AI au titre de la prestation est limitée au **montant effectivement payé par le commanditaire sur les douze (12) mois précédant le fait générateur**. Sedona AI ne saurait être tenue responsable des dommages indirects, pertes d'exploitation, atteinte à la réputation, pertes de données, pertes de chance ou manque à gagner.

# E.14 — Absence de garantie d'absence d'incident futur

Le présent rapport reflète l'état de la surface d'attaque externe à un instant T. Il ne constitue **en aucun cas une garantie d'absence d'incident de sécurité futur**. Environ 80 nouvelles vulnérabilités (CVE) sont publiées chaque jour. Sedona AI ne peut être tenue responsable d'une intrusion, fuite, rançongiciel ou autre incident survenu postérieurement à la génération du rapport.

# Autres clauses (synthèse)

Les 15 clauses ci-dessous figurent dans la version intégrale — titre seul ici.

- **E.2 Périmètre et limites** — audit limité aux noms de domaine / IP fournis ; aucun accès au SI interne.
- **E.3 Validité temporelle** — résultats valables 30 jours maximum.
- **E.5 Absence de garantie d'absence de faux positifs** — validation manuelle recommandée avant action.
- **E.6 Recours à l'intelligence artificielle** — LLM utilisé pour mise en forme uniquement, jamais pour les données factuelles.
- **E.9 Estimations financières** — indicatives, fondées sur statistiques publiques (IBM, autorités de contrôle).
- **E.10 Confidentialité et diffusion** — classification CONFIDENTIEL — DIFFUSION RESTREINTE.
- **E.11 Protection des données personnelles** — Sedona AI sous-traitant au sens du RGPD.
- **E.12 Loi applicable et juridiction** — droit français, tribunaux de Perpignan.
- **E.13 Recours à des experts tiers** — juriste, DPO, RSSI, auditeur PASSI, courtier cyber-assurance, SOC/MSSP.
- **E.15 Caractère non destructif des scans** — aucune exploitation aboutie, aucune modification de données.
- **E.16 Continuité de service Sedona Radar** — obligation de moyens, pas de SLA hors Scale/Enterprise.
- **E.17 Réutilisation du rapport vis-à-vis de tiers** — usage interne ; communication à des tiers sous responsabilité du commanditaire.
- **E.18 Articulation avec l'assurance cyber et obligations réglementaires** — ne se substitue pas aux audits PASSI / SOC 2 / ISO 27001 / PCI DSS / HDS.
- **E.19 Évolution des référentiels de conformité** — scores calculés sur les versions en vigueur à la date du scan.
- **E.20 Propriété intellectuelle et utilisation autorisée** — reverse engineering et réutilisation pour entraîner un modèle IA concurrent strictement interdits.

> **Mentions légales intégrales (E.1 → E.20)**
>
> Le détail complet des 20 clauses est disponible sur : https://sedona-ai.com/legal/rapport-v1 (version permanente, archivée pour traçabilité). Une copie peut être obtenue sur demande à legal@sedona-ai.com.