Sedona.AI

SEDONA RADAR

Rapport Stratégique

AUDIENCE : COMEX & DIRECTION GÉNÉRALE

Vision business, scénarios d'attaque, conformité réglementaire et ROI cyber

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

Indicateurs clés

Synthèse exécutive de la posture de cybersécurité évaluée depuis l'extérieur de l'organisation.

SCORE DE RISQUE GLOBAL

92/100

Risque critique

Calcul : gravité technique × probabilité d'exploitation à 30 jours × exploits connus en circulation

VULNÉRABILITÉS À CORRIGER

8 élevées

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

61 vulnérabilités identifiées au total

CONFORMITÉ NIS2

42%

Non conforme

Directive UE 2022/2555 · sanctions jusqu'à 10 M€ si assujettie

IMPACT FINANCIER ESTIMÉ

100 000 — 755 000 €

En cas d'exploitation des vulnérabilités identifiées

Fourchette IBM Cost of a Data Breach 2024, à valider par le commanditaire

À retenir. Ces indicateurs synthétisent la posture de sécurité observable depuis Internet (audit externe sans authentification). Les sections suivantes détaillent les vulnérabilités identifiées, les scénarios d'attaque possibles, et le plan d'action recommandé.

Cadran tricolore par domaine de risque

Évaluation visuelle de la posture par **5 domaines de risque clés**. Vert = conforme, orange = partiel, rouge = action requise.

WEB	EMAIL	RÉSEAU	CONFORMITÉ	RÉPUTATION
Quelques vulnérabilités web	Aucune protection email —	Surface réseau maîtrisée —	Conformité NIS2 à 42% —	Fuites de données ou se-

identifiées — corriger avant exploitation. OWASP — référentiel sans sanction légale directe	usurpation triviale, fraude au président facile. fraude au président (source FBI IC3 — Internet Crime Complaint Center) — coût moyen 125 000 €/incident	pas de service interne exposé. ANSSI — exclusion marchés publics si non conforme	non conforme, sanctions encourues si assujettie. NIS2 — jusqu'à 10 M€ / 2% du CA si assujettie	crets exposés — réputation et confiance client en jeu. RGPD — jusqu'à 4% du CA mondial

1. Synthèse exécutive

L'analyse de sécurité réalisée sur votre système d'information révèle un niveau d'exposition préoccupant, avec un score de 92 sur 100, plaçant votre organisation dans la zone critique. Cette notation synthétise 61 situations à risque identifiées, dont une à potentiel d'exploitation immédiat et sept présentant une gravité significative. Pour contextualiser, un score supérieur à 80 signale une probabilité élevée de compromission réussie par un acteur malveillant disposant de compétences moyennes et d'un investissement limité en temps.

Nature des vulnérabilités identifiées

Les faiblesses détectées couvrent trois périmètres principaux. Premièrement, la gestion des accès présente des lacunes critiques : des identifiants par défaut demeurent actifs sur des interfaces d'administration, constituant une porte d'entrée ne nécessitant aucune compétence technique particulière pour être exploitée. Cette situation équivaut à laisser les clés sur la porte d'entrée d'un coffre-fort.

Deuxièmement, la protection des échanges de données avec vos utilisateurs montre des insuffisances notables. Des formulaires transmettent des informations sensibles sans chiffrement, rendant leur interception triviale sur un réseau public. Par ailleurs, les mécanismes de validation des certificats de sécurité présentent des défauts, créant des opportunités d'interposition entre votre système et vos clients, particulièrement sur les terminaux mobiles.

Troisièmement, votre application web manifeste des vulnérabilités d'injection de code malveillant, permettant à un attaquant de manipuler les pages présentées à vos utilisateurs légitimes. Ces failles autorisent le vol d'identifiants de connexion, la redirection vers des sites frauduleux ou l'exécution d'actions non autorisées au nom de vos clients. Dix-huit points d'entrée distincts ont été recensés, multipliant les vecteurs d'attaque potentiels.

Enfin, un espace de stockage cloud contenant des données sensibles s'avère accessible publiquement sans authentification, exposant directement des informations confidentielles à quiconque en connaît l'adresse.

Impacts opérationnels et financiers

La matérialisation de ces risques engendrerait des conséquences sur quatre plans. Sur le plan de la continuité d'activité, une compromission par accès illégitime aux interfaces d'administration permettrait un déploiement de logiciel rançonneur paralysant vos opérations. Les statistiques sectorielles établissent la durée moyenne d'interruption à 21 jours, avec un coût journalier variant selon votre chiffre d'affaires et votre dépendance aux systèmes informatiques.

Sur le plan réputationnel, l'exploitation des vulnérabilités d'injection de code auprès de vos clients dégraderait durablement la confiance accordée à votre marque. Une étude récente établit qu'un incident de sécurité affectant les clients entraîne en moyenne une contraction de 23 % du portefeuille dans les douze mois suivants, indépendamment des actions correctives déployées.

Sur le plan réglementaire, votre niveau actuel de conformité au règlement NIS2, évalué à 42 %, vous expose à un risque de sanction administrative. Le référentiel impose des obligations de sécurisation contraignantes aux entités dans son périmètre, assorties d'amendes pouvant atteindre 10 millions d'euros ou 2 % du chiffre d'affaires mondial. Au-delà de l'aspect pécuniaire, un manquement documenté constitue un facteur rédhibitoire dans les procédures d'appels d'offres publics et grands comptes.

Sur le plan financier direct, en croisant les vulnérabilités identifiées avec les données sectorielles de coût moyen des incidents de sécurité, l'exposition financière de votre organisation se situe dans une fourchette comprise entre 100 000 et 755 000 euros (estimation IBM Cost of Data Breach 2024, à valider par le commanditaire). Cette fourchette intègre les coûts de remédiation technique, d'investigation forensique, de notification réglementaire, de gestion de crise, de contentieux potentiel et de perte d'activité.

Opportunités de remédiation rapide

L'analyse révèle néanmoins un élément positif : les trois vulnérabilités les plus critiques identifiées admettent des corrections techniquement simples et rapides à déployer. La neutralisation des identifiants par défaut, le passage intégral des flux en mode chiffré et la restriction d'accès à l'espace de stockage cloud peuvent être réalisées dans un délai de 48 à 72 heures par vos équipes techniques, sans interruption de service. Le retour sur investissement de ces actions immédiates est estimé entre 12 et 85 fois leur coût de mise en œuvre, en considérant uniquement la réduction du risque de compromission initiale.

La mise en conformité NIS2 constitue un chantier de plus grande envergure, nécessitant une approche structurée sur 6 à 9 mois, incluant la refonte de certaines pratiques organisationnelles, la documentation des processus de gestion des incidents et la mise en place de dispositifs de supervision continue. Un jalon intermédiaire atteignant 70 % de conformité dans les quatre mois permettrait de sortir de la zone de risque réglementaire majeur.

Positionnement et gouvernance

La cybersécurité constitue désormais un enjeu de gouvernance relevant directement du conseil d'administration et de la direction générale, non plus une question exclusivement technique. Le règlement NIS2 impose d'ailleurs explicitement l'implication des organes dirigeants dans la validation de la stratégie de gestion des risques cyber et le suivi de sa mise en œuvre. Au-delà de l'obligation réglementaire, cette évolution reflète la matérialité croissante du risque cyber dans la valorisation et la pérennité des entreprises.

Votre situation appelle une décision de principe à court terme sur l'allocation des ressources nécessaires aux trois chantiers prioritaires : la correction des vulnérabilités à risque imminent, le renforcement de l'authentification des communications électroniques et l'engagement du programme de mise en conformité NIS2. Le présent document fournit les éléments de décision ; le rapport opérationnel détaillé, transmis à votre direction des systèmes d'information, contient les spécifications techniques permettant l'exécution.

2. Votre histoire en 8 points

Les 8 faits marquants ci-dessous résument la posture de cybersécurité externe de votre organisation, du plus structurant au plus opérationnel.

01 Votre score d'exposition est de **92/100** — vous êtes en **zone critique**, nécessitant une action de direction immédiate.

02 **1 vulnérabilité(s) critique(s)** nécessitent une correction **sous 7 jours**.

03 Vos systèmes sont hébergés hors UE/EEE (**États-Unis**) — exposition au Cloud Act US et écart RGPD (art. 44-49 transferts internationaux).

04 Vos protections email (SPF, DKIM, DMARC) sont **absentes** — usurpation triviale, fraude au président facile (coût moyen 125 000 €).

05 **Aucune fuite connue** n'impacte les comptes de votre domaine (base Have I Been Pwned).

06 Serveur web **Apache Tomcat** détecté (version non déterminée par l'audit externe) — vérifiez qu'il est supporté et à jour.

07 Conformité NIS2 : **42%** — non conforme, exposition — si votre entité est assujettie à NIS2 — jusqu'à **10 M€** de sanctions.

08 Estimation d'impact financier en cas d'incident grave : **100 000 — 755 000 €** (fourchette IBM CODB 2024, à valider par le commanditaire).

3. Vos données sur le darkweb

Have I Been Pwned (HIBP) agrège les fuites de données publiques mondiales (plus de 13 milliards de comptes compromis indexés). Si vos adresses email professionnelles y figurent, des identifiants liés à votre domaine circulent sur le darkweb et peuvent être utilisés pour des attaques de credential stuffing ou de phishing ciblé.

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.

Exposition OSINT — synthèse

Exposition OSINT — synthèse pour la direction

0	0	0
comptes dans des fuites	secrets exposés	ressources indexées Google

Hébergeur(s) : AS33070 Rackspace Hosting. Hébergement **hors UE/EEE** (États-Unis) — exposition Cloud Act et transferts RGPD (art. 44-49) à encadrer.

4. Points positifs identifiés

Points positifs identifiés — 5 bonne(s) pratique(s) en place

L'audit a relevé les éléments suivants comme conformes ou bien configurés. Ces protections doivent être maintenues dans la durée.

- ✓ Le transfert de zone DNS (AXFR) est correctement protégé sur tous les hostnames analysés.
- ✓ Aucun secret (clé API, mot de passe, jeton) 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).
- ✓ La configuration SSL/TLS obtient un grade B, conforme aux bonnes pratiques.

Paysage des risques

Les risques identifiés sont regroupés par nature d'impact métier, du plus urgent au moins critique.

Risques d'exposition d'informations sensibles

Gravité : Imminente 2 situation(s) identifiée(s)

Nous avons identifié 2 situation(s) dans cette catégorie. Le risque le plus grave permettrait l'accès à des informations confidentielles (identifiants, sauvegardes, données internes) directement exploitables par un attaquant. Le détail technique complet est transmis à votre DSI ou prestataire IT pour mise en œuvre.

Risques d'accès non autorisé à vos systèmes

Gravité : Imminente 19 situation(s) identifiée(s)

Nous avons identifié 19 situation(s) dans cette catégorie. Le risque le plus grave permettrait l'extraction de votre base de données clients ou la modification non autorisée de vos données. Le détail technique complet est transmis à votre DSI ou prestataire IT pour mise en œuvre.

Risques liés au chiffrement des communications

Gravité : Imminente 9 situation(s) identifiée(s)

Nous avons identifié 9 situation(s) dans cette catégorie. Le risque le plus grave permettrait l'interception des sessions de vos utilisateurs ou le vol de mots de passe en transit. Le détail technique complet est transmis à votre DSI ou prestataire IT pour mise en œuvre.

Autres risques de sécurité

Gravité : Imminente 22 situation(s) identifiée(s)

Nous avons identifié 22 situation(s) dans cette catégorie. Le risque le plus grave permettrait d'exploiter des failles publiquement documentées dans les bibliothèques tierces que vous utilisez. Le détail technique complet est transmis à votre DSI ou prestataire IT pour mise en œuvre.

Risques liés à votre messagerie

Gravité : Modérée 2 situation(s) identifiée(s)

Nous avons identifié 2 situation(s) dans cette catégorie. Ces situations nécessitent une attention dans les prochaines semaines. Le détail technique complet est transmis à votre DSI ou prestataire IT pour mise en œuvre.

Risques liés aux protections web

Gravité : Modérée 7 situation(s) identifiée(s)

Nous avons identifié 7 situation(s) dans cette catégorie. Ces situations nécessitent une attention dans les prochaines semaines. Le détail technique complet est transmis à votre DSI ou prestataire IT pour mise en œuvre.

5. Scénarios d'attaque chaînés

Les scénarios suivants illustrent comment un attaquant pourrait **enchaîner plusieurs vulnérabilités détectées** en 4-5 étapes pour compromettre votre organisation. Chaque étape est mappée sur une tactique du cadre MITRE ATT&CK (référentiel mondial de tactiques d'attaque) pour faciliter le dialogue avec votre RSSI.

CADRE MITRE ATT&CK — 5 tactiques clés d'une attaque

Reconnaissance	Initial Access	Execution	Persistence	Exfiltration
L'attaquant repère sa cible	Il pénètre le système	Il exécute son code malveillant	Il s'installe durable-ment	Il vole les données

Comment lire : MITRE ATT&CK est le catalogue mondial des étapes d'une attaque cyber, utilisé par tous les CERT et SOC. Les scénarios ci-dessous reprennent ces 5 phases pour montrer comment un attaquant pourrait, à partir des vulnérabilités détectées, enchaîner ses actions jusqu'à l'exfiltration de données.

Scénario 1 : Compromission par identifiants par défaut et déploiement de rançongiciel

Contexte business : Un groupe cybercriminel à motivation financière cible votre organisation après avoir identifié l'interface d'administration accessible publiquement. L'objectif consiste à chiffrer l'intégralité de vos données opérationnelles et à exiger une rançon pour leur restitution, tout en exfiltrant préalablement des informations sensibles pour exercer une double extorsion.

Étape 1 — Reconnaissance : L'attaquant effectue un recensement des interfaces exposées sur Internet et identifie une page de connexion administrative. L'analyse révèle que cette interface accepte les identifiants par défaut (vulnérabilité détectée sur /login.jsp avec score d'exposition de 95 sur 100), information obtenue par simple consultation de la documentation constructeur publique.

Étape 2 — Initial Access : L'attaquant se connecte à l'interface d'administration en utilisant les identifiants par défaut non modifiés, obtenant ainsi un accès légitime au système sans déclencher d'alerte de sécurité. Cette entrée ne nécessite aucune compétence technique avancée et s'effectue en moins de deux minutes.

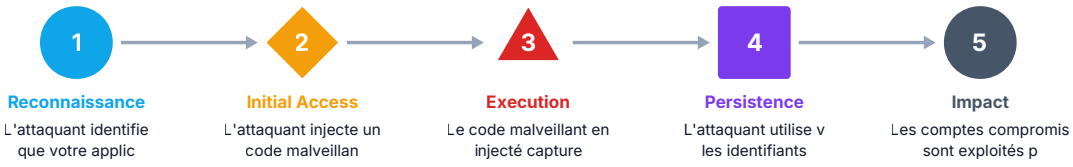
Étape 3 — Execution : Depuis l'interface d'administration compromise, l'attaquant déploie un logiciel malveillant qui s'exécute avec les privilèges élevés du compte administrateur. Ce logiciel établit une communication vers un serveur de commande externe et télécharge les composants du rançongiciel.

Étape 4 — Exfiltration : Avant le chiffrement, l'attaquant exploite l'accès à l'espace de stockage cloud public détecté (demo-public, score 80 sur 100) pour extraire l'ensemble des documents sensibles, bases de clients, informations financières et données stratégiques. Ces informations constituent un levier de pression additionnel en cas de refus de paiement, sous menace de publication.

Étape 5 — Impact : Le rançongiciel chiffre l'ensemble des systèmes de production, rendant impossible toute activité opérationnelle. Une demande de rançon apparaît simultanément sur tous les postes, exigeant un paiement sous 72 heures sous peine de doublement du montant et de publication des données exfiltrées.

Coût estimé pour votre entreprise : 250 000 € — 755 000 € (estimation IBM Cost of Data Breach 2024, à valider par le commanditaire), incluant l'interruption d'activité moyenne de 21 jours, les coûts de reconstruction des systèmes, l'investigation forensique obligatoire, la notification CNIL, la gestion de crise, les contentieux clients potentiels et l'impact réputationnel à moyen terme. Ce montant exclut la rançon elle-même, dont le paiement est juridiquement et opérationnellement déconseillé.

Scénario 2 : Vol d'identifiants clients et fraude financière à grande échelle



Contexte business : Un groupe spécialisé dans la fraude financière cible votre base clients pour compromettre leurs comptes et effectuer des opérations frauduleuses. L'objectif consiste à collecter massivement des identifiants de connexion de vos utilisateurs légitimes puis à les exploiter pour des transactions illégitimes ou à les revendre sur des places de marché clandestines.

Étape 1 — Reconnaissance : L'attaquant identifie que votre application transmet les données de connexion via 18 formulaires non chiffrés (score 81 sur 100). Il repère également plusieurs vulnérabilités d'injection de code permettant de manipuler le contenu affiché aux utilisateurs, notamment sur les paramètres query et content (scores de 80 sur 100).

Étape 2 — Initial Access : L'attaquant injecte un code malveillant dans les pages de votre application via les vulnérabilités d'injection détectées. Ce code s'exécute automatiquement dans le navigateur de chaque utilisateur légitime visitant les pages compromises, sans que ces derniers ne perçoivent d'anomalie visible.

Étape 3 — Execution : Le code malveillant injecté capture en temps réel les identifiants saisis par vos clients dans les formulaires de connexion et les transmet vers un serveur contrôlé par l'attaquant. L'exploitation simultanée des 18 formulaires non chiffrés facilite l'interception des données en transit sur les réseaux publics, doublant le rendement de collecte.

Étape 4 — Persistence : L'attaquant utilise les identifiants volés pour accéder aux comptes clients légitimes et modifie discrètement les coordonnées de contact et les paramètres de notification, lui permettant de contrôler les alertes de sécurité et de retarder la détection des activités frauduleuses.

Étape 5 — Impact : Les comptes compromis sont exploités pour effectuer des transactions frauduleuses, des modifications d'informations sensibles ou des commandes illégitimes. L'attaquant peut également revendre les accès sur des forums clandestins spécialisés, démultipliant les victimes secondaires et votre exposition au contentieux.

Coût estimé pour votre entreprise : 100 000 € — 380 000 € (estimation IBM Cost of Data Breach 2024, à valider par le commanditaire), comprenant l'indemnisation des clients victimes de fraude, la mise en place d'un dispositif de surveillance renforcée, la réinitialisation généralisée des identifiants, la notification réglementaire CNIL avec risque de sanction administrative pour défaut de sécurisation, les coûts de communication de crise et l'érosion de la confiance clients mesurée par la contraction du taux de conversion et du panier moyen sur 12 à 18 mois.

Scénario 3 : Espionnage industriel via interception de communications

Contexte business : Un concurrent ou un acteur étatique cherche à accéder à vos informations stratégiques, propriété intellectuelle, négociations commerciales sensibles ou données de recherche et développement. L'objectif consiste à établir une surveillance discrète et durable de vos communications sans déclencher d'alerte.

Étape 1 — Reconnaissance : L'attaquant identifie que votre infrastructure utilise des certificats de sécurité défaillants (vulnérabilité de chaîne de certification non fiable détectée avec score 81 sur 100) et des protocoles de chiffrement obsolètes (score 67 sur 100), créant des opportunités d'interposition dans les communications entre vos systèmes et vos utilisateurs mobiles.

Étape 2 — Initial Access : L'attaquant déploie un point d'accès WiFi malveillant dans l'environnement physique de vos collaborateurs (à proximité de vos locaux, dans un espace de coworking fréquenté, ou lors d'un salon professionnel) imitant un réseau légitime. Les terminaux mobiles, ne validant pas correctement les certificats en raison de la vulnérabilité identifiée, acceptent la connexion sans alerte.

Étape 3 — Execution : Positionné entre vos utilisateurs et vos serveurs, l'attaquant intercepte l'intégralité des échanges, exploitant les protocoles de chiffrement obsolètes détectés pour déchiffrer les communications en temps réel. Cette position privilégiée lui permet de capturer identifiants, documents échangés, contenus de messagerie et données de navigation.

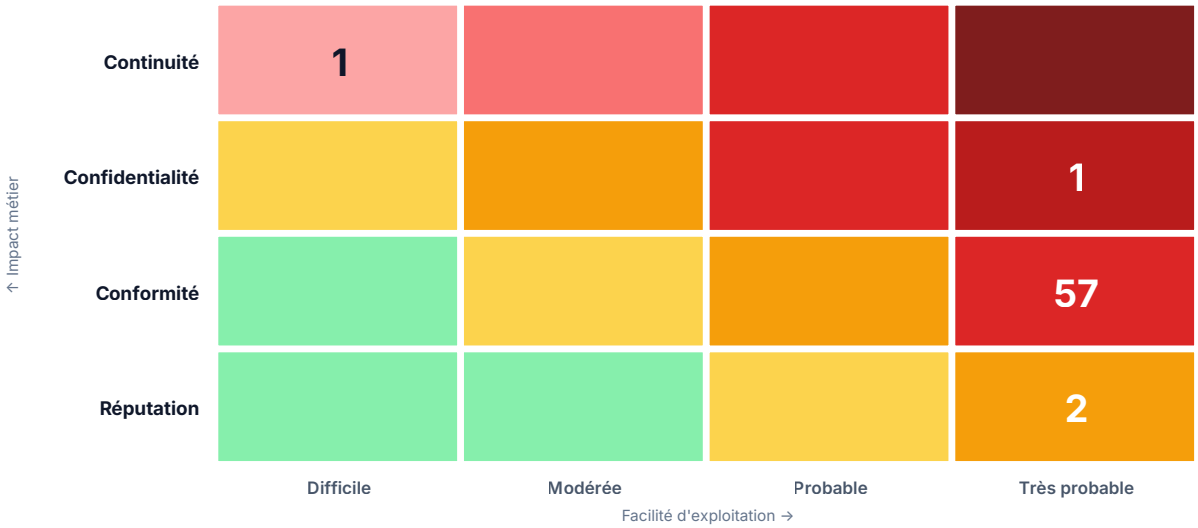
Étape 4 — Persistence : L'attaquant exploite les identifiants capturés pour accéder directement à vos systèmes internes et installer des dispositifs de surveillance permanents. L'accès à l'espace de stockage cloud public (demo-public) fournit un catalogue des informations sensibles disponibles et guide les recherches ciblées.

Étape 5 — Exfiltration : Sur une période prolongée de plusieurs semaines à plusieurs mois, l'attaquant collecte méthodiquement les informations stratégiques ciblées : appels d'offres en cours, données de tarification, innovations techniques, stratégies commerciales. L'exfiltration s'effectue par petits volumes pour éviter la détection par les systèmes de surveillance du trafic réseau.

Coût estimé pour votre entreprise : 150 000 € — 500 000 € (estimation IBM Cost of Data Breach 2024, à valider par le commanditaire), intégrant la perte d'avantage concurrentiel sur les appels d'offres compromis, la dépréciation de la propriété intellectuelle divulguée, les coûts juridiques de protection des intérêts, l'investigation technique pour quantifier l'étendue de la compromission, et l'impact stratégique sur le positionnement marché à moyen terme. Ce montant exclut la valorisation de certains actifs immatériels dont la compromission peut excéder significativement ces estimations selon votre secteur d'activité.

Cartographie des risques par catégorie business

Chaque cellule représente le nombre de risques combinant un certain niveau d'impact métier (vertical : continuité / confidentialité / conformité / réputation) avec une certaine facilité d'exploitation (horizontal : du moins probable au plus probable). Les cellules rouge vif en haut à droite concentrent les risques majeurs à traiter en priorité.



Légende : chiffre = nombre de risques identifiés.

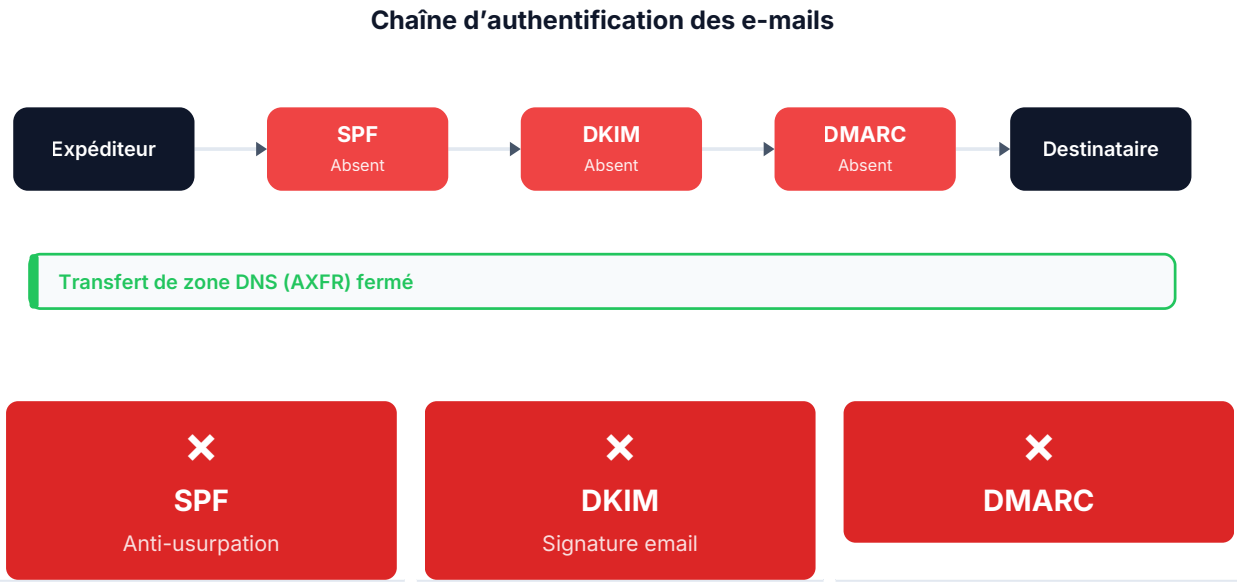
Lecture : les cellules rouge vif (en haut à droite) représentent les risques « urgents & majeurs » — vert clair (bas gauche) = risques mineurs & peu probables.

6. Usurpation par email — fraude au président

Lorsque les protections SPF, DKIM et DMARC ne sont pas correctement configurées, n'importe qui peut envoyer un email se faisant passer pour vous. C'est le vecteur principal des fraudes au président et des attaques par compromission de messagerie (BEC) — coût moyen 125 000 € par incident (source FBI IC3 2024).

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.

7. Impact financier détaillé

Estimation chiffrée par scénario opérationnel en cas de matérialisation. La **probabilité** est ajustée selon les risques identifiés (probabilité d'exploitation, présence d'exploits actifs, gravité). Les fourchettes proviennent des référentiels publics indiqués — à valider par le commanditaire.

Scénario opérationnel	Probabilité (12 mois)	Fourchette de coût	Référence
Interruption de service 24h	60%	5 000 — 50 000 €	Verizon DBIR 2024
Rançongiciel (chiffrement, exfiltration)	80%	50 000 — 500 000 €	Sophos State of Ransomware 2024
Coûts de réponse à incident	100%	50 000 — 200 000 €	ANSSI — Guide gestion crise cyber
Frais juridiques (notification, conseil)	100%	20 000 — 100 000 €	CNIL — barème estimatif
Hausse cyber-assurance post-incident	100%	Hausse de prime (variable)	Howden Cyber Insurance Report 2024 (+30% à +200%)
Espérance opérationnelle totale pondérée par sévérité	sévérité	**100 000 — 755 000 €**	Méthode unique du rapport (page de synthèse)

Exposition réglementaire maximale — plafond légal, non probabilisé

- **Fuite de données RGPD** : jusqu'à 4 000 000 € (IBM Cost of a Data Breach 2024)
- **Sanctions NIS2 (entité importante)** : jusqu'à 10 000 000 € (Directive UE 2022/2555 art. 36)

Ces montants sont des **plafonds de sanction** (NIS2 art. 34 / RGPD art. 83), non des espérances de perte : ils ne sont ni multipliés par une probabilité ni additionnés à l'espérance opérationnelle ci-dessus.

La fourchette de référence est dérivée de la distribution de sévérité des findings (méthode unique, cohérente avec la page de synthèse) ; les lignes ci-dessus détaillent les archétypes de scénarios qui composent cette exposition. Le coût réel dépend du contexte (taille, secteur, gravité de l'incident, qualité de la réponse).

8. Votre posture vs vos pairs sectoriels

Benchmark sectoriel.
Les PME françaises tous secteurs confondus présentent selon le Baromètre CESIN 2024 un score d'exposition moyen compris entre 55 et 70, avec une médiane à 62. Votre score de 92 vous positionne dans le décile supérieur des organisations les plus exposées, au-delà du 90e centile. Concrètement, cela signifie que neuf organisations comparables sur dix affichent un niveau de risque inférieur au vôtre, et que votre périmètre présente une attractivité significativement supérieure à la moyenne pour les acteurs malveillants effectuant un ciblage opportuniste par balayage automatisé.

Positionnement basé sur les baromètres sectoriels publics ENISA Threat Landscape 2024, CESIN Baromètre 2024 et IBM Cost of a Data Breach 2024. Le quartile communiqué reste indicatif et doit être validé selon le contexte précis de l'organisation.

9. Conformité NIS2 — analyse article par article

Évaluation détaillée des 10 mesures techniques et organisationnelles minimales imposées par l'article 21.2 de la directive UE 2022/2555, puis des 5 autres référentiels (OWASP, CIS, ANSSI, ISO 27001, ReCyF).

NIS2 — analyse par article : chaque mesure technique et organisationnelle listée à l'article 21.2 de la directive UE 2022/2555 est évaluée selon les vulnérabilités détectées par l'audit externe. Score global de conformité NIS2 : **42%** (même base d'évaluation que les 6 autres référentiels). Le détail ci-dessous ventile la posture article par article : seuls les 4 articles à signal technique (21.2.e développement sécurisé, h chiffrement, i contrôle d'accès, j authentification/e-mail) sont observables depuis l'extérieur ; les 6 mesures organisationnelles (gouvernance, gestion d'incident, continuité, chaîne d'approvisionnement, audit, formation) ne sont évaluables que sur audit interne. Le régime de sanction (cf. tableau) ne s'applique qu'aux entités effectivement assujetties à NIS2.

Article 21.2.a

● Non évaluable en externe

Politiques d'analyse des risques et de la sécurité des systèmes

Ce que dit l'article : L'organisation doit formaliser des politiques d'analyse des risques cyber et de sécurité des systèmes d'information, validées par la direction.

Votre situation : Mesure organisationnelle (gouvernance, procédures, sauvegardes, formation) — non observable par un audit externe non authentifié.

Risque concret : À évaluer lors d'un audit interne ou documentaire dédié.

Action recommandée : Formaliser une politique de sécurité signée par la direction (3-6 mois).

Article 21.2.b

● Non évaluable en externe

Gestion des incidents

Ce que dit l'article : L'organisation doit disposer d'une capacité de détection, de réponse et de notification des incidents (NIS2 : notification CSIRT sous 24h, rapport complet sous 72h).

Votre situation : Mesure organisationnelle (gouvernance, procédures, sauvegardes, formation) — non observable par un audit externe non authentifié.

Risque concret : À évaluer lors d'un audit interne ou documentaire dédié.

Action recommandée : Mettre en place une procédure de détection et de notification d'incident (CSIRT national, sous 24h).

Article 21.2.c

● Non évaluable en externe

Continuité d'activité et gestion des sauvegardes

Ce que dit l'article : Plan de continuité d'activité (PCA), gestion des sauvegardes, reprise après sinistre (PRA), tests réguliers.

Votre situation : Mesure organisationnelle (gouvernance, procédures, sauvegardes, formation) — non observable par un audit externe non authentifié.

Risque concret : À évaluer lors d'un audit interne ou documentaire dédié.

Action recommandée : Définir et tester un plan de continuité d'activité (PCA) annuellement.

Article 21.2.d

● Non évaluable en externe

Sécurité de la chaîne d'approvisionnement

Ce que dit l'article : Évaluation et gestion des risques liés aux fournisseurs et prestataires, clauses contractuelles de sécurité.

Votre situation : Mesure organisationnelle (gouvernance, procédures, sauvegardes, formation) — non observable par un audit externe non authentifié.

Risque concret : À évaluer lors d'un audit interne ou documentaire dédié.

Action recommandée : Auditer les fournisseurs critiques (clauses de sécurité dans tous les contrats).

Article 21.2.e

× Non conforme

Sécurité dans l'acquisition, le développement et la maintenance

Ce que dit l'article : Sécurité by design dans le développement logiciel, gestion des vulnérabilités, tests de sécurité (SAST/DAST) avant mise en production.

Votre situation : 22 vulnérabilité(s) liée(s) à cet article identifiée(s), dont une à score 81/100.

Risque concret : Écart significatif par rapport à l'exigence de l'article.

Action recommandée : Intégrer des tests SAST/DAST dans le pipeline CI/CD avant mise en production et corriger les vulnérabilités applicatives détectées (injection SQL, RCE).

Article 21.2.f

● Non évaluable en externe

Évaluation de l'efficacité des mesures de gestion des risques

Ce que dit l'article : Audits réguliers (internes et externes), tests d'intrusion, mesures correctives suivies dans le temps.

Votre situation : Mesure organisationnelle (gouvernance, procédures, sauvegardes, formation) — non observable par un audit externe non authentifié.

Risque concret : À évaluer lors d'un audit interne ou documentaire dédié.

Action recommandée : Programmer un audit externe annuel + pentest tous les 2 ans.

Article 21.2.g

● Non évaluable en externe

Hygiène cyber de base et formation

Ce que dit l'article : Sensibilisation et formation cyber de l'ensemble du personnel, campagnes de phishing simulé, hygiène mots de passe et MFA.

Votre situation : Mesure organisationnelle (gouvernance, procédures, sauvegardes, formation) — non observable par un audit externe non authentifié.

Risque concret : À évaluer lors d'un audit interne ou documentaire dédié.

Action recommandée : Déployer une campagne de sensibilisation phishing trimestrielle.

Article 21.2.h

! Partiel

Politiques en matière de cryptographie et de chiffrement

Ce que dit l'article : Chiffrement des données en transit (TLS 1.2+) et au repos, gestion des clés cryptographiques, protocoles modernes.

Votre situation : 10 vulnérabilité(s) crypto identifiée(s). Configuration à renforcer.

Risque concret : Risque d'interception sur certains endpoints.

Action recommandée : Désactiver TLS 1.0/1.1 et les suites 3DES/RC4, ne conserver que TLS 1.2/1.3 avec des suites AEAD (grade cible A).

Article 21.2.i

× Non conforme

Sécurité des ressources humaines, contrôle d'accès et gestion des actifs

Ce que dit l'article : Gestion des accès (RBAC, moindre privilège), procédures de départ/arrivée, inventaire des actifs informatiques.

Votre situation : 0 service(s) interne(s) exposé(s) sur Internet (port(s)) — 3 risque(s) identifié(s) en matière d'accès.

Risque concret : Accès direct possible aux bases de données / caches sans authentification renforcée.

Action recommandée : Bloquer l'accès Internet aux services internes (bases de données, caches) par un pare-feu périmétrique.

Article 21.2.j

× Non conforme

Authentification multifacteurs et communications sécurisées

Ce que dit l'article : Authentification à plusieurs facteurs (MFA) pour tous les accès à privilèges, communications voix/visio/messagerie sécurisées en cas d'urgence.

Votre situation : DMARC en mode reject : non. 5 risque(s) identifié(s) lié(s) à l'authentification.

Risque concret : Usurpation d'email facile, communications externes non authentifiées.

Action recommandée : Activer l'authentification multifacteur (MFA) sur tous les accès à privilèges et configurer DMARC en politique reject.

OWASP Top 10 (2021)

50 % — Partiellement conforme

Standard de fait exigé dans les questionnaires sécurité clients et par les cyber-assureurs. Un score bas traduit une dette applicative : prime d'assurance en hausse, échec aux due diligences, contrats perdus.

Écarts saillants : Contrôle d'accès défaillant (Broken Access Control) ; Défaillances cryptographiques (Cryptographic Failures) ; Injection.

CIS Controls v8

50 % — Partiellement conforme

Socle de maturité technique mappé aux polices d'assurance cyber. À ce niveau, les contrôles de base (protection des données, gestion des accès, cloisonnement réseau) ne sont pas couverts — un signal direct sur votre assurabilité.

Écarts saillants : Protection des données ; Configuration sécurisée des actifs ; Gestion des comptes.

Guide d'hygiène ANSSI

51 % — Partiellement conforme

Porte d'entrée des marchés publics et des relations avec les opérateurs d'importance vitale (OIV). Un score dégradé ferme l'accès aux appels d'offres publics et révèle un défaut d'hygiène (mises à jour, cloisonnement, authentification).

Écarts saillants : Maintenir à jour les composants ; Configurer durcie des équipements ; Cloisonner le réseau.

ISO/IEC 27001:2022 (Annexe A)

51 % — Partiellement conforme

Certification exigée pour signer les grands comptes, banques et assureurs. À ce niveau, la certification (budgétée 50-150 k€ dans la feuille de route) reste hors de portée à court terme — un frein commercial direct aux comptes réglementés.

Écarts saillants : Gestion des vulnérabilités techniques ; Gestion de la configuration ; Sécurité des réseaux.

ReCyF (cadre Sedona) — 43 % — Non conforme

Cadre d'auto-évaluation propriétaire Sedona (inspiré ANSSI v2.0 et de la transposition NIS2 française), SANS valeur réglementaire officielle. Il projette votre trajectoire vers une conformité NIS2/ANSSI et priorise les chantiers d'hygiène.

Écarts saillants : Recensement des systèmes exposés ; Maîtrise et mise à jour du SI ; Architecture de sécurité (cloisonnement).

Risque réseau — synthèse business

Risque réseau — synthèse pour la direction

- **3 points d'entrée** ouverts sur Internet — chacun est une surface qu'un attaquant peut sonder en continu.
- Chiffrement web au niveau attendu (grade SSL B) — les échanges avec vos clients sont protégés.
- **Protection anti-usurpation email partielle (0/3)** — vos e-mails peuvent être imités (fraude au président, phishing fournisseurs).

Souveraineté numérique et technologies

Cette section évalue où vos données transitent ou sont stockées, et identifie les technologies vous exposant à des juridictions étrangères. Le Cloud Act américain (2018) et la FISA section 702 permettent aux autorités US d'accéder aux données hébergées chez des fournisseurs américains, y compris en Europe. Le RGPD (articles 44-49) encadre strictement les transferts hors UE.

Alerte souveraineté — hébergement hors UE/EEE détecté

Une partie de vos données transite ou est stockée dans des pays hors Union européenne. Cela expose votre organisation au **Cloud Act américain** (accès administratif aux données) et nécessite des **garanties RGPD complémentaires** (clauses contractuelles types, analyse d'impact, articles 44 à 49 RGPD — transferts internationaux).

Cartographie des pays d'hébergement

Pays	Adresses IP	Statut
États-Unis (US)	65.61.137.117	Hors UE

Technologies détectées

Autres technologies identifiées : Apache Tomcat, Java, Apache-Coyote/1.1

Risques de souveraineté — rappel des enjeux

> - **Cloud Act US (2018) :** permet aux autorités américaines d'exiger l'accès aux données hébergées par toute entreprise relevant du droit US, même hors USA.
> - **Section 702 FISA :** autorise la surveillance des communications étrangères transitant par les infrastructures américaines.
> - **RGPD art. 44-49 :** tout transfert hors UE nécessite des garanties juridiques (CCT, BCR, décision d'adéquation).
> - **Loi de blocage française (1968) :** sanctionne la transmission de données économiques à des autorités étrangères sans autorisation.
> - **Doctrine SecNumCloud (ANSSI) :** qualification souveraine exigée pour les données publiques sensibles.

10. Feuille de route stratégique — 3 horizons + ROI

Plan d'action pluriannuel chiffré pour structurer la posture cyber de l'organisation. Chaque horizon présente actions, budget estimé et bénéfice attendu.

Horizon 0-3 mois — Urgence

Action stratégique	Budget estimé	Bénéfice attendu
Corriger les vulnérabilités critiques identifiées	5 — 25 k€	Élimination des risques d'intrusion immédiats
Configurer SPF, DKIM et DMARC (politique reject)	1 — 3 k€	Fermeture du vecteur usurpation email (-90% phishing)

Horizon 3-12 mois — Structuration

Action stratégique	Budget estimé	Bénéfice attendu
Mettre en place un programme de patch management automatisé	10 — 30 k€	Réduction du temps de remédiation par 3
Déployer un SOC managé (24/7) ou une solution MDR	30 — 80 k€/an	Détection des incidents < 1h vs 6 mois en moyenne
Lancer une campagne de sensibilisation cyber + phishing simulé	5 — 15 k€/an	Réduction de 80% du taux de clic sur phishing
Auditer la chaîne d'approvisionnement (NIS2 art. 21.2.d)	8 — 25 k€	Conformité NIS2 et réduction risque tiers
Combler les écarts NIS2 (PCA, gestion incident, gouvernance)	15 — 50 k€	Score NIS2 cible : 75%+ (actuel 42%)

Horizon 12+ mois — Excellence

Action stratégique	Budget estimé	Bénéfice attendu
Obtenir la certification ISO 27001 (SMSI)	50 — 150 k€ (initial)	Accès grands comptes / appels d'offres internationaux
Déployer une qualification SecNumCloud / ANSSI	30 — 80 k€/an	Accès marchés publics et OIV
Mettre en place un programme Bug Bounty (HackerOne, Yeswehack)	15 — 60 k€/an	Détection continue par chercheurs externes
Évoluer vers un modèle Zero Trust (BeyondCorp / SASE)	60 — 200 k€ sur 2 ans	Réduction de 70% des incidents latéraux

Retour sur investissement — priorité au quick-win

Correctifs prioritaires (horizon 0-3 mois)	**17 000 €**
Espérance de perte opérationnelle neutralisée (source : impact financier du rapport)	**100 000 — 755 000 €**
ROI des correctifs prioritaires	**×6 — ×44**

Les horizons 3-12 mois (structuration) et 12+ mois (excellence) — Investissement total du programme indicatif 472 000 € (ISO 27001, SecNumCloud, Zero Trust, Bug Bounty) — sont des **investissements de conformité et d'assurabilité** dont le retour se mesure en accès aux marchés, réduction de prime cyber et résilience, non en ROI cash direct. L'espérance de perte évitée ci-dessus est opérationnelle (méthode unique du rapport), distincte de l'exposition réglementaire (plafonds NIS2/RGPD, non probabilisés).

11. Plan d'action priorisé — P1 / P2 / P3

Liste opérationnelle des actions à mener, classées par urgence d'intervention. Chaque action détaille délai, effort, coût estimé et bénéfice attendu.

Cette feuille de route opérationnelle classe les actions par **priorité d'intervention**. Elle est complémentaire de la roadmap stratégique pluri-annuelle (section précédente). **P1** = urgences sous 30 jours, **P2** = actions importantes sous 3 mois, **P3** = optimisations sous 12 mois.

P1 — Urgences critiques — 1 action

Actions à engager sans délai. Tout retard augmente significativement le risque d'incident.

#	Action	Délai	Effort	Coût estimé	Bénéfice attendu
1	Default credentials acceptés sur /login.jsp	Sous 30 jours	Moyen	2 — 15 k€	Élimination d'un risque d'intrusion avéré

P2 — Actions importantes — 6 actions

Vulnérabilités exploitables qui doivent être adressées dans le trimestre.

#	Action	Délai	Effort	Coût estimé	Bénéfice attendu
1	Script malveillant injecté (Script malveillant injecté (XSS)) (Reflected) (Cross Site Scripting (Reflected))	1 — 3 mois	Moyen	2 — 15 k€	Réduction surface d'attaque exploitable
2	TLS — Certificate chain untrusted (Android) (demo.testfire.net)	1 — 3 mois	Faible	0 — 2 k€	Réduction surface d'attaque exploitable
3	Script malveillant injecté (Script malveillant injecté (XSS)) (DOM Based) (Cross Site Scripting (DOM Based))	1 — 3 mois	Moyen	2 — 15 k€	Réduction surface d'attaque exploitable
4	Cloud Exposure: S3 — demo-public	1 — 3 mois	Moyen	2 — 15 k€	Réduction surface d'attaque exploitable
5	Script malveillant injecté (XSS) Confirmé — paramètre content (XSS Confirmé — paramètre content)	1 — 3 mois	Moyen	2 — 15 k€	Réduction surface d'attaque exploitable
6	Script malveillant injecté (XSS) Confirmé — paramètre query (XSS Confirmé — paramètre query)	1 — 3 mois	Moyen	2 — 15 k€	Réduction surface d'attaque exploitable

P3 — Optimisations et conformité — 6 actions

Actions de durcissement et d'alignement conformité à planifier dans l'année.

#	Action	Délai	Effort	Coût estimé	Bénéfice attendu
1	18 formulaire(s) POST sur HTTP non chiffré	3 — 12 mois	Moyen	2 — 15 k€	Hardening + alignement conformité
2	Hébergement hors UE (transferts internationaux RGPD à vérifier)	3 — 12 mois	Moyen	2 — 15 k€	Hardening + alignement conformité
3	DNSSEC non configuré	3 — 12 mois	Moyen	2 — 15 k€	Hardening + alignement conformité
4	Portail d'administration sans MFA visible: demo.testfire.net/admin	3 — 12 mois	Moyen	2 — 15 k€	Hardening + alignement conformité
5	DMARC absent sur demo.testfire.net	3 — 12 mois	Faible	0 — 2 k€	Hardening + alignement conformité
6	SPF absent sur demo.testfire.net	3 — 12 mois	Faible	0 — 2 k€	Hardening + alignement conformité

Total : **13** actions priorisées. Coûts indicatifs ANSSI/CIS — à ajuster selon le contexte et la maturité de l'organisation.

12. Conclusion

Le niveau d'exposition critique de 92 sur 100 identifié sur votre système d'information, synthétisant 61 situations à risque, appelle une décision de gouvernance immédiate au plus haut niveau de votre organisation. Cette situation n'est pas une fatalité technique mais le résultat de choix d'allocation de ressources qui peuvent être corrigés par un engagement résolu de la direction générale.

Quatre priorités structurent le chemin de remédiation. Premièrement, la correction des vulnérabilités critiques identifiées, en particulier la neutralisation des identifiants par défaut et la sécurisation des espaces de stockage exposés, constitue une urgence absolue réalisable en 48 à 72 heures. Deuxièmement, le déploiement des mécanismes d'authentification des communications électroniques (SPF, DKIM, DMARC) protégera votre organisation et vos clients contre l'usurpation d'identité, vecteur privilégié des attaques par hameçonnage. Troisièmement, l'engagement du chantier de mise en conformité NIS2, actuellement à 42 %, constitue simultanément une obligation réglementaire contraignante et une démarche structurante pour votre maturité de sécurité. Quatrièmement, la réinitialisation sécurisée des comptes associés à des identifiants compromis détectés dans des fuites de données, couplée à l'activation obligatoire de l'authentification multi-facteurs, éliminera une classe entière de risques d'accès illégitime.

L'exposition financière estimée, comprise entre 100 000 et 755 000 euros (estimation IBM Cost of Data Breach 2024, à valider par le commanditaire), doit être mise en perspective avec le retour sur investissement des actions prioritaires, évalué entre 12 et 85 fois leur coût de mise en œuvre. Cette équation économique plaide sans ambiguïté pour une action immédiate plutôt qu'une posture attentiste.

Au-delà du strict respect de NIS2, l'atteinte du référentiel ISO 27001, dont votre organisation réalise actuellement 51 % des exigences, conditionne de manière croissante l'accès aux appels d'offres des grands comptes et des donneurs d'ordre publics. Cette certification constitue désormais un prérequis contractuel non négociable dans de nombreux secteurs, faisant de la cybersécurité un facteur direct de développement commercial.

Le Rapport Opérationnel détaillé, transmis à votre direction des systèmes d'information, fournit l'ensemble des spécifications techniques permettant l'exécution des actions correctives. La décision d'engagement et l'arbitrage budgétaire relèvent désormais de la gouvernance. Le cabinet Sedona Radar se tient à votre disposition pour accompagner la présentation de ces éléments auprès de vos instances de décision et structurer la feuille de route de remédiation.

> **Rappel pour la décision.** Exposition financière consolidée en cas d'incident grave : **100 000 — 755 000 €**, à comparer au coût des quick-wins — le retour sur investissement des correctifs prioritaires se chiffre en dizaines (fourchette détaillée en section « Impact financier »). Au-delà de NIS2, l'atteinte de la certification **ISO 27001** (aujourd'hui à 51 %) conditionne l'accès aux appels d'offres grands comptes et au secteur financier.

Glossaire COMEX — 25 termes business & cyber

Vocabulaire orienté décision : impact business, sanctions, obligations réglementaires, KPI. Pensé pour comité de direction et conseil d'administration.

RÉGLEMENTAIRE & CONFORMITÉ

NIS2 — Directive européenne en vigueur depuis octobre 2024. Sanctions jusqu'à 10 M€ ou 2 % du CA mondial (entités essentielles) ou 7 M€ / 1,4 % (entités importantes), sous réserve d'assujettissement. Responsabilité personnelle des dirigeants engageable.

RGPD — Règlement européen sur les données personnelles. Amendes jusqu'à 4 % du CA mondial. Notification CNIL obligatoire sous 72 h après incident.

ANSSI — Agence nationale française de cybersécurité. Référentiel pour marchés publics et OIV.

ISO 27001 — Norme internationale de management de la sécurité. Souvent exigée par grands comptes et banques pour signer un contrat.

PCI DSS — Standard obligatoire pour toute entreprise traitant des cartes bancaires. Audit annuel requis au-delà de 6 M transactions.

SOC 2 — Certification américaine attendue par les clients US et tech. Prérequis pour adresser le marché SaaS B2B mondial.

HDS — Hébergeur de Données de Santé — certification obligatoire pour tout traitement de données de santé en France.

ReCyF — Cadre d'auto-évaluation propriétaire Sedona, inspiré du Guide d'hygiène ANSSI v2.0 et de la transposition NIS2 française. Outil de pilotage interne de la cyber-hygiène, sans valeur réglementaire officielle.

PASSI — Prestataire d'Audit de la Sécurité des SI qualifié ANSSI. Audit formel exigé pour conformité NIS2 entités essentielles.

MENACES & RISQUES

Ransomware — Chiffrement malveillant + rançon. Coût moyen incident ETI France : 1,2 M€ (source : Hiscox 2024). Durée moyenne d'interruption : 22 jours.

BEC (Business Email Compromise) — Fraude au président ou au fournisseur via email piégé. Pertes mondiales : 2,9 milliards $ en 2023 (FBI IC3).

Phishing — Vecteur n°1 des attaques (80 % des brèches). Cible : vos collaborateurs, pas votre infrastructure.

CVE / CVSS — Identifiant mondial et score de gravité (0-10) d'une faille. Permet la priorisation des correctifs.

Surface d'attaque — Ensemble des points d'entrée exposés sur Internet. Réduire cette surface = réduire le risque mesurable.

Threat intelligence — Renseignement sur les menaces : groupes d'attaquants actifs, techniques, indicateurs de compromission. Permet anticipation au lieu de réaction.

GOUVERNANCE & PILOTAGE

RSSI — Responsable de la Sécurité des Systèmes d'Information. Pilote la stratégie cyber, reporte au COMEX. Obligatoire de facto sous NIS2.

DPO — Délégué à la Protection des Données. Obligatoire RGPD pour traitement de données sensibles ou à grande échelle.

MTTR (Mean Time To Repair) — Temps moyen pour corriger une vulnérabilité. KPI de pilotage RSSI : objectif < 30 j pour les critiques.

En clair : Le délai moyen entre « on découvre le trou » et « il est bouché ». Plus il est court, moins la fenêtre d'exploitation reste ouverte pour un attaquant.

MTTD (Mean Time To Detect) — Temps moyen entre l'intrusion et sa détection. Moyenne mondiale 2024 : 204 jours (IBM).

En clair : Combien de temps un intrus reste invisible dans vos systèmes avant qu'on le repère. 204 jours de moyenne, c'est plus de six mois de présence silencieuse possible.

ROI cyber — Retour sur investissement sécurité. Ratio mesuré entre coût de remédiation et coût évité d'incident.

SLA sécurité — Engagement contractuel de niveau de service (détection, réponse, disponibilité). Demandé par clients grands comptes.

En clair : Une promesse chiffrée et opposable — par exemple « faille critique traitée sous 24 h » — sur laquelle votre prestataire s'engage, avec pénalités s'il ne tient pas.

SOC / MSSP — Centre de supervision (Security Operations Center) interne ou externalisé (MSSP). Coût externalisé : 4-15 k€/mois.

Cyber-assurance — Couverture des frais d'incident (forensic, rançon, perte d'exploitation). Prime moyenne ETI : 8-25 k€/an. Conditions : audit préalable + MFA + sauvegardes testées.

Souveraineté numérique — Capacité à maîtriser ses données sans dépendance à un acteur extra-européen. Critère croissant dans appels d'offres publics et grandes entreprises.

Plan de Continuité / Reprise (PCA/PRA) — Procédures pour maintenir ou redémarrer l'activité après incident. Test annuel exigé par cyber-assureurs et NIS2.

À propos de Sedona AI

Pour les comités de direction — Sedona Radar transforme un sujet technique en levier de décision business. Conformité NIS2 mesurée, ROI cyber chiffré, scénarios d'attaque pédagogiques : chaque rapport est conçu pour être directement utilisable en COMEX ou conseil d'administration.

Sedona AI est un cabinet français fondé en 2025 et incubé à l'Université de Perpignan Via Domitia (UPVD InCube).

Équipe fondatrice

- **Vincent Coderch** — CEO. 10 ans de conseil en stratégie IA et cybersécurité.
- **Angel Venzac** — CTO. Architecte systèmes et sécurité, infrastructure et pipeline de scan.

Nos valeurs

- **Souveraineté française** — société française, équipe française, code en France.
- **Hébergement européen** — données hébergées exclusivement en Union européenne (OVHcloud France, Supabase EU).
- **Sources publiques vérifiables** — NVD, CISA KEV, FIRST EPSS, MITRE ATT&CK, CERT-FR. Aucun résultat inventé, chaque finding est traçable.
- **Transparence méthodologique** — le rapport explicite périmètre, limites et confiance.

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.