

SEDONA RADAR

Rapport Opérationnel

AUDIENCE : DSI / RSSI / ÉQUIPES SÉCURITÉ

Détail technique exhaustif, CVE/CVSS/EPSS, méthodologie, contrôles de conformité

demo.testfire.net

SCORE D'EXPOSITION

92 / 100

CRITIQUE

Référence : SR-98819F7E-20260729

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

Plateforme : Sedona Radar v3

CONFIDENTIEL — Diffusion restreinte

Table des matières

Tableau de bord technique	3
Cadre technique de l'audit	4
Vulnérabilités identifiées — 61 findings	5
Cockpit d'exploitabilité	18
Chaîne d'attaque MITRE ATT&CK	19
Matrice CVSS × EPSS × KEV	20
Analyse de conformité technique	21
Détail par référentiel — OWASP, CIS, ANSSI, ISO 27001, ReCyF	38
Infrastructure et surface d'attaque	44
Renseignement ouvert (OSINT)	49
Remédiation	50
Conclusion	52
Glossaire technique DSI / RSSI — 30 termes	58
À propos de Sedona AI	60
Annexe E — Mentions légales (synthèse)	62
E.1 — Nature de la prestation	62
E.4 — Absence de garantie d'exhaustivité	62
E.7 — Responsabilité du commanditaire	62
E.8 — Limitation de responsabilité de Sedona AI	62
E.14 — Absence de garantie d'absence d'incident futur	63
Autres clauses (synthèse)	63

Tableau de bord technique

Synthèse quantitative de l'audit : score composite global (base pondérée CVSS v3.1 × 50 % + EPSS × 30 %, puis bonus +25 pts (CISA KEV) / +15 pts (module Metasploit) / +10 pts (exploit public / PoC)), volumétrie par sévérité, surface mesurée (sous-domaines, ports, grade SSL), couverture des sources d'enrichissement (NVD, FIRST EPSS, CISA KEV, MITRE ATT&CK).

Score composite global	92/100 (zone critique)
Vulnérabilités totales	61 (1 critique, 7 élevées, 2 moyennes, 22 faibles, 29 informationnelles)
Vulnérabilités CISA KEV	0 (exploitées activement)
Sous-domaines découverts	1
Ports ouverts	3 (80, 443, 8080)
Grade SSL/TLS	B
WAF/CDN	aucun détecté
Nuclei templates	17 exécutés

Cadre technique de l'audit

Audit non destructif de la surface externe, conforme aux méthodologies PTES (Penetration Testing Execution Standard), OWASP Testing Guide v4.2 et NIST SP 800-115. Reconnaissance passive + scan actif de vulnérabilité. Aucune exploitation aboutie, aucun déni de service, aucune modification de données ni exécution de code.

Cible	demo.testfire.net
Date	2026-07-29 15:59 UTC
Mode	Audit de surface externe (reconnaissance passive + scan actif non destructif)
Sous-domaines	1 découverts
Ports	80, 443, 8080

Outils mobilisés

Recon: Subfinder, Amass, HTTPX, Masscan, Nmap, theHarvester • Web: Nuclei (7000+ templates), Nikto, Feroxbuster, ZAP, SQLmap, Arjun, Katana • SSL: testssl.sh, SSLyze • DNS: DNSx, dig • Infra: OpenVAS (210K+ plugins), WPScan, WhatWeb, Wafw00f • OSINT: Shodan, GreyNoise, AbuseIPDB, VirusTotal, Gitleaks, TruffleHog, S3Scanner • Scoring: NVD, EPSS, CISA KEV, ExploitDB, MITRE ATT&CK

Limites

- Surface externe uniquement — pas d'audit interne/AD/OT
- Résultats point-in-time
- Pas d'audit de code source
- Pas de social engineering

Vulnérabilités identifiées — 61 findings

1 critique, 7 élevées, 2 moyennes, 22 faibles, 29 informationnelles. Score d'exposition : 92/100 (zone critique).

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, la remédiation concrète et le mapping vers les référentiels de conformité applicables (MITRE ATT&CK, OWASP, NIS2, ANSSI).

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 critique — 1 vulnérabilité

Default credentials acceptés sur /login.jsp

95

/100 — Critique

Score composite	95/100
CVSS estimé (base interne)	9.5
CWE	CWE-521
Service	web
Hôte	demo.testfire.net
Détecté par	default-creds-scanner
Confiance	80%

Description technique

Le formulaire de login à `https://demo.testfire.net/login.jsp` accepte la paire ``jsmith / demo1234`` (différence response significative vs paire invalide). C'est une des paires default les plus connues (``admin/admin``, ``admin/password``, etc.). Tout attaquant peut se connecter au panel d'administration en quelques secondes.

Preuve / Constat

```
POST https://demo.testfire.net/doLogin avec credentials `jsmith / demo1234` →  
status=302 (wrong_password = status=302, body_diff=0 bytes)
```

Remédiation — Planifier lors de la prochaine maintenance

- Corriger la configuration selon les recommandations de l'outil de détection.

Mapping conformité

- MITRE ATT&CK : Initial Access / T1078.001 — Valid Accounts: Default Accounts
- OWASP : A07
- NIS2 : Art. 21.2.i
- ANSSI : R3
- CWE : CWE-521

Findings de sévérité élevée — 7 vulnérabilités

Script malveillant injecté (Script malveillant injecté (XSS)) (Reflected) (Cross Site Scripting (Reflected))

81

/100 — Élevé

Score composite	81/100
CVSS estimé (base interne)	7.5
CWE	CWE-79
Service	http
Hôte	demo.testfire.net
Détecté par	zap:40012
Confiance	80%

Description technique

Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an email client. The code itself is usually written in HTML/JavaScript, but may also extend to VBScript, ActiveX, Java, Flash, or any other browser-supported technology. When an attacker gets a user's browser to

Preuve / Constat

URLs: <https://demo.testfire.net/sendFeedback> | Param: name

Remédiation — Planifier lors de la prochaine maintenance

- Corriger la configuration selon les recommandations de l'outil de détection.

Mapping conformité

- MITRE ATT&CK : Initial Access / T1189 — Drive-by Compromise
- OWASP : A03
- NIS2 : Art. 21.2.e
- ANSSI : R24
- CWE : CWE-79

TLS — Certificate chain untrusted (Android) (demo.testfire.net)

81

/100 — Élevé

Score composite 81/100**CVSS estimé (base interne)** 7.5**CWE** CWE-310**Service** https://demo.testfire.net:443**Hôte** demo.testfire.net**Détecté par** ssl-audit**Confiance** 80%

Description technique

Certificate chain does not validate against trust store.

Preuve / Constat

```
sslyze: path validation failed for Android
```

Remédiation — Planifier lors de la prochaine maintenance

- Mettre à jour la configuration TLS : désactiver les protocoles/ciphers obsolètes.

Vérification : Tester avec testssl.sh ou SSLabs.

Mapping conformité

- MITRE ATT&CK : Credential Access / T1557 — Adversary-in-the-Middle
- OWASP : A02
- NIS2 : Art. 21.2.h
- ANSSI : R16
- CWE : CWE-310

18 formulaire(s) POST sur HTTP non chiffré

81

/100 — Élevé

Score composite	81/100
CWE	CWE-319
Service	http
Hôte	demo.testfire.net
Détecté par	gdpr-scanner
Confiance	95%

Description technique

URLs concernées : <http://demo.testfire.net/admin/login.aspx%E2%80%93>, <http://demo.testfire.net/admin/login.aspx/.htaccess.aspx->, <http://demo.testfire.net/admin/login.aspx/login.aspx> (+15 autres).

Remédiation

Migrer vers HTTPS + HSTS + redirect 301 systématique.

Mapping conformité

- NIS2 : Art. 21.2.h
- CWE : CWE-319

Script malveillant injecté (Script malveillant injecté (XSS)) (DOM Based) (Cross Site Scripting (DOM Based))

81

/100 — Élevé

Score composite	81/100
CVSS estimé (base interne)	7.5
CWE	CWE-79
Service	http
Hôte	demo.testfire.net
Détecté par	zap:40026
Confiance	80%

Description technique

Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an email client. The code itself is usually written in HTML/JavaScript, but may also extend to VBScript, ActiveX, Java, Flash, or any other browser-supported technology. When an attacker gets a user's browser to

Preuve / Constat

```
URLs: https://demo.testfire.net/#jaVaScRipt:/*-/*`/*\`/*'/*"/**/(/* */
oNcliCk=alert(5397) )//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!
>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
```

Remédiation — Planifier lors de la prochaine maintenance

- Corriger la configuration selon les recommandations de l'outil de détection.

Mapping conformité

- MITRE ATT&CK : Initial Access / T1189 — Drive-by Compromise
- OWASP : A03
- NIS2 : Art. 21.2.e
- ANSSI : R24
- CWE : CWE-79

Cloud Exposure: S3 — demo-public

80

/100 — Élevé

Score composite	80/100
CVSS estimé (base interne)	7.5
Service	s3
Détecté par	cloud-scanner:s3
Confiance	70%

Description technique

Public s3 resource detected. Status: exposed. Permissions publiques actives : perm_all_users_read. Output: {"bucket":{"name":"demo-public","region":"eu-west-1","exists":1,"date_scanned":"2026-07-29T15:54:32.490441918Z","objects":null,"objects_enumerated":

Remédiation — Planifier lors de la prochaine maintenance

- Corriger la configuration selon les recommandations de l'outil de détection.

Mapping conformité

- MITRE ATT&CK : Initial Access / T1190 — Exploit Public-Facing Application
- NIS2 : Art. 21.2.e
- ANSSI : R24

Script malveillant injecté (XSS) Confirmé — paramètre content (XSS Confirmé — paramètre content)

80

/100 — Élevé

Score composite	80/100
CVSS estimé (base interne)	7.5
CWE	CWE-79
Service	http
Hôte	demo.testfire.net
Détecté par	dalfox

Description technique

Une faille XSS Confirmé a été confirmée par Dalfox sur le paramètre « content ». Cette vulnérabilité permet à un attaquant d'injecter du code JavaScript arbitraire dans les pages vues par les utilisateurs. Le code malveillant s'exécute dans le navigateur de la victime avec les mêmes privilèges que l'utilisateur connecté.

Preuve / Constat

```
URL : https://demo.testfire.net/index.jsp?
content=%3Cdetails%20open%20ontoggle%3Dalert%281%29%20class%3Ddlx56e4b5a5%3E&job=
ExecutiveAssistant%3AAdministration
Payload : <details open ontoggle=alert(1) class=dlx56e4b5a5>
Type d'injection : inHTML
```

Remédiation — Planifier lors de la prochaine maintenance

- Corriger la configuration selon les recommandations de l'outil de détection.

Mapping conformité

- MITRE ATT&CK : Initial Access / T1189 — Drive-by Compromise
- OWASP : A03
- NIS2 : Art. 21.2.e
- ANSSI : R24
- CWE : CWE-79

Script malveillant injecté (XSS) Confirmé — paramètre query (XSS Confirmé — paramètre query)

80

/100 — Élevé

Score composite	80/100
CVSS estimé (base interne)	7.5
CWE	CWE-79
Service	http
Hôte	demo.testfire.net
Détecté par	dalfox

Description technique

Une faille XSS Confirmé a été confirmée par Dalfox sur le paramètre « query ». Cette vulnérabilité permet à un attaquant d'injecter du code JavaScript arbitraire dans les pages vues par les utilisateurs. Le code malveillant s'exécute dans le navigateur de la victime avec les mêmes privilèges que l'utilisateur connecté.

Preuve / Constat

```
URL : http://demo.testfire.net/search.jsp?
query=%3Csvg%20onload%3Dalert%281%29%20class%3Ddlx56e4b5a5%3E
Payload : <svg onload=alert(1) class=dlx56e4b5a5>
Type d'injection : inHTML
```

Remédiation — Planifier lors de la prochaine maintenance

- Corriger la configuration selon les recommandations de l'outil de détection.

Mapping conformité

- MITRE ATT&CK : Initial Access / T1189 — Drive-by Compromise
- OWASP : A03
- NIS2 : Art. 21.2.e
- ANSSI : R24
- CWE : CWE-79

Findings de sévérité moyenne — 2 vulnérabilités

Ces vulnérabilités présentent un risque modéré. Elles doivent être traitées dans un délai de 30 à 90 jours dans le cadre d'un plan de remédiation structuré. Le détail technique de chaque finding (description, remédiation, mapping conformité) reste disponible dans le tableau de bord en ligne — le tableau ci-dessous synthétise les informations essentielles pour la priorisation.

Risque	Titre & contexte	Remédiation
MOY 67	Deprecated TLS Detection http	
MOY 32	Hébergement hors UE (transferts internationaux RGD à vérifier) infra	Documenter les Clauses Contractuelles Types (CCT) avec le fournisseur. Considérer hébergement EU-west (AWS Frankfurt, OVH Gravelines, Scaleway Paris) pour les données sensibles.

Findings de sévérité faible — 51 vulnérabilités

Ces observations représentent un risque faible. Elles correspondent généralement à des fuites d'information mineures ou des bonnes pratiques non respectées. Leur correction peut être planifiée à plus long terme.

Risque	Titre & contexte	Remédiation
FAI 32	DNSSEC non configuré	Activer DNSSEC auprès de votre registrar ou hébergeur DNS : 1) Générer les clés DNSSEC (KSK et ZSK) ; 2) Signer la zone DNS ; 3) Publier l'enregistrement DS dans la zone parente via le registrar ; 4) Vérifier avec &
FAI 32	Portail d'administration sans MFA visible: demo.testfire.net/admin web	
FAI 32	DMARC absent sur demo.testfire.net DNS	Restreindre / corriger : Ajouter : _dmarc.demo.testfire.net IN TXT "v=DMARC1; p=quarantine; rua=mailto:dmarc@demo.testfire.net"
FAI 32	SPF absent sur demo.testfire.net DNS	Restreindre / corriger : Ajouter un enregistrement TXT SPF : v=spf1 include:_spf.provider.net -all
FAI 32	Deprecated TLS protocol — TLS 1.0 (demo.testfire.net) https://demo.testf	Désactiver TLS 1.0 dans la config TLS, forcer TLS 1.2+ minimum.
FAI 32	Deprecated TLS protocol — TLS 1.1 (demo.testfire.net) https://demo.testf	Désactiver TLS 1.1 dans la config TLS, forcer TLS 1.2+ minimum.
FAI 24	Cookie sans attribut SameSite http	Ajouter `SameSite=Strict` (ou `SameSite=Lax` si redirections externes nécessaires) sur tous les cookies. Ex: `Set-Cookie: session=...; SameSite=Strict; Secure; HttpOnly`. Bloque les requêtes cross-site qui sont la racine
FAI 22	Divulgateion d'information : server http	Masquer l'en-tête `server` côté serveur ou reverse-proxy. Nginx : `server_tokens off; more_clear_headers 'server';`. Apache : `ServerTokens Prod` + `l'en-tête unset server`. Réduit l'info utile
FAI 22	Absence of Anti-Requête falsifiée (CSRF) Tokens (Absence of Anti-CSRF Tokens) http	Phase: Architecture and Design Utilisez a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. For example, Utilisez anti-CSRF packages te

Risque	Titre & contexte	Remédiation
FAI 18	Cross-Domain JavaScript Source File Inclusion http	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end utilisateurs of the application.
FAI 18	Expired SSL Certificate http	
FAI 18	Chiffrement faible Suites Detection (Weak Cipher Suites Detection) http	
FAI 18	Secure Pages Include Mixed Content (×2 URLs) http	Restreindre / corriger : A page that is available over SSL/TLS must be comprised completely of content which is transmitted over SSL/TLS. The page must not contain any content that is transmitted over unencrypted HT
FAI 18	En-tête de sécurité manquant : content-security-policy http	Définir une CSP stricte : `Content-Security-Policy: default-src 'self'; script-src 'self'; style-src 'self'; img-src 'self' data;; connect-src 'self'; frame-ancestors &#x`
FAI 18	En-tête de sécurité manquant : x-content-type-options http	Ajouter `X-Content-Type-Options: nosniff`. Empêche le navigateur de deviner le MIME type (prévient l'exécution de scripts cachés dans des assets servis avec un mauvais type).
FAI 18	En-tête de sécurité manquant : x-frame-options http	Ajouter `X-Frame-Options: DENY` (ou `SAMEORIGIN` si l'iframe interne est nécessaire). Équivalent moderne via CSP : `frame-ancestors 'none'`. Protège contre le clickjacking.
FAI 18	Secure Pages Include Mixed Content (Including Scripts) http	Restreindre / corriger : A page that is available over SSL/TLS must be comprised completely of content which is transmitted over SSL/TLS. The page must not contain any content that is transmitted over unencrypted HT
FAI 18	Aucun WAF/CDN détecté en frontal 80/tcp	Déployer un WAF en frontal (Cloudflare, ModSecurity, AWS WAF).
FAI 18	Reflected Script malveillant injecté (Script malveillant injecté (XSS)) (Reflected Cross-Site Scripting) http	
FAI 18	Absence de rate-limiting détectée web	
FAI 18	En-tête de sécurité manquant : strict-transport-security http	Ajouter l'en-tête `Strict-Transport-Security: max-age=63072000; includeSubDomains; preload` côté serveur (nginx: `add_header Strict-Transport-Security ...;`, Apache: `l'en-tête always Définissez ...`).
FAI 12	security.txt manquant (RFC 9116) web	Créer un fichier <code>/.well-known/security.txt</code> avec au minimum les champs Contact, Expires (>1y), Preferred-Languages.
INF 10	Fuite d'information - Suspicious Comments (×7 URLs) (Information Disclosure - Suspicious Comments (×7 URLs)) http	Supprimez all comments that return information that may help an attacker and fix any underlying problems they refer to — (suite tronquée par la longueur)
		1. Valider stricte/whitelist tous les paramètres acceptés. 2. Authentification + autorisation par

Risque	Titre & contexte	Remédiation
INF 10	API parameter discovered: customize.jsp (2 params)	endpoint sensible. 3. Rate limit par utilisateur sur API critique.
INF 10	API parameter discovered: Privacypolicy.aspx (3 params)	1. Valider stricte/whitelist tous les paramètres acceptés. 2. Authentification + autorisation par endpoint sensible. 3. Rate limit par utilisateur sur API critique.
INF 10	API parameter discovered: search.jsp (1 params)	1. Valider stricte/whitelist tous les paramètres acceptés. 2. Authentification + autorisation par endpoint sensible. 3. Rate limit par utilisateur sur API critique.
INF 10	Fuite d'information - Suspicious Comments (Information Disclosure - Suspicious Comments) http	Supprimez all comments that return information that may help an attacker and fix any underlying problems they refer to — (suite tronquée par la longueur)
INF 10	API parameter discovered: Privacypolicy.jsp (2 params)	1. Valider stricte/whitelist tous les paramètres acceptés. 2. Authentification + autorisation par endpoint sensible. 3. Rate limit par utilisateur sur API critique.
INF 10	Public Swagger API - Detect http	Limiter les informations exposées : retirer les headers verbose (Server, X-Powered-By), désactiver mode debug, contrôler les pages d'erreur génériques. Audit régulier des assets publics.
INF 10	API parameter discovered: default.aspx (2 params)	1. Valider stricte/whitelist tous les paramètres acceptés. 2. Authentification + autorisation par endpoint sensible. 3. Rate limit par utilisateur sur API critique.
INF 10	WAF Detection http	Limiter les informations exposées : retirer les headers verbose (Server, X-Powered-By), désactiver mode debug, contrôler les pages d'erreur génériques. Audit régulier des assets publics.
INF 5	Re-examine Cache-control Directives http	For secure content, ensure the cache-control HTTP l'en-tête is Définissez with "no-cache, no-store, must-revalidate". If an asset should be cached Envisagez setting the directives "public, max
INF 5	Modern Web Application (×2 URLs) http	Restreindre / corriger : This is an informational alert and so no changes are required.
INF 5	javascript finding @ demo.testfire.net http	
INF 5	Re-examine Cache-control Directives (×2 URLs) http	For secure content, ensure the cache-control HTTP l'en-tête is Définissez with "no-cache, no-store, must-revalidate". If an asset should be cached Envisagez setting the directives "public, max
INF 5	Missing Cookie SameSite Strict http	Configurer les headers HTTP de sécurité : CSP (Content-Security-Policy), X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy.
	ssl finding @ demo.testfire.net http	

Risque	Titre & contexte	Remédiation
INF 5		
INF 5	Session Management Response Identified (×2 URLs) <code>http</code>	This is an informational alert rather than a vulnérabilité and so there is nothing to fix.
INF 5	HTTP Missing Security Headers	Configurer les headers HTTP de sécurité : CSP (Content-Security-Policy), X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy.
INF 5	Modern Web Application <code>http</code>	Restreindre / corriger : This is an informational alert and so no changes are required.
INF 5	Apache Detection <code>http</code>	
INF 5	Session Management Response Identified (×4 URLs) <code>http</code>	This is an informational alert rather than a vulnérabilité and so there is nothing to fix.
INF 5	Re-examine Cache-control Directives (×8 URLs) <code>http</code>	For secure content, ensure the cache-control HTTP l'en-tête is Définissez with "no-cache, no-store, must-revalidate". If an asset should be cached Envisagez setting the directives "public, max
INF 5	http finding @ demo.testfire.net	
INF 5	Session Management Response Identified <code>http</code>	This is an informational alert rather than a vulnérabilité and so there is nothing to fix.
INF 5	Re-examine Cache-control Directives (×5 URLs) <code>http</code>	For secure content, ensure the cache-control HTTP l'en-tête is Définissez with "no-cache, no-store, must-revalidate". If an asset should be cached Envisagez setting the directives "public, max
INF 5	Cookies without Secure attribute - Detect <code>http</code>	
INF 5	Session Management Response Identified (×5 URLs) <code>http</code>	This is an informational alert rather than a vulnérabilité and so there is nothing to fix.
INF 4	Modern Web Application (×3 URLs) <code>http</code>	Restreindre / corriger : This is an informational alert and so no changes are required.
INF 4	Session Management Response Identified (×7 URLs) <code>http</code>	This is an informational alert rather than a vulnérabilité and so there is nothing to fix.
INF 4	Surface d'attaque : sous-domaines découverts par BBOT <code>dns</code>	Étape 1 — Inventorier tous les sous-domaines et vérifier leur légitimité Étape 2 — Supprimer les entrées DNS des sous-domaines non utilisés Étape 3 — Mettre en place un monitoring Certificate Transparency

Cockpit d'exploitabilité

Vue d'ensemble de l'exploitabilité réelle des vulnérabilités détectées. Ces 4 zones permettent de prioriser les actions au-delà du seul score CVSS.

Zone	Critère	Compteur	Top 3 vulnérabilités
OK — Exploitation active	aucune vulnérabilité dans cette zone, c'est un bon signe (Présent dans CISA KEV).		
Exploitation probable	EPSS > 0.5 (30j)	1	Deprecated TLS Detection (CVE-2014-3566)
OK — Exploit public disponible	aucune vulnérabilité dans cette zone, c'est un bon signe (exploit-db / github / metasploit).		
OK — SLA dépassé	aucune vulnérabilité dans cette zone, c'est un bon signe (due_date < aujourd'hui).		

Chaîne d'attaque MITRE ATT&CK

Répartition des techniques MITRE ATT&CK observées sur les 7 phases de la kill chain Sedona. Plus une phase est rouge, plus l'attaquant dispose d'options pour cette étape de son attaque.

Reconnais- sance	Pénétration	Exécution	Maintien	Propagation	Collecte / C2	Exfiltration / Impact
17	20	0	0	16	0	0

Lecture : les compteurs à 0 indiquent que la surface externe n'expose pas d'éléments observables à ces étapes — la fenêtre d'attaque détectable se concentre sur les phases initiales. Ce déséquilibre est typique d'un audit externe non-authentifié : les phases post-intrusion (maintien, collecte, exfiltration) ne sont mesurables qu'avec une sonde interne.

Lecture compteurs : chaque compteur = nombre de findings dont la tactique MITRE est rattachée à cette phase. Le détail des techniques observées est ci-dessous, phase par phase active.

Reconnaissance — 17 technique(s) observée(s)

L'attaquant identifie et étudie sa cible

- T1592 — Gather Victim Host Information ×14
- T1596.001 — Search Open Technical Databases: DNS/Passive DNS ×3

Pénétration — 20 technique(s) observée(s)

Première intrusion via une faille ou un identifiant volé

- T1189 — Drive-by Compromise ×9
- T1190 — Exploit Public-Facing Application ×8
- T1190 — Exploit Public-Facing Application — CSRF ×2

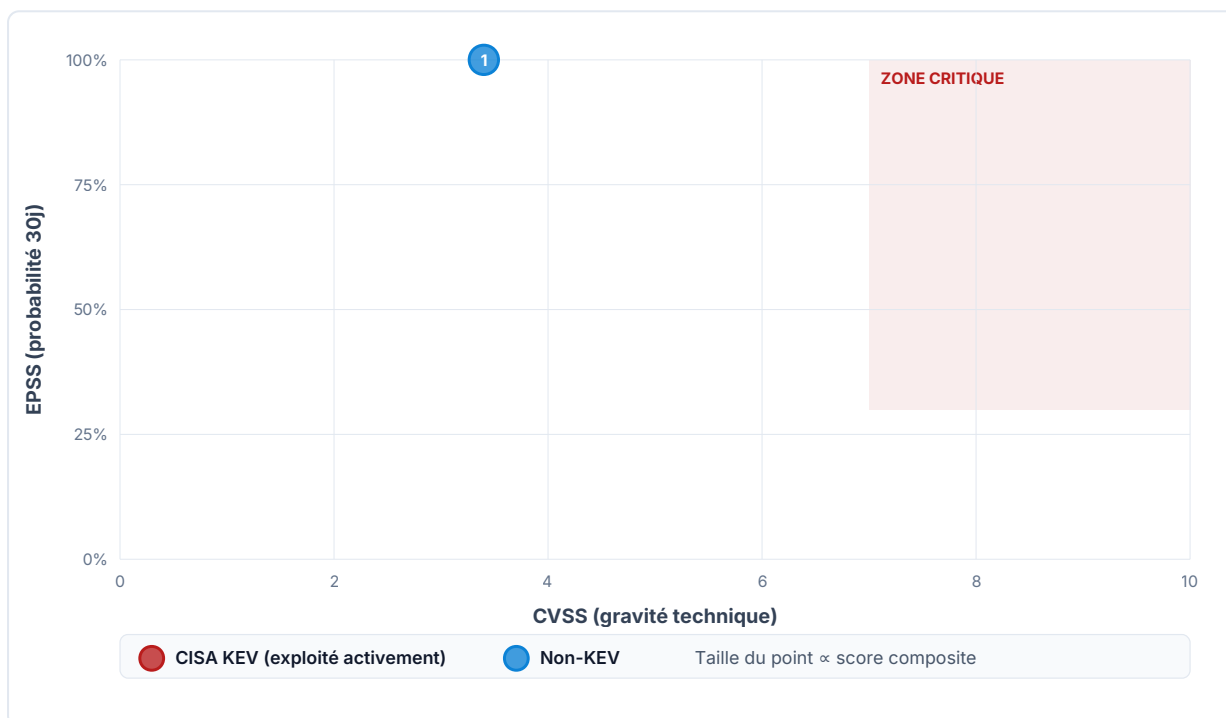
Propagation — 16 technique(s) observée(s)

Vol d'identifiants et déplacement latéral

- T1557 — Adversary-in-the-Middle ×10
- T1552 — Unsecured Credentials ×6

Matrice CVSS × EPSS × KEV

Cartographie des vulnérabilités disposant à la fois d'un score CVSS et d'une probabilité EPSS — axe X : score CVSS, axe Y : probabilité EPSS d'exploitation à 30 jours, taille du point : score composite, couleur : présence dans la liste CISA KEV (rouge = exploité activement). Les vulnérabilités sans probabilité EPSS établie ne sont pas tracées (aucune position inventée).



Données partielles. 1 vulnérabilité(s) sur 10 disposent des enrichissements CVSS+EPSS requis. Lancez un nouveau scan avec enrichissement NVD + FIRST.org EPSS pour densifier ce graphique.

Pourquoi la matrice est peu dense ? 1 point(s) sur 10 affichés — la majorité de vos findings sont des misconfigurations sans CVE associée (en-têtes HTTP manquants, CSP, SRI). Les CVE positionnées correspondent à des bibliothèques tierces obsolètes (jQuery, etc.). Pour densifier l'analyse, voir la section « Vulnérabilités identifiées ».

1. 1. Deprecated TLS Detection (CVE-2014-3566) — score 67

Analyse de conformité technique

Cette section évalue la posture de conformité de l'organisation vis-à-vis de 6 référentiels de cybersécurité reconnus. **Les référentiels ne sont pas évalués en totalité depuis la surface externe** : certains contrôles (organisationnels, physiques, internes) nécessitent un accès au réseau interne ou aux processus de l'entreprise pour être mesurés. Les scores ci-dessous reflètent uniquement la partie évaluable en audit externe.

Chaque référentiel est évalué sur les contrôles applicables en externe. Le score reflète le pourcentage de conformité sur ces contrôles. Les écarts identifiés (gaps) sont détaillés avec leur risque associé et la remédiation recommandée.

Scores de conformité

NIS2

Non conforme

4 articles techniques sur 10 évaluables en externe

42%

OWASP 2021

Partiellement conforme

7 catégories sur 10 évaluables en externe

50%

OWASP 2025

Partiellement conforme

7 catégories sur 10 évaluables en externe (édition 2025)

50%

CIS

Partiellement conforme

12 contrôles sur 18 évaluables en externe

50%

ANSSI

Partiellement conforme

16 mesures sur 42 évaluables en externe

51%

ISO 27001

Partiellement conforme

13 contrôles Annexe A évaluables en externe

51%

ReCyF

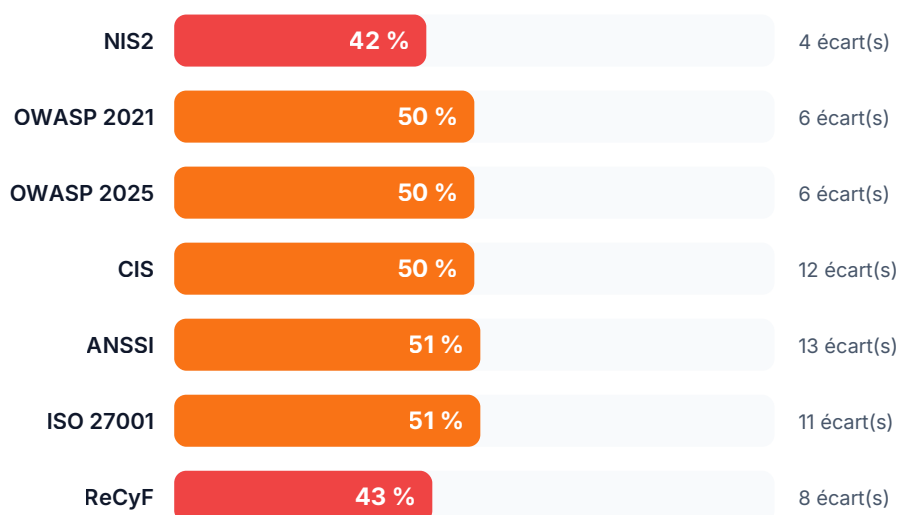
Non conforme

8 objectifs sur 20 évaluables en externe

43%

Scores calculés sur la partie évaluable en externe uniquement — les référentiels ne sont pas couverts en totalité. Certains contrôles nécessitent un accès au réseau interne, aux processus organisationnels ou aux postes de travail (voir section « Contrôles nécessitant un audit interne » ci-dessous). OWASP : 7/10 catégories évaluables (A04, A08, A09 requièrent un audit interne).

Écarts de conformité par référentiel



CIS

50%

Le CIS Controls v8 est un ensemble de 18 contrôles techniques de cybersécurité développé par le Center for Internet Security. Il constitue la référence opérationnelle pour le durcissement des systèmes d'information. 12 des 18 contrôles sont évaluables depuis la surface externe.

0/12 contrôles conformes, 12/12 en écart.

Contrôle	Description	Statut
CIS-1	Inventaire des actifs matériels	EN ÉCART
CIS-2	Inventaire des logiciels	EN ÉCART
CIS-3	Protection des données	EN ÉCART
CIS-4	Configurations sécurisées	EN ÉCART

Contrôle	Description	Statut
CIS-5	Gestion des comptes	EN ÉCART
CIS-6	Gestion des contrôles d'accès	EN ÉCART
CIS-7	Gestion des vulnérabilités	EN ÉCART
CIS-9	Protection de la messagerie	EN ÉCART
CIS-12	Défense du périmètre réseau	EN ÉCART
CIS-15	Sécurité de la chaîne d'approvisionnement	EN ÉCART
CIS-16	Sécurité applicative	EN ÉCART
CIS-17	Réponse aux incidents	EN ÉCART

Les écarts ci-dessus intègrent les contrôles directement contredits par une vulnérabilité détectée lors de l'audit (corrélation finding → contrôle), en complément des écarts remontés par le moteur de conformité.

Détail des écarts identifiés

CIS-1 — Inventaire des actifs

Risque : Les actifs non inventoriés (shadow IT) ne sont ni patchés ni surveillés. Ce sont les cibles préférées des attaquants car personne ne les monitorise.

Remédiation : 1. Comparer les sous-domaines découverts avec l'inventaire officiel. 2. Investiguer les actifs inconnus. 3. Automatiser la découverte d'actifs avec un scan régulier.

CIS-2 — Inventaire logiciels MOYEN

Risque : Les logiciels obsolètes (end-of-life) ne reçoivent plus de patches de sécurité. Chaque CVE publiée restera non corrigée indéfiniment.

Remédiation : 1. Identifier tous les logiciels en fin de vie. 2. Planifier la migration vers des versions supportées. 3. Mettre en place un processus de suivi des versions.

CIS-3 — Protection des données

Risque : Un fichier .env exposé contient les clés API et mots de passe. Un bucket S3 public peut contenir des données clients. Une base de données exposée = fuite de données massive.

Remédiation : 1. Supprimer immédiatement les fichiers sensibles exposés. 2. Configurer les buckets cloud en privé par défaut. 3. Auditer les permissions de stockage cloud. 4. Implémenter du DLP (Data Loss Prevention).

CIS-4 — Configs sécurisées

Risque : Le mode debug expose le code source et les variables d'environnement. Les configs par défaut ont des mots de passe connus. Les headers manquants permettent les attaques côté client.

Remédiation : 1. Désactiver le mode debug en production. 2. Supprimer les pages par défaut (phpinfo, server-status). 3. Configurer tous les headers de sécurité HTTP. 4. Appliquer un hardening guide (CIS Benchmarks).

CIS-6 — Gestion des contrôles d'accès **ÉLEVÉ**

Risque : Sans protection contre le brute-force, un attaquant peut tester des milliers de mots de passe par seconde. Les credentials par défaut sont testés en priorité par les scanners automatisés.

Remédiation : 1. Activer le MFA sur tous les comptes exposés. 2. Implémenter un rate-limiting sur les endpoints d'authentification. 3. Changer tous les mots de passe par défaut. 4. Utiliser un gestionnaire de mots de passe d'entreprise.

CIS-7 — Gestion des vulnérabilités **MOYEN**

Risque : Les CVE non patchées sont le vecteur #1 des ransomwares. Les exploits publics permettent à n'importe qui d'exploiter ces failles automatiquement.

Remédiation : 1. Corriger les CVE critiques (CVSS ≥ 9) sous 48h. 2. Corriger les CVE élevées (CVSS ≥ 7) sous 30 jours. 3. Scanner régulièrement avec Sedona Radar. 4. S'abonner aux alertes CERT-FR.

CIS-9 — Protection de la messagerie

Risque : Sans SPF/DKIM/DMARC, n'importe qui peut envoyer des emails en se faisant passer pour votre organisation. C'est le vecteur principal du phishing ciblé (spear phishing).

Remédiation : 1. Configurer SPF avec une politique stricte (-all). 2. Activer DKIM sur le serveur de messagerie. 3. Déployer DMARC en mode reject (p=reject). 4. Configurer une politique CSP pour les contenus web.

CIS-12 — Gestion périmètre réseau

Risque : Chaque service exposé inutilement augmente la surface d'attaque. Les services comme Redis, MongoDB ou Docker API exposés sans authentification permettent un accès direct.

Remédiation : 1. Auditer tous les ports ouverts et fermer ceux non nécessaires. 2. Ne jamais exposer de bases de données sur Internet. 3. Utiliser des firewalls avec des règles en whitelist.

CIS-15 — Gestion des fournisseurs de services

Risque : Un CDN compromis peut injecter du code malveillant sur votre site (supply chain attack). Sans vérification d'intégrité (SRI), votre navigateur exécutera le code modifié.

Remédiation : 1. Ajouter l'attribut integrity= (SRI) sur tous les scripts CDN. 2. Épingler les versions des dépendances. 3. Auditer régulièrement les fournisseurs tiers.

CIS-16 — Sécurité applicative ÉLEVÉ

Risque : Une injection SQL permet de lire toute la base de données. Un XSS permet de voler les sessions utilisateur. Un RCE permet l'exécution de commandes système.

Remédiation : 1. Utiliser des requêtes paramétrées. 2. Encoder les sorties HTML. 3. Valider toutes les entrées utilisateur. 4. Déployer un WAF. 5. Former les développeurs à la sécurité applicative.

NIS2**42%**

La directive européenne NIS2 (UE 2022/2555) impose aux entités essentielles et importantes des obligations de sécurité des réseaux et systèmes d'information. L'article 21.2 définit 10 mesures de gestion des risques ; 4 d'entre elles (développement sécurisé, chiffrement, contrôle d'accès, authentification/email) présentent un signal technique évaluable en audit externe. Les 6 mesures organisationnelles (gouvernance, gestion des incidents, continuité, chaîne d'approvisionnement, audit, formation) requièrent un audit interne.

0/4 article évaluable conforme, 4/4 en écart. 6 mesures organisationnelles non évaluables en externe (audit interne requis).

Article	Mesure	Statut
Art. 21.2.a	Politiques d'analyse des risques et de la sécurité des systèmes	NON ÉVALUABLE
Art. 21.2.b	Gestion des incidents	NON ÉVALUABLE
Art. 21.2.c	Continuité d'activité et gestion des sauvegardes	NON ÉVALUABLE
Art. 21.2.d	Sécurité de la chaîne d'approvisionnement	NON ÉVALUABLE
Art. 21.2.e	Sécurité dans l'acquisition, le développement et la maintenance	EN ÉCART
Art. 21.2.f	Évaluation de l'efficacité des mesures de gestion des risques	NON ÉVALUABLE
Art. 21.2.g	Hygiène cyber de base et formation	NON ÉVALUABLE
Art. 21.2.h	Politiques en matière de cryptographie et de chiffrement	EN ÉCART
Art. 21.2.i		EN ÉCART

Article	Mesure	Statut
	Sécurité des ressources humaines, contrôle d'accès et gestion des actifs	
Art. 21.2.j	Authentification multifacteurs et communications sécurisées	EN ÉCART

Détail des écarts identifiés

Art. 21.2.e — Sécurité dans l'acquisition, le développement et la maintenance **ÉLEVÉ**

Risque : 22 vulnérabilité(s) liée(s) à cet article identifiée(s), dont une à score 81/100. Écart significatif par rapport à l'exigence de l'article.

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

Art. 21.2.h — Politiques en matière de cryptographie et de chiffrement **ÉLEVÉ**

Risque : 10 vulnérabilité(s) crypto identifiée(s). Configuration à renforcer. Risque d'interception sur certains endpoints.

Remédiation : 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).

Art. 21.2.i — Sécurité des ressources humaines, contrôle d'accès et gestion des actifs **ÉLEVÉ**

Risque : 0 service(s) interne(s) exposé(s) sur Internet (port(s)) — 3 risque(s) identifié(s) en matière d'accès. Accès direct possible aux bases de données / caches sans authentification renforcée.

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

Art. 21.2.j — Authentification multifacteurs et communications sécurisées **ÉLEVÉ**

Risque : DMARC en mode reject : non. 5 risque(s) identifié(s) lié(s) à l'authentification. Usurpation d'email facile, communications externes non authentifiées.

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

ANSSI

Le guide d'hygiène informatique de l'ANSSI définit 42 mesures de sécurité fondamentales. 16 mesures sont évaluables depuis la surface externe, couvrant la mise à jour des logiciels, le chiffrement des communications, la gestion des accès et la sécurisation des sites web.

51%

3/16 contrôles conformes, 13/16 en écart.

Contrôle	Description	Statut
R1	Inventaire des actifs	EN ÉCART
R2	Protection des comptes administrateurs	CONFORME
R3	Politique de mots de passe	EN ÉCART
R7	Mise à jour des logiciels	EN ÉCART
R8	Classification des données sensibles	EN ÉCART
R9	Gestion des flux réseau	CONFORME
R10	Sécurité des échanges réseau (STARTTLS)	EN ÉCART
R11	Protection de la messagerie (SPF/DKIM/DMARC)	EN ÉCART
R12	Segmentation réseau	CONFORME
R16	Chiffrement des communications	EN ÉCART
R21	Sécurisation de la messagerie	EN ÉCART
R22	Gestion des accès	EN ÉCART
R24	Sécurisation des sites web	EN ÉCART
R25	Passerelle de sécurité Internet (WAF)	EN ÉCART
R29	Chiffrement des données sensibles	EN ÉCART
R30	Gestion des certificats numériques	EN ÉCART

Les écarts ci-dessus intègrent les contrôles directement contredits par une vulnérabilité détectée lors de l'audit (corrélation finding → contrôle), en complément des écarts remontés par le moteur de conformité.

Détail des écarts identifiés

R1 — Connaître et maîtriser le SI

Risque : Les actifs non répertoriés (shadow IT) échappent à la gouvernance sécurité et ne sont jamais patchés ni surveillés.

Remédiation : Comparer les sous-domaines et IPs découverts par ce scan avec l'inventaire officiel. Investiguer tout actif inconnu.

R3 — Appliquer une politique de mots de passe ÉLEVÉ

Risque : Les identifiants par défaut (admin/admin, root/password) sont testés en premier par les botnets. Un seul compte compromis peut suffire à prendre le contrôle total.

Remédiation : Changer immédiatement tous les mots de passe par défaut. Imposer 12+ caractères, complexité, et rotation régulière.

R7 — Mettre à jour les logiciels **MOYEN**

Risque : Les logiciels non mis à jour accumulent les CVE exploitables. C'est le premier vecteur d'entrée des ransomwares et des APT.

Remédiation : Patcher les CVE critiques sous 48h. Mettre à jour les composants obsolètes (EOL). Automatiser les mises à jour de sécurité.

R8 — Identifier et classer les données sensibles

Risque : Une base de données exposée = fuite de données clients. Un backup accessible = accès au code source et aux secrets. Un bucket S3 public = données exfiltrables en masse.

Remédiation : Supprimer immédiatement tout fichier sensible accessible publiquement. Configurer les buckets cloud en privé. Auditer les permissions de stockage.

R11 — Protéger la messagerie (SPF/DKIM/DMARC)

Risque : Sans SPF/DKIM/DMARC, un attaquant peut envoyer des emails qui semblent venir de votre domaine. C'est la base du phishing ciblé (CEO fraud, BEC).

Remédiation : 1. SPF : publier un enregistrement DNS avec -all. 2. DKIM : signer les emails sortants. 3. DMARC : passer en p=reject après une période de monitoring.

R16 — Chiffrer les communications **ÉLEVÉ**

Risque : Le trafic non chiffré peut être intercepté (mots de passe, sessions, données RGPD). Les protocoles obsolètes (TLS 1.0) ont des failles connues exploitables.

Remédiation : Désactiver TLS 1.0/1.1. Activer HSTS. Utiliser des cipher suites modernes. Renouveler les certificats avant expiration.

R22 — Gérer les accès

Risque : Un accès anonyme à un service de base de données ou d'administration permet la compromission immédiate sans même avoir besoin de mot de passe.

Remédiation : Ajouter une authentification sur tous les services exposés. Appliquer le principe du moindre privilège. Activer le MFA.

R24 — Sécuriser les sites web (headers HTTP) **ÉLEVÉ**

Risque : Sans CSP, le site est vulnérable au XSS. Sans X-Frame-Options, il est vulnérable au clickjacking. Sans X-Content-Type-Options, le navigateur peut mal interpréter les fichiers.

Remédiation : Restreindre / corriger : Configurer CSP, X-Frame-Options (DENY), X-Content-Type-Options (nosniff), Referrer-Policy (strict-origin), Permissions-Policy.

R25 — Sécuriser les passerelles Internet (WAF/CDN)

Risque : Sans WAF, les attaques applicatives (injection, XSS, brute-force) arrivent directement sur l'application. Sans CDN, le site est vulnérable aux DDoS.

Remédiation : Déployer un WAF/CDN (Cloudflare, AWS WAF, Akamai). Configurer les règles de filtrage. Activer la protection DDoS.

R29 — Chiffrer les données sensibles transmises

Risque : Les protocoles en clair (HTTP, FTP, Telnet) exposent les identifiants et données à l'interception réseau.

Remédiation : Restreindre / corriger : Migrer HTTP vers HTTPS, FTP vers SFTP, Telnet vers SSH. Rediriger automatiquement HTTP vers HTTPS.

OWASP 2021

50%

L'OWASP Top 10 édition 2021 classe les 10 catégories de risques applicatifs les plus critiques. 7 catégories sur 10 sont évaluables en audit externe (A04 Insecure Design, A08 Software Integrity et A09 Logging requièrent un audit interne).

1/7 contrôles conformes, 6/7 en écart.

Contrôle	Description	Statut
A01	Broken Access Control	EN ÉCART
A02	Cryptographic Failures	EN ÉCART
A03	Injection	EN ÉCART
A05	Security Misconfiguration	EN ÉCART
A06	Vulnerable and Outdated Components	EN ÉCART
A07	Identification and Authentication Failures	EN ÉCART
A10	Server-Side Request Forgery (SSRF)	CONFORME

Les écarts ci-dessus intègrent les contrôles directement contredits par une vulnérabilité détectée lors de l'audit (corrélation finding → contrôle), en complément des écarts remontés par le moteur de conformité.

Détail des écarts identifiés

A01 — Broken Access Control

Risque : Un attaquant peut lire ou modifier les données d'autres utilisateurs, accéder aux interfaces d'administration, ou télécharger des fichiers sensibles. C'est la vulnérabilité #1 du classement OWASP.

Remédiation : 1. Implémenter un contrôle d'accès côté serveur (jamais côté client). 2. Appliquer le principe du moindre privilège. 3. Désactiver le directory listing. 4. Journaliser tous les échecs d'accès.

A02 — Cryptographic Failures **ÉLEVÉ**

Risque : Un attaquant sur le réseau peut intercepter les mots de passe, sessions, et données personnelles en transit. Les algorithmes faibles (MD5, SHA1, RC4) peuvent être cassés.

Remédiation : 1. Forcer HTTPS partout avec HSTS. 2. Désactiver TLS 1.0/1.1. 3. Utiliser des cipher suites modernes (AES-256-GCM, ChaCha20). 4. Ne jamais stocker de mots de passe en clair ou en MD5.

A03 — Injection **ÉLEVÉ**

Risque : SQL injection = accès complet à la base de données (lecture, modification, suppression). XSS = vol de sessions utilisateur, redirection vers un site malveillant. Command injection = exécution de commandes système arbitraires.

Remédiation : 1. Utiliser des requêtes paramétrées (prepared statements) pour SQL. 2. Encoder les sorties HTML (échappement XSS). 3. Valider et sanitiser toutes les entrées utilisateur côté serveur. 4. Déployer un WAF en complément.

A04 — Insecure Design

Risque : Sans rate-limiting, un attaquant peut bruteforcer les mots de passe ou les tokens. Un CORS mal configuré permet à un site malveillant d'accéder aux données de vos utilisateurs. Les redirections ouvertes facilitent le phishing.

Remédiation : 1. Implémenter du rate-limiting sur les endpoints d'authentification et les API. 2. Configurer CORS de manière restrictive (origines spécifiques, pas '*'). 3. Valider les URL de redirection contre une whitelist.

A05 — Security Misconfiguration

Risque : Un fichier .env exposé révèle les clés API, mots de passe de base de données, et secrets applicatifs. Un répertoire .git exposé permet de télécharger le code source complet. Le mode debug en production affiche les stack traces avec les chemins internes.

Remédiation : 1. Supprimer/protéger les fichiers sensibles (.env, .git, phpinfo.php). 2. Désactiver le mode debug en production. 3. Configurer les headers de sécurité manquants. 4. Supprimer les pages et comptes par défaut.

A07 — Identification and Authentication Failures **ÉLEVÉ**

Risque : Un attaquant peut deviner ou bruteforcer les mots de passe, réutiliser des sessions volées, ou exploiter des identifiants par défaut pour prendre le contrôle des comptes.

Remédiation : 1. Implémenter le MFA sur tous les comptes sensibles. 2. Bloquer après 5 tentatives échouées (account lockout). 3. Changer tous les mots de passe par défaut. 4. Utiliser des tokens de session sécurisés (HttpOnly, Secure, SameSite).

A08 — Software and Data Integrity Failures

Risque : Si un CDN est compromis, un attaquant peut injecter du code malveillant dans tous les sites qui en dépendent. Sans SRI (Subresource Integrity), le navigateur exécute aveuglément le script modifié.

Remédiation : 1. Ajouter l'attribut integrity= sur tous les scripts CDN externes. 2. Utiliser des versions épinglées (pinned) des dépendances. 3. Vérifier les signatures des mises à jour logicielles.

ReCyF

43%

Le cadre Sedona ReCyF est un référentiel d'auto-évaluation inspiré du Guide d'hygiène ANSSI v2.0 et de la transposition NIS2 française. Il définit 20 objectifs de sécurité (OS1-OS20), dont 8 sont mesurables depuis la surface externe.

0/8 contrôles conformes, 8/8 en écart.

Contrôle	Description	Statut
OS1	Recensement des systèmes d'information	EN ÉCART
OS5	Maîtrise des systèmes d'information	EN ÉCART
OS7	Architecture de sécurité du SI	EN ÉCART
OS8	Accès distant sécurisé	EN ÉCART
OS9	Protection contre les codes malveillants	EN ÉCART
OS10	Gestion des identités et des accès	EN ÉCART
OS12	Protection des données	EN ÉCART
OS18	Sécurisation de la configuration des ressources	EN ÉCART

Les écarts ci-dessus intègrent les contrôles directement contredits par une vulnérabilité détectée lors de l'audit (corrélation finding → contrôle), en complément des écarts remontés par le moteur de conformité.

Détail des écarts identifiés

OS1 — Recensement des systèmes d'information ÉLEVÉ

Risque : Actifs oubliés = surface d'attaque non maîtrisée (shadow IT).

Remédiation : Scanner régulièrement la surface externe, décommissionner les actifs obsolètes.

OS3 — Maîtrise de l'écosystème

Risque : Un fournisseur compromis (CDN, lib JS) injecte du code malveillant sur votre site (supply chain attack type Magecart). Un sous-domaine pointant vers un service tiers décommissionné = subdomain takeover.

Remédiation : Inventorier les domaines tiers (CSP, CNAME). Implémenter Subresource Integrity (SRI) sur les scripts CDN. Auditer les CNAME orphelins. Pinning des versions tierces.

OS5 — Maîtrise des systèmes d'information **MOYEN**

Risque : Composants non patchés = exploitation de CVE connues.

Remédiation : Appliquer les correctifs critiques sous 72h, décommissionner les versions EOL.

OS7 — Sécurisation de l'architecture des systèmes d'information **ÉLEVÉ**

Risque : Services internes exposés = pivot réseau possible pour un attaquant.

Remédiation : Fermer les ports non nécessaires, isoler les environnements de dev/staging.

OS8 — Sécurisation des accès distants aux systèmes d'information

Risque : Accès distant non sécurisé = compromission via brute-force ou credential stuffing.

Remédiation : Activer MFA sur tous les accès distants, utiliser TLS 1.2+ minimum.

OS9 — Protection des systèmes d'information contre les codes malveillants

Risque : Code malveillant = exfiltration de données, ransomware, pivot réseau.

Remédiation : Déployer EDR, scanner les fichiers exposés, surveiller les IOC.

OS10 — Gestion des identités et des accès des utilisateurs aux systèmes d'information **ÉLEVÉ**

Risque : Accès non contrôlé = escalade de privilèges, accès non autorisé aux données.

Remédiation : Supprimer les comptes par défaut, implémenter RBAC, désactiver les accès inutilisés.

OS12 — Identification et réaction aux incidents de sécurité

Risque : Absence de détection = attaques non identifiées pendant des mois.

Remédiation : Implémenter security.txt, déployer monitoring, configurer alertes.

ISO 27001

51%

La norme ISO 27001:2022 (Annexe A) définit 93 contrôles de sécurité. 13 contrôles technologiques de l'Annexe A sont évaluables en audit externe, couvrant la gestion des vulnérabilités, la cryptographie, la sécurité des réseaux et la configuration des systèmes.

2/13 contrôles conformes, 11/13 en écart.

Contrôle	Description	Statut
A.5.7	Threat intelligence	CONFORME
A.5.14	Information transfer (email security)	EN ÉCART
A.5.23	Cloud services security	EN ÉCART
A.8.7	Malware protection	CONFORME
A.8.8	Vulnerability management	EN ÉCART
A.8.9	Configuration management	EN ÉCART
A.8.12	Data leakage prevention	EN ÉCART
A.8.20	Network security	EN ÉCART
A.8.21	Network services security	EN ÉCART
A.8.24	Use of cryptography	EN ÉCART
A.8.25	Secure development	EN ÉCART
A.8.26	Application security requirements	EN ÉCART
A.8.28	Secure coding	EN ÉCART

Les écarts ci-dessus intègrent les contrôles directement contredits par une vulnérabilité détectée lors de l'audit (corrélation finding → contrôle), en complément des écarts remontés par le moteur de conformité.

Détail des écarts identifiés

A.5.14 — Information transfer

Risque : Sans SPF/DKIM/DMARC, les emails du domaine peuvent être usurpés pour du phishing. Sans STARTTLS, les emails transitent en clair.

Remédiation : Déployer SPF (-all), DKIM et DMARC (p=reject). Activer STARTTLS sur les serveurs MX. Vérifier avec des outils de test MX.

A.5.23 — Information security for use of cloud services **ÉLEVÉ**

Risque : Un bucket S3 ou un Firebase public expose les données stockées à n'importe qui sur Internet. Des fuites massives de données clients sont causées chaque année par des buckets mal configurés.

Remédiation : Auditer les permissions de tous les buckets cloud. Configurer l'accès en privé par défaut. Activer les logs d'accès. Utiliser AWS Config / Azure Policy pour prévenir les misconfigurations.

A.8.8 — Management of technical vulnerabilities **MOYEN**

Risque : Les CVE non gérées s'accumulent et augmentent exponentiellement la surface d'attaque. Les exploits publics rendent chaque CVE exploitable par des attaquants peu qualifiés.

Remédiation : Mettre en place un cycle de scan régulier (mensuel minimum). Définir des SLA de correction : critique < 48h, élevé < 30j, moyen < 90j. Documenter les exceptions.

A.8.9 — Configuration management

Risque : Les fichiers .env et .git exposés révèlent les secrets applicatifs. Le mode debug affiche le code source et les variables d'environnement. Les directory listings exposent la structure du site.

Remédiation : Supprimer les fichiers sensibles accessibles (.env, .git, phpinfo). Désactiver le debug en production. Configurer les headers de sécurité. Appliquer les CIS Benchmarks.

A.8.12 — Data leakage prevention

Risque : Des clés API, tokens, ou mots de passe exposés dans le code ou les fichiers permettent l'accès direct aux systèmes internes. Un dump de base de données public = fuite RGPD majeure.

Remédiation : Scanner et supprimer tous les secrets exposés. Mettre en place un outil de détection de secrets (TruffleHog, Gitleaks) dans la CI/CD. Rotation des secrets compromis.

A.8.20 — Networks security

Risque : Des services comme Redis, MongoDB, Elasticsearch ou Docker API exposés sans authentification permettent un accès direct aux données ou l'exécution de commandes.

Remédiation : Fermer tous les ports non nécessaires. Configurer le firewall en whitelist. Ne jamais exposer de bases de données sur Internet. Utiliser un VPN pour l'administration distante.

A.8.24 — Use of cryptography **ÉLEVÉ**

Risque : Les protocoles SSL/TLS obsolètes (Heartbleed, POODLE, BEAST, DROWN) permettent le déchiffrement du trafic. Un certificat expiré rend le site inaccessible.

Remédiation : Désactiver SSL 3.0 et TLS 1.0/1.1. Activer HSTS. Utiliser des cipher suites AEAD (AES-GCM, ChaCha20). Automatiser le renouvellement des certificats.

A.8.26 — Application security requirements ÉLEVÉ

Risque : Les vulnérabilités applicatives permettent le vol de données (SQLi), la prise de contrôle des sessions utilisateur (XSS), l'exécution de commandes système (RCE).

Remédiation : Utiliser des requêtes paramétrées. Encoder les sorties HTML. Valider les entrées. Former les développeurs. Déployer un WAF.

A.8.28 — Secure coding ÉLEVÉ

Risque : Les erreurs verbeuses (stack traces) révèlent l'architecture interne, les chemins de fichiers et les technologies. Les secrets hardcodés dans le JavaScript sont accessibles à tous.

Remédiation : Désactiver les messages d'erreur détaillés en production. Ne jamais stocker de secrets dans le code source. Utiliser des variables d'environnement ou un vault.

A.8.5 — Secure authentication ÉLEVÉ

Risque : Sans MFA sur les portails publics (OWA, M365, VPN, admin), un identifiant compromis suffit à prendre le contrôle. Sans rate-limiting, le brute-force réussit en quelques heures.

Remédiation : Activer le MFA sur tous les portails exposés. Imposer du rate-limiting (max 5 tentatives/min/IP). Migrer HTTP Basic Auth vers OAuth/OIDC. Bloquer les IPs malveillantes (AbuseIPDB).

OWASP 2025**50%**

L'OWASP Top 10 édition 2025 (à paraître) intègre les risques émergents : sécurité de la supply chain logicielle, mauvaise configuration des LLM, défauts cryptographiques modernes. 7 catégories sur 10 sont évaluable en audit externe.

1/7 contrôles conformes, 6/7 en écart.

Contrôle	Description	Statut
A01	Broken Access Control	EN ÉCART
A02	Cryptographic Failures	EN ÉCART
A03	Injection	EN ÉCART
A05	Security Misconfiguration	EN ÉCART
A06	Vulnerable and Outdated Components	EN ÉCART
A07	Identification and Authentication Failures	EN ÉCART
A10	Mishandling of Exceptional Conditions / SSRF étendu	CONFORME

Les écarts ci-dessus intègrent les contrôles directement contredits par une vulnérabilité détectée lors de l'audit (corrélation finding → contrôle), en complément des écarts remontés par le moteur de conformité.

Détail des écarts identifiés

A01 — Broken Access Control

Risque : Lecture/modification de données d'autres utilisateurs, accès aux interfaces d'administration, SSRF vers métadonnées cloud. Reste la vulnérabilité #1.

Remédiation : 1. Contrôle d'accès côté serveur (jamais côté client). 2. Principe du moindre privilège. 3. Désactiver directory listing. 4. Filtrer les URL pour bloquer SSRF.

A02 — Security Misconfiguration

Risque : Fichiers .env exposés, mode debug en production, headers de sécurité manquants, comptes par défaut non changés.

Remédiation : 1. Désactiver le mode debug. 2. Supprimer pages par défaut. 3. Configurer headers de sécurité. 4. Appliquer CIS Benchmarks.

A04 — Cryptographic Failures **ÉLEVÉ**

Risque : Interception de mots de passe et données personnelles en transit, déchiffrement avec MD5/SHA1/RC4, clés exposées.

Remédiation : Restreindre / corriger : 1. HTTPS partout avec HSTS. 2. TLS 1.2+. 3. Cipher suites AEAD (AES-256-GCM, ChaCha20). 4. Pas de stockage en clair ni MD5.

A05 — Injection **ÉLEVÉ**

Risque : SQLi = accès complet à la DB. XSS = vol de sessions. Command injection = exécution de commandes système.

Remédiation : 1. Requêtes paramétrées. 2. Encoder les sorties HTML. 3. Valider toutes les entrées. 4. WAF en défense en profondeur.

A06 — Insecure Design

Risque : Absence de rate-limiting, CORS trop permissif, logique métier contournable, upload non restreint.

Remédiation : 1. Threat modeling dès la conception. 2. Rate-limiting sur endpoints d'auth. 3. CORS restrictif. 4. Validation des règles métier côté serveur.

A07 — Authentication Failures **ÉLEVÉ**

Risque : Brute-force réussissant, sessions volées réutilisées, contournement MFA, credentials par défaut exploités.

Remédiation : 1. MFA sur comptes sensibles. 2. Lockout après 5 tentatives. 3. Tokens session HttpOnly+Secure+SameSite. 4. Changer mots de passe par défaut.

A08 — Software or Data Integrity Failures

Risque : Si CDN compromis, code malveillant injecté. Désérialisation non sécurisée = RCE.

Remédiation : 1. SRI sur scripts CDN. 2. Versions épinglées. 3. Signature des mises à jour. 4. Désactiver désérialisation non typée.

Contrôles nécessitant un audit interne

Les contrôles suivants ne sont pas évalués en totalité depuis la surface externe. Leur évaluation nécessite un accès au réseau interne, aux processus organisationnels ou aux équipements physiques. Ils couvrent des aspects critiques : gouvernance (politiques de sécurité, formation, gestion de crise), contrôles physiques (accès aux locaux, protection des équipements), et contrôles techniques internes (Active Directory, journalisation, sauvegardes, gestion des postes de travail).

La sonde **Sedona Radar On-Premise** permet d'évaluer ces contrôles — voir la section « Prochaines étapes » pour plus de détails.

Synthèse par framework

Framework	Total contrôles	Évaluables en externe	Nécessitent un audit interne
CIS	18	12	6
NIS2	10	4	6
ANSSI	42	16	26
OWASP	10	7	3
ReCyF	20	8	12
ISO27001	?	?	74

CIS — 6 contrôle(s) non évaluable(s) en externe

3 exemples (sur 6) :

- **CIS-8** — Audit Log Management (8.1-8.12)
- **CIS-10** — Malware Defenses (10.1-10.7)
- **CIS-11.1** — Data Recovery Process

Détail complet des 6 contrôles disponible via un audit interne ou la sonde Sedona Radar On-Premise.

NIS2 — 6 contrôle(s) non évaluable(s) en externe

3 exemples (sur 6) :

- **Art. 21.2.f** — Évaluation de l'efficacité des mesures de sécurité
- **Art. 21.2.g** — Hygiène cyber et formation du personnel
- **Art. 21.2.j (comms)** — Communications voix/vidéo/urgence sécurisées

Détail complet des 6 contrôles disponible via un audit interne ou la sonde Sedona Radar On-Premise.

ANSSI — 26 contrôle(s) non évaluable(s) en externe

3 exemples (sur 26) :

- **R1 (officiel)** — Former les équipes opérationnelles à la sécurité
- **R2 (officiel)** — Sensibiliser les utilisateurs aux bonnes pratiques
- **R3 (officiel)** — Maîtriser les risques de l'infogérance

Détail complet des 26 contrôles disponible via un audit interne ou la sonde Sedona Radar On-Premise.

OWASP — 3 contrôle(s) non évaluable(s) en externe

2 exemples (sur 3) :

- — Security Logging and Monitoring Failures
- — Insecure Design — business logic & threat modeling

Détail complet des 3 contrôles disponible via un audit interne ou la sonde Sedona Radar On-Premise.

ReCyF — 12 contrôle(s) non évaluable(s) en externe

3 exemples (sur 12) :

- **OS2** — Mise en œuvre d'un cadre de gouvernance de la sécurité numérique
- **OS3 (revue contractuelle)** — Maîtrise contractuelle des fournisseurs
- **OS4** — Intégration de la sécurité numérique dans la gestion des ressources humaines

Détail complet des 12 contrôles disponible via un audit interne ou la sonde Sedona Radar On-Premise.

ISO27001 — 74 contrôle(s) non évaluable(s) en externe

3 exemples (sur 74) :

- **A.5.1** — Politiques pour la sécurité de l'information
- **A.5.2** — Rôles et responsabilités sécurité
- **A.5.3** — Séparation des tâches

Détail complet des 74 contrôles disponible via un audit interne ou la sonde Sedona Radar On-Premise.

Détail par référentiel — OWASP, CIS, ANSSI, ISO 27001, ReCyF

OWASP Top 10 (2021)

50 % — Partiellement conforme

6/7 contrôle(s) évaluable(s) en écart. Analyse contrôle par contrôle, rattachée aux vulnérabilités réellement détectées.

Contrôle	Statut	Ce qu'exige le contrôle	Votre situation / remédiation
A01 Contrôle d'accès défaillant (Broken Access Control)	EN ÉCART	Restreindre l'accès aux ressources et services aux seuls utilisateurs autorisés (moindre privilège, authentification).	Default credentials acceptés sur /login.jsp (+2 autres) → Authentifier ou cloisonner (pare-feu) tous les services exposés ; restreindre les consoles d'administration.

Contrôle	Statut	Ce qu'exige le contrôle	Votre situation / remédiation
A02 Défaillances cryptographiques (Cryptographic Failures)	EN ÉCART	Chiffrer les données en transit et au repos avec des protocoles et suites modernes ; ne jamais exposer de secrets.	Weak Cipher Suites Detection (+1 autre) → Désactiver TLS 1.0/1.1 et 3DES/RC4, retirer .env/.git de l'espace web, activer HSTS.
A03 Injection	EN ÉCART	Valider et paramétrer toutes les entrées (requêtes SQL préparées, échappement) pour empêcher l'injection.	Cross Site Scripting (Reflected) (+5 autres) → Utiliser des requêtes paramétrées, valider les entrées, déployer un WAF en défense en profondeur.
A05 Mauvaise configuration de sécurité (Security Misconfiguration)	EN ÉCART	Durcir la configuration : en-têtes de sécurité, pas de page de debug/info, pas de transfert de zone DNS ouvert.	En-tête de sécurité manquant : content-security-policy (+2 autres) → Ajouter X-Frame-Options/CSP, supprimer phpinfo/server-status, fermer le transfert de zone DNS (AXFR).
A06 Composants vulnérables et obsolètes (Vulnerable & Outdated Components)	EN ÉCART	Maintenir à jour tous les composants (serveur, CMS, bibliothèques) et retirer les technologies en fin de vie.	Divulgaration d'information : server → Appliquer les correctifs éditeur (Apache, Jenkins, WordPress, OpenSSL), migrer les technologies en fin de vie.
A07 Défaillances d'authentification (Identification & Authentication Failures)	EN ÉCART	Imposer des mots de passe robustes, l'authentification multifacteur (MFA) et interdire les identifiants par défaut.	Default credentials acceptés sur /login.jsp (+1 autre) → Réinitialiser les mots de passe faibles/par défaut et activer le MFA sur tous les accès à privilèges.
A10 Falsification de requête côté serveur (SSRF)	CONFORME	Filtrer et restreindre les requêtes sortantes initiées par le serveur pour prévenir la SSRF.	Aucun écart détecté par l'audit externe.

CIS Controls v8

50 % — Partiellement conforme

8/8 contrôle(s) évaluable(s) en écart. Analyse contrôle par contrôle, rattachée aux vulnérabilités réellement détectées.

Contrôle	Statut	Ce qu'exige le contrôle	Votre situation / remédiation
CIS-3 Protection des données	EN ÉCART	Protéger les données sensibles (chiffrement, contrôle d'accès) et ne pas les exposer.	Default credentials acceptés sur /login.jsp (+1 autre) → Retirer les secrets exposés (.env/.git), fermer

Contrôle	Statut	Ce qu'exige le contrôle	Votre situation / remédiation
			l'accès Internet aux bases de données.
CIS-4 Configuration sécurisée des actifs	EN ÉCART	Appliquer une configuration durcie (en-têtes, services, comptes par défaut).	Default credentials acceptés sur /login.jsp (+4 autres) → Durcir la configuration des serveurs web (en-têtes de sécurité, suppression des pages techniques).
CIS-5 Gestion des comptes	EN ÉCART	Gérer le cycle de vie des comptes et proscrire les identifiants faibles/par défaut.	Écart détecté. → Réinitialiser les comptes à mot de passe faible et supprimer les comptes par défaut.
CIS-6 Gestion des contrôles d'accès	EN ÉCART	Appliquer le moindre privilège et l'authentification forte (MFA) sur les accès.	Portail d'administration sans MFA visible: demo.testfire.net/admin → Authentifier tous les services d'infrastructure, activer le MFA sur les accès à privilèges.
CIS-7 Gestion continue des vulnérabilités	EN ÉCART	Détecter et corriger en continu les vulnérabilités (patch management).	Cloud Exposure: S3 — demo-public (+4 autres) → Mettre en place un patch management priorisé (KEV/EPSS) et corriger les CVE critiques.
CIS-9 Protection de la messagerie et des navigateurs	EN ÉCART	Authentifier les emails (SPF/DKIM/DMARC) pour empêcher l'usurpation.	DMARC absent sur demo.testfire.net (+2 autres) → Configurer SPF, DKIM et DMARC en politique reject.
CIS-12 Gestion de l'infrastructure réseau	EN ÉCART	Cloisonner le réseau et n'exposer que les services strictement nécessaires.	Cloud Exposure: S3 — demo-public → Fermer au pare-feu les ports d'infrastructure (bases, caches, Docker) exposés sur Internet.
CIS-16 Sécurité applicative	EN ÉCART	Développer et exploiter des applications sûres (tests, validation des entrées).	Cross Site Scripting (Reflected) (+6 autres) → Corriger les vulnérabilités applicatives (injection, RCE) et intégrer des tests SAST/DAST.

Guide d'hygiène ANSSI

51 % — Partiellement conforme

5/5 contrôle(s) évaluable(s) en écart. Analyse contrôle par contrôle, rattachée aux vulnérabilités réellement détectées.

Contrôle	Statut	Ce qu'exige le contrôle	Votre situation / remédiation
M10 Maintenir à jour les composants	EN ÉCART	Appliquer les correctifs de sécurité et retirer les logiciels obsolètes.	Divulgarion d'information : server (+1 autre) → Déployer un processus de mise à jour régulier ; corriger Apache/Jenkins/WordPress/OpenSSL.
M11 Configurer durcie des équipements	EN ÉCART	Désactiver les services inutiles et durcir la configuration (en-têtes, pages techniques).	Default credentials acceptés sur /login.jsp (+4 autres) → Durcir la configuration : en-têtes de sécurité, suppression de phpinfo/server-status.
M16 Cloisonner le réseau	EN ÉCART	Segmenter le réseau et n'exposer aucun service interne sur Internet.	Cloud Exposure: S3 — demo-public → Cloisonner et fermer au pare-feu les services internes exposés (bases, caches, Docker).
M21 Authentifier les accès	EN ÉCART	Imposer une authentification forte et proscrire les identifiants par défaut/faibles.	Default credentials acceptés sur /login.jsp (+1 autre) → Activer l'authentification (MFA) sur les services et accès à privilèges.
M26 Chiffrer les flux réseau	EN ÉCART	Chiffrer les communications (TLS 1.2+) et authentifier la messagerie (SPF/DKIM/DMARC).	TLS — Certificate chain untrusted (Android) (demo.testfire.net) (+7 autres) → Rétablir un chiffrement conforme (TLS 1.2/1.3, suites AEAD) et configurer DMARC en reject.

ISO/IEC 27001:2022 (Annexe A)

51 % — Partiellement conforme

7/7 contrôle(s) évaluable(s) en écart. Analyse contrôle par contrôle, rattachée aux vulnérabilités réellement détectées.

Contrôle	Statut	Ce qu'exige le contrôle	Votre situation / remédiation
A.8.8 Gestion des vulnérabilités techniques	EN ÉCART	Identifier, évaluer et corriger les vulnérabilités techniques en temps voulu.	Cloud Exposure: S3 — demo-public (+4 autres) → Établir un processus de gestion des vulnérabilités

Contrôle	Statut	Ce qu'exige le contrôle	Votre situation / remédiation
			priorisé et corriger les CVE critiques.
A.8.9 Gestion de la configuration	EN ÉCART	Définir, documenter et maintenir des configurations sécurisées.	Default credentials acceptés sur /login.jsp (+3 autres) → Formaliser des lignes de base de configuration durcie et supprimer les pages techniques exposées.
A.8.20 Sécurité des réseaux	EN ÉCART	Sécuriser et cloisonner les réseaux ; ne pas exposer les services internes.	Cloud Exposure: S3 — demo-public → Cloisonner le réseau et fermer les services d'infrastructure exposés sur Internet.
A.8.24 Utilisation de la cryptographie	EN ÉCART	Employer des protocoles et suites cryptographiques robustes.	TLS — Certificate chain untrusted (Android) (demo.testfire.net) (+4 autres) → Désactiver TLS 1.0/1.1 et 3DES/RC4 ; ne conserver que TLS 1.2/1.3 avec suites AEAD.
A.5.17 Informations d'authentification	EN ÉCART	Gérer les secrets d'authentification (mots de passe forts, MFA, pas de valeurs par défaut).	Default credentials acceptés sur /login.jsp (+1 autre) → Réinitialiser les identifiants faibles/par défaut et déployer le MFA.
A.8.23 Filtrage web	EN ÉCART	Filtrer le trafic web (WAF) pour bloquer les attaques applicatives.	Cross Site Scripting (Reflected) (+6 autres) → Déployer un WAF/CDN en frontal et filtrer les requêtes malveillantes.
A.8.12 Prévention des fuites de données	EN ÉCART	Empêcher l'exposition ou l'exfiltration de données sensibles et de secrets.	Portail d'administration sans MFA visible: demo.testfire.net/admin → Retirer les secrets exposés (.env/.git) et cloisonner les données sensibles.

ReCyF (cadre Sedona)

43 % — Non conforme

7/7 contrôle(s) évaluable(s) en écart. Analyse contrôle par contrôle, rattachée aux vulnérabilités réellement détectées.

Contrôle	Statut	Ce qu'exige le contrôle	Votre situation / remédiation
	EN ÉCART		Cloud Exposure: S3 — demo-public

Contrôle	Statut	Ce qu'exige le contrôle	Votre situation / remédiation
OS1 Recensement des systèmes exposés		Connaître et maîtriser sa surface d'exposition (services et ports ouverts).	→ Inventorier la surface externe et fermer les services non nécessaires.
OS5 Maîtrise et mise à jour du SI	EN ÉCART	Maintenir les composants à jour et supprimer les technologies obsolètes.	Divulgaration d'information : server (+1 autre) → Corriger les composants vulnérables et migrer les technologies en fin de vie.
OS7 Architecture de sécurité (cloisonnement)	EN ÉCART	Cloisonner l'architecture et n'exposer aucun service interne.	Cloud Exposure: S3 — demo-public → Cloisonner le réseau et fermer au pare-feu les services d'infrastructure exposés.
OS8 Accès distant sécurisé	EN ÉCART	Sécuriser les accès distants (authentification forte, chiffrement).	Default credentials acceptés sur /login.jsp → Restreindre et authentifier fortement les accès distants (MFA, VPN).
OS10 Gestion des identités et des accès	EN ÉCART	Gérer les identités et appliquer le moindre privilège avec MFA.	Default credentials acceptés sur /login.jsp (+1 autre) → Réinitialiser les comptes faibles et déployer le MFA sur les accès à privilèges.
OS12 Protection des données	EN ÉCART	Protéger les données sensibles et empêcher l'exposition de secrets.	Portail d'administration sans MFA visible: demo.testfire.net/admin → Retirer les secrets exposés et chiffrer/cloisonner les données sensibles.
OS18 Sécurisation de la configuration	EN ÉCART	Appliquer une configuration durcie des ressources exposées.	En-tête de sécurité manquant : content-security-policy (+2 autres) → Durcir la configuration (en-têtes de sécurité, suppression des pages techniques).

Infrastructure et surface d'attaque

Cartographie de la surface externe en 6 axes : configuration SSL/TLS (testssl.sh + SSLyze + Qualys grading), hygiène DNS et messagerie (SPF/DKIM/DMARC + AXFR + DNSSEC), services exposés (Nmap + Masscan), intelligence passive IP (Shodan + AbuseIPDB + GreyNoise), détection WAF (Wafw00f), scanners actifs (Nuclei + SQLmap).

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.

L'énumération protocolaire n'a pas pu être complétée sur ce périmètre : aucune conclusion sur la conformité des protocoles ne peut être affirmée. Voir l'analyse SSL/TLS détaillée.

Protocoles supportés (synthèse DSI)

Sur ce périmètre, 6 version(s) de protocole n'ont pas pu être testées (collecte protocolaire incomplète : services n'exposant pas l'interface TLS attendue, ou analyse partielle). Le détail ci-dessous est donc incomplet ; le grade global est indicatif et doit être confirmé par un scan TLS complet.

Protocole	Statut
SSL 2.0	Non testé
SSL 3.0	Non testé
TLS 1.0	Non testé
TLS 1.1	Non testé
TLS 1.2	Non testé
TLS 1.3	Non testé

Cipher suites

Aucun cipher faible/déprécié détecté sur les endpoints scannés.

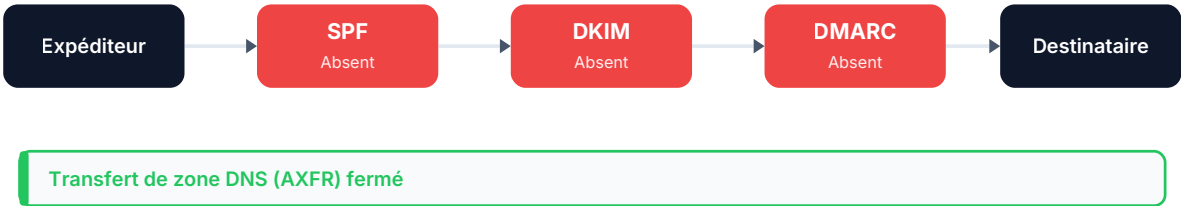
Vulnérabilités SSL connues

Nom	CVE	Statut
Heartbleed	CVE-2014-0160	Non testé / non concluant
POODLE	CVE-2014-3566	Non testé / non concluant
BEAST	CVE-2011-3389	Non testé / non concluant
CRIME	CVE-2012-4929	Non testé / non concluant
BREACH	—	Non testé / non concluant
DROWN	CVE-2016-0800	Non testé / non concluant
LOGJAM	CVE-2015-4000	Non testé / non concluant
FREAK	CVE-2015-0204	Non testé / non concluant

Configuration DNS et messagerie

La configuration DNS et les protocoles d'authentification email (SPF, DMARC, DKIM) protègent contre l'usurpation d'identité par email (phishing, BEC — Business Email Compromise). Leur absence expose l'organisation à des campagnes de phishing ciblé utilisant son propre nom de domaine.

Chaîne d'authentification des e-mails



Domaine principal — demo.testfire.net

SPF	ABSENT
DMARC	ABSENT
DKIM	ABSENT
AXFR	PROTÉGÉ
MX	Aucun
NS	Aucun

SPF absent — Le protocole SPF (Sender Policy Framework) définit quels serveurs sont autorisés à envoyer des emails au nom de votre domaine. Sans SPF, n'importe quel serveur dans le monde peut envoyer des emails en se faisant passer pour votre organisation. C'est le vecteur principal des attaques de phishing ciblé et du BEC (Business Email Compromise) — un type de fraude qui coûte en moyenne 125 000 € par incident (source FBI IC3 2024).

DMARC absent — DMARC (Domain-based Message Authentication, Reporting and Conformance) indique aux serveurs destinataires comment traiter les emails non authentifiés : les rejeter, les mettre en quarantaine, ou les accepter. Sans DMARC, même si SPF est configuré, les serveurs destinataires n'ont aucune instruction et peuvent accepter les emails frauduleux.

DKIM absent — DKIM (DomainKeys Identified Mail) appose une signature cryptographique sur chaque email sortant, permettant au destinataire de vérifier que le message n'a pas été altéré en transit. Sans DKIM, les emails légitimes ont plus de chances d'être classés comme spam.

Services détectés

Les services suivants ont été identifiés par le scan de ports (Nmap). Chaque service exposé sur Internet constitue un point d'entrée potentiel pour un attaquant.

Port	Service	Produit	Version	CPE
80	http	Apache-Coyote/1.1	—	—
443	https	Apache-Coyote/1.1	—	—
8080	http	Apache-Coyote/1.1	—	—

Matrice ports x risque

Web

Port 8080
Apache Tomcat/Coyote

Port 80
Apache Tomcat/Coyote

Port 443
apache-coyote

Les services de base de données, cache, conteneur et administration distante ne devraient jamais être joignables depuis Internet (rouge = critique, orange = élevé, jaune = moyen).

Stack technologique détectée

Apache Tomcat

version détectée

Java

version détectée

Apache-Coyote

v 1.1 · version détectée

Système d'exploitation détecté (empreinte réseau)

Empreinte TCP/IP relevée par nmap. Un OS obsolète élargit la surface d'attaque (exploits noyau connus, fin de support des correctifs).

- Microsoft Windows Server 2008 R2 or Windows 7 SP1 — fiabilité 89 %
- Microsoft Windows Server 2008 R2 or Windows 8 — fiabilité 89 %
- Microsoft Windows 7 or Windows Server 2008 R2 — fiabilité 85 %
- Microsoft Windows Server 2008 R2 SP1 or Windows 8 — fiabilité 85 %
- Microsoft Windows Server 2016 — fiabilité 85 %

Port 80 — Service web : Ce port expose le site web principal. Il constitue la surface d'attaque la plus large car il est accessible à tout le monde. **Recommandation** : Configurer les headers de sécurité, forcer HTTPS, déployer un WAF.

Port 443 — Service web : Ce port expose le site web principal. Il constitue la surface d'attaque la plus large car il est accessible à tout le monde. **Recommandation** : Configurer les headers de sécurité, forcer HTTPS, déployer un WAF.

Port 8080 — Service web / applicatif (HTTP alternatif) : Le port 8080 héberge fréquemment des consoles d'administration ou applicatifs (proxy, CI, serveurs d'applications) parfois moins durcis que le front principal. **Recommandation** : Identifier le service exact, appliquer authentification et headers de sécurité, restreindre l'accès si console d'administration.

Intelligence infrastructure (Shodan / IPInfo / AbuseIPDB / GreyNoise)

Synthèse des données de renseignement passif agrégées par adresse IP. Lignes en rouge : réputation suspecte (score AbuseIPDB > 25, classification malveillante, ou CVE exposées sur la bannière Shodan).

IP	ASN / Pays	Score AbuseIPDB	GreyNoise	CVE (Shodan)
65.61.137.117	AS33070 Rackspace Hosting / US	0/100	—	—

Toutes les IP analysées présentent une réputation acceptable (score AbuseIPDB ≤ 25, pas de classification malveillante GreyNoise).

Cartographie de l'hébergement par IP

65.61.137.117

AS33070 Rackspace Hosting

hors UE

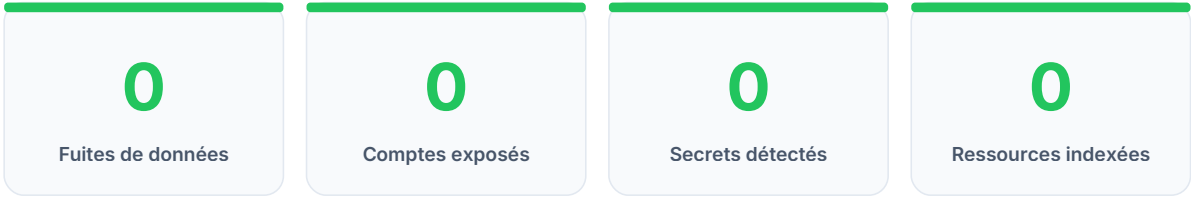
Réputation : saine

Résultats des scanners

Scanner	Résultat
SQLMap	0 URL testée, 0 injection détectée
Nuclei	17 correspondances sur 7000+ templates (terminé)
WAF/CDN	Aucun WAF/CDN détecté

Renseignement ouvert (OSINT)

Cette section rassemble les expositions de surface détectées par les sources OSINT (Open Source Intelligence) : secrets dans le code public, ressources sensibles indexées par les moteurs de recherche, buckets cloud accessibles.



Secrets exposés

Aucun secret détecté (scan Gitleaks / TruffleHog sur les sources publiques associées au domaine).

Google dorks indexés

Aucune ressource sensible confirmée indexée par les moteurs de recherche pour ce domaine.

Exposition cloud

Provider	Bucket / Resource	Statut	ACL
s3	demo-public	À vérifier	—

Remédiation

Synthèse de la feuille de route

Budget estimé total : **22 à 40 jours-homme** (17 k à 31 k€ base TJM 800€). Le détail par vulnérabilité figure dans la section "Vulnérabilités identifiées" et la section "Cockpit d'exploitabilité".

Horizon	Compteur	Top 3 actions
Quick wins < 7 jours	20	• DMARC absent sur demo.testfire.net (score 32) — Restreindre / corriger : Ajouter : _dmarc.demo.testfire.net IN TXT "v=DMARC1; p=quarantine; rua=mailto:dmarc@demo.testfire.net" • SPF absent sur demo.testfire.net (score 32) — Restreindre / corriger : Ajouter un enregistrement TXT SPF : v=spf1 include:_spf.provider.net -all • En-tête de sécurité manquant : content-security-policy (score 18) — Définir une CSP stricte : `Content-Security-Policy: default-src 'self'; script-src 'self'; style-src 'self'; img-src 'self' data;; connect-src 'self'; frame-ancestors 'none'; base-uri 'self'; form-act`
Moyen terme < 30 jours	8	• Default credentials acceptés sur /login.jsp (score 95) — 1. CHANGER IMMÉDIATEMENT le mot de passe par défaut (priorité absolue). 2. Forcer la rotation des credentials sur tous les comptes par défaut. 3. Activer l'authentification multi-facteurs (MFA). 4. Me • Cross Site Scripting (Reflected) (score 81) — Phase: Architecture and Design Utilisez a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. Examples of libraries and fr • TLS — Certificate chain untrusted (Android) (demo.testfire.net) (score 81) — Restreindre / corriger : Verify intermediate certificates and root CA.
Long terme < 90 jours	33	• Deprecated TLS Detection (score 67) — • Hébergement hors UE (transferts internationaux RGPD à vérifier) (score 32) — Documenter les Clauses Contractuelles Types (CCT) avec le fournisseur. Considérer hébergement EU-west (AWS Frankfurt, OVH Gravelines, Scaleway Paris) pour les données sensibles. • DNSSEC non configuré (score 32) — Activer DNSSEC auprès de votre registrar ou hébergeur DNS : 1) Générer les clés DNSSEC (KSK et ZSK) ; 2) Signer la zone DNS ; 3) Publier l'enregistrement DS dans la zone parente via le registrar ; 4)
		Transformations structurelles : refonte WAF, politique patch management, gouvernance sécurité (NIS2 art. 21).

Horizon	CompteurTop 3 actions
Straté- gique > 90 jours	

Re-scan recommandé 30 jours après les quick wins, puis 90 jours après les actions moyen terme pour valider l'efficacité des corrections. Score cible après remédiation : **25-35/100**.

Échéances recommandées par sévérité

Positionnement des vulnérabilités sur trois échéances calculées à partir de la date de début du scan (29 juillet 2026) : **30 j — 28 août 2026 · 90 j — 27 octobre 2026 · 180 j — 25 janvier 2027**.



- À retenir.** Trois jalons structurent la remédiation :
- **Sous 30 jours — 28 août 2026** : corriger les 1 vulnérabilité critique et les 7 élevées (exploitables depuis Internet).
 - **Sous 90 jours — 27 octobre 2026** : traiter les 2 vulnérabilités moyennes.
 - **Sous 180 jours — 25 janvier 2027** : résorber les 22 vulnérabilités faibles et durcir la configuration.

Conclusion

Conclusion technique et perspectives

1. Synthèse technique priorisée

L'analyse de surface d'attaque révèle un score de risque de **92/100**, plaçant le périmètre audité en **zone critique**. Sur les **61 observations** relevées, **1 vulnérabilité critique** (CVSS ≥ 9.0) et **7 vulnérabilités élevées** (CVSS 7.0–8.9) nécessitent une remédiation prioritaire sous 72 heures à 7 jours selon les référentiels CISA BOD 22-01.

Cause racine identifiée : l'exposition directe de services d'infrastructure non authentifiés ou insuffisamment durcis constitue le vecteur d'entrée principal. L'acceptation de credentials par défaut sur des interfaces d'administration web, combinée à l'absence de contrôles d'accès réseau restrictifs, permet une compromission initiale triviale. Cette situation traduit une lacune dans les processus de durcissement post-déploiement et de gestion du cycle de vie des secrets.

Les vulnérabilités critiques et élevées se concentrent sur trois catégories : - **Authentification faible** : comptes par défaut actifs, absence de mécanismes anti-bruteforce ; - **Exposition de services sensibles** : interfaces d'administration accessibles depuis Internet sans segmentation réseau ; - **Configuration défaillante** : absence de headers de sécurité, chiffrement TLS obsolète ou absent, services versionnés vulnérables.

2. Prochaines étapes et jalons de remédiation

Échéance J+30 : - Remédiation complète des findings critiques et élevés avec validation par re-scan automatisé ; - Mise en œuvre de contrôles compensatoires (WAF, IP whitelisting) sur les services d'infrastructure exposés en attendant leur désactivation ou migration interne ; - Rotation forcée de l'ensemble des secrets par défaut identifiés et déploiement de l'authentification multi-facteurs sur les interfaces d'administration ; - Audit des comptes de service et désactivation des comptes dormants ou de test (type `jsmith`, `admin`, `demo`).

Échéance J+90 : - Réduction du périmètre exposé : migration des services d'infrastructure (panels d'administration, bases de données, API internes) derrière un VPN ou bastion avec authentification forte ; - Déploiement de politiques de durcissement automatisées (CIS Benchmarks, STIGs) sur l'ensemble des composants web et applicatifs ; - Mise en conformité des configurations TLS (grade SSL Labs A minimum) et déploiement de DMARC en mode `reject` sur l'ensemble des domaines ; - Pentest applicatif ciblé sur les interfaces d'administration et les flux d'authentification.

Échéance J+180 : - Audit de code source sur les composants custom identifiés comme vulnérables (injection, SSRF, LFI) ; - Exercice Red Team simulant un scénario d'attaque par compromission initiale via credentials par défaut, suivi de mouvement latéral et exfiltration ; - Intégration continue de scans de surface d'attaque (hebdomadaire) avec alerting automatique sur nouveaux assets exposés ou findings KEV.

3. Indicateurs de suivi RSSI

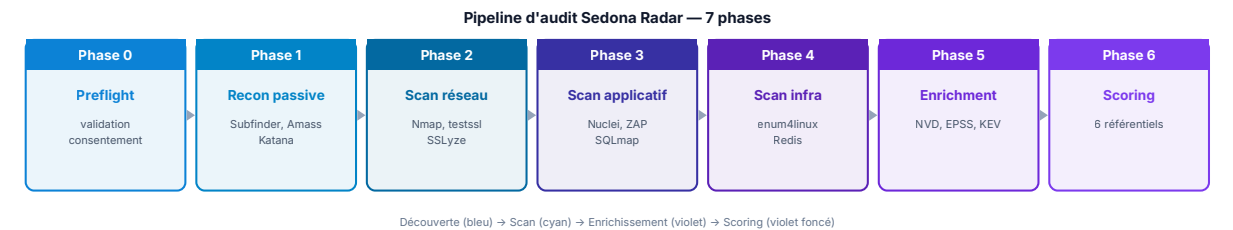
Les objectifs quantitatifs suivants doivent guider le plan de remédiation et faire l'objet d'un reporting mensuel au CODIR :

Indicateur	Valeur actuelle	Cible J+30	Cible J+90	Cible J+180
Score de risque ASM	92/100	≤ 60/100	≤ 35/100	≤ 25/100
Findings critiques ouverts	1	0	0	0
Findings élevés ouverts	7	≤ 2	0	0
Services d'infrastructure exposés	N (à qualifier)	-50%	-90%	0
Findings KEV (CISA) ouverts	0 (à valider)	0	0	0
Respect SLA CISA 21 jours	À établir	100%	100%	100%
Grade SSL Labs	À qualifier	B minimum	A	A+
DMARC en mode reject	Non	Non	Oui	Oui
Authentification MFA	Partielle	100% admin	100% users	100% + SSO

Recommandations de suivi : - **Re-scan ASM à J+30 et J+90** pour valider la cinétique de remédiation et détecter toute régression ou nouveau vecteur d'exposition ; - **Audits complémentaires** : pentest interne (J+60), audit de code source sur composants custom (J+90), exercice Red Team (J+180) ; - **Gouvernance** : revue mensuelle du backlog de remédiation avec priorisation CVSS × exposition × criticité métier ; escalade CODIR si dérive du planning > 15 jours.

La trajectoire de remédiation vise un retour en **zone de risque acceptable (score ≤ 35/100) sous 90 jours**, conditionnée à l'allocation des ressources engineering nécessaires et à l'arbitrage des dépendances applicatives. Tout écart significatif devra faire l'objet d'une analyse de risque résiduel formalisée et d'une acceptation explicite par le Risk Owner.

Annexe F — Méthodologie détaillée



Pipeline d'audit (7 phases)

Phase 0 — Preflight

Validation DNS du domaine cible, vérification du consentement, contrôle de la blacklist (adresses IP privées, domaines gouvernementaux). Aucun scan n'est lancé sans consentement explicite et vérification du périmètre.

Phase 1 — Reconnaissance passive

Découverte de la surface d'attaque sans interaction directe avec la cible.

Outil	Rôle
Subfinder	Enumération de sous-domaines via sources passives (APIs, CT logs)
Amass	Cartographie DNS et découverte d'actifs
Katana	Crawling web et découverte d'URLs
TruffleHog	Détection de secrets dans les dépôts publics
HIBP	Vérification des fuites de données connues
SerpAPI	Recherche Google Dorks pour fuites d'information
Shodan	Intelligence sur les services exposés
IPinfo	Géolocalisation et ASN des adresses IP
AbuseIPDB	Réputation des adresses IP
GreyNoise	Classification du trafic (bénin vs malveillant)
OTX AlienVault	Indicateurs de compromission
GrayhatWarfare	Détection de buckets cloud exposés

Phase 2 — Scan réseau

Outil	Rôle
Masscan	Scan de ports TCP rapide (top 1000 ports)
Rustscan	Scan de ports complémentaire haute performance
Nmap (T3 + NSE)	Fingerprinting des services, détection de versions, scripts NSE
testssl.sh	Analyse complète de la configuration SSL/TLS
SSLyze	Vérification des certificats et des cipher suites
Headers audit	Analyse des en-têtes HTTP de sécurité
Playwright	Captures d'écran des interfaces web exposées

Phase 3 — Scan applicatif

Outil	Rôle
Nuclei	Scan de vulnérabilités (7 000+ templates)
Nikto	Scan de serveur web (configurations, fichiers exposés)
Feroxbuster	Découverte de répertoires et fichiers cachés
SQLmap	Détection d'injections SQL (niveau L3, risque R2)
OWASP ZAP	Scan de vulnérabilités web automatisé
WPScan	Audit spécifique WordPress (plugins, themes, utilisateurs)
JS Analysis	Extraction de secrets et endpoints dans le JavaScript
Arjun	Découverte de paramètres HTTP cachés

Phase 4 — Scan infrastructure

Outil	Rôle
enum4linux-ng	Enumération SMB (partages, utilisateurs)
Redis scan	Détection de bases Redis non authentifiées
MongoDB scan	Détection de bases MongoDB exposées
Elasticsearch scan	Détection de clusters Elasticsearch ouverts
Docker API scan	Détection d'API Docker exposées
LDAP scan	Détection de serveurs LDAP accessibles
SMTP scan	Analyse de la configuration du serveur mail
OpenVAS	Scan de vulnérabilités infrastructure (conditionnel)

Phase 5 — Enrichissement

Source	Rôle
CVE Linker	Corrélation vulnérabilités/CVE (triple recherche : CPE, keyword, produit)
NVD (NIST)	Scores CVSS v3.1 officiels et descriptions
FIRST EPSS	Probabilité d'exploitation dans les 30 jours
CISA KEV	Catalogue des vulnérabilités activement exploitées
ExploitDB	Exploits publiquement disponibles
Metasploit	Modules d'exploitation automatisés
MITRE ATT&CK	Mapping tactiques et techniques d'attaque
CERT-FR	Alertes et avis de sécurité nationaux

Phase 6 — Scoring et conformité

Score composite (par vulnérabilité)

Chaque vulnérabilité reçoit un score composite (0-100) calculé selon la formule :

Indicateur	Poids	Source	Description
CVSS v3.1	50%	NVD (NIST)	Score standardisé de sévérité technique
EPSS	30%	FIRST.org	Probabilité d'exploitation dans les 30 jours
CISA KEV	+25 pts	CISA (USA)	Vulnérabilité activement exploitée
Module Metasploit	+15 pts	Rapid7	Module d'exploitation Metasploit disponible
Exploit public / PoC	+10 pts	ExploitDB	Code d'exploitation ou preuve de concept publié
Confiance faible	-30%	Multi-outils	Réduction si confiance < 40%

Score de confiance (par vulnérabilité)

Le score de confiance (0-100%) évalue la fiabilité de chaque finding en fonction du nombre d'outils qui le détectent (consensus multi-outils), de la fiabilité historique de chaque outil, et de la déduplication sémantique. Les vulnérabilités avec une confiance inférieure à 40% voient leur score composite réduit de 30%. Les faux positifs signalés par l'utilisateur sont exclus du scoring.

Conformité (6 référentiels)

Référentiel	Contrôles évalués	Total	Méthode
NIS2 (Art. 21.2)	4	10	

Référentiel	Contrôles évalués	Total	Méthode
			Mapping vulnérabilités vers articles (e, h, i, j évaluables en externe)
OWASP Top 10 2021	7	10	Mapping CWE déterministe (A04/A08/A09 requièrent un audit interne)
CIS Controls v8	12	18	Évaluation des contrôles techniques
ANSSI Hygiène	16	42	Mapping vers les 42 mesures
ISO 27001:2022	13	93	Contrôles Annexe A technologiques
ReCyF — cadre Sedona (auto-évaluation)	8	20	Auto-évaluation cyberhygiène, inspiré ANSSI v2.0 + NIS2 FR

Seuls les contrôles évaluables depuis la surface externe sont mesurés. Les contrôles organisationnels, RH et physiques nécessitent un audit interne complémentaire.

Phase 7 — Génération du rapport

Le rapport repose sur une **architecture à slots éditoriaux**. La structure du document, les tableaux, les scores, les identifiants CVE, les scores CVSS/EPSS et l'ensemble des données factuelles sont assemblés de manière **entièrement déterministe** à partir des résultats de scan et des bases de référence : ils sont reproductibles et vérifiables, sans aucune intervention générative.

Seuls des **slots rédactionnels ciblés** (synthèses, mises en contexte business, vulgarisation) sont confiés à des modèles de langage adaptés à chaque usage — un modèle de raisonnement pour les synthèses à enjeu, un modèle plus léger pour les reformulations courtes. Chaque slot reçoit un contexte restreint à sa seule section et ne peut ni créer, ni altérer une donnée technique. Une validation programmatique vérifie ensuite l'absence de CVE fabriquées, de dates incohérentes, d'emoji et de champs non renseignés, suivie d'une passe de relecture rédactionnelle.

Le rapport est rendu en PDF via WeasyPrint, avec polices professionnelles embarquées (Inter, Source Serif, JetBrains Mono), visualisations SVG générées et pagination automatique.

Glossaire technique DSI / RSSI — 30 termes

Définitions techniques précises avec références (RFC, NIST, MITRE, OWASP). Pensé pour DSI, RSSI, architectes sécurité, équipes SOC.

MENACES & VULNÉRABILITÉS

CVE — Common Vulnerabilities and Exposures — identifiant standard MITRE. Format `CVE-AAAA-NNNNN`.

CVSS v3.1 — Common Vulnerability Scoring System (FIRST). Vecteur AV/AC/PR/UI/S/C/I/A. Score 0,0-10,0. v4.0 publiée mais NVD publie encore en v3.1.

EPSS — Exploit Prediction Scoring System (FIRST). Probabilité 0-1 d'exploitation dans les 30 j. Mis à jour quotidiennement.

En clair : Une météo du risque : la probabilité qu'une faille soit réellement attaquée dans le mois. Le CVSS dit « c'est grave si exploité » ; l'EPSS dit « voici la chance que ça le soit vraiment ».

KEV — Known Exploited Vulnerabilities catalog (CISA). Vulns avec exploitation avérée. SLA correction CISA : 21 jours.

MITRE ATT&CK — Framework de tactiques/techniques adversaires (TTP). 14 tactiques, 200+ techniques. Référence pour threat modeling.

OWASP Top 10 — Top 10 risques applis web OWASP (versions 2021 et 2025). Référence audit web.

CWE — Common Weakness Enumeration (MITRE). Taxonomie des faiblesses logicielles (~600). Cité par chaque CVE.

RCE — Remote Code Execution. Exécution de code arbitraire à distance. Souvent CVSS 9-10.

SSRF — Server-Side Request Forgery (OWASP A10:2021). Permet d'atteindre métadonnées cloud (AWS IMDS, GCP metadata).

En clair : On piège votre serveur pour qu'il aille chercher lui-même une ressource interne à la place de l'attaquant : le serveur, digne de confiance sur le réseau, devient le coursier de l'intrus et peut lire des secrets cloud inaccessibles de l'extérieur.

IDOR / BOLA — Insecure Direct Object Reference / Broken Object Level Authorization (API). Nécessite test authentifié.

XSS — Cross-Site Scripting (Stored / Reflected / DOM). Mitigé par CSP + escape contextuel.

CSRF — Cross-Site Request Forgery. Mitigé par tokens synchroniser ou SameSite cookies.

DÉTECTION & RÉPONSE

SOC — Security Operations Center. Modèles SIEM-driven ou XDR-driven. Mesuré en MTTD/MTTR.

SIEM — Security Information & Event Management. Collecte logs, corrélation, alerting (Splunk, Elastic, Sentinel, Wazuh).

EDR / XDR — Endpoint / eXtended Detection & Response. Télémétrie endpoint + réponse automatisée.

MDR — Managed Detection & Response. SOC externalisé 24/7 (CrowdStrike, Arctic Wolf, Sekoia, Tehtris).

WAF — Web Application Firewall. Filtrage couche 7 (Cloudflare, AWS WAF, Akamai, ModSecurity).

CDN — Content Delivery Network. Réduit latence + protection DDoS L7. Rôle double sécurité/performance.

IDS / IPS — Intrusion Detection / Prevention System. Réseau (Suricata, Snort, Zeek) ou hôte (OSSEC, Wazuh).

PAM — Privileged Access Management (CyberArk, BeyondTrust, HashiCorp Vault). Coffre-fort + rotation + session recording.

DURCISSEMENT & PROTOCOLES

CSP — Content Security Policy (W3C). Header HTTP qui limite les sources autorisées. Mitigation XSS forte.

En clair : Une liste blanche des serveurs autorisés à fournir scripts, images et styles à votre page ; tout script injecté depuis une source non listée est bloqué par le navigateur. Le pirate qui ne laisse entrer que les invités sur la liste.

HSTS — HTTP Strict Transport Security (RFC 6797). Force HTTPS côté navigateur. Pré-charge via hstspreload.org.

En clair : Une fois le site visité en HTTPS, le navigateur refuse ensuite toute connexion non chiffrée à ce domaine — même si l'utilisateur tape l'adresse en `http://`. Empêche l'interception sur un Wi-Fi public.

CORS — Cross-Origin Resource Sharing (Fetch spec). Une mauvaise configuration `Access-Control-Allow-Origin: *` + credentials = fuite.

SPF / DKIM / DMARC — Authentification email (RFC 7208 / 6376 / 7489). DMARC en `p=reject` bloque le spoofing du domaine.

DNSSEC — DNS Security Extensions (RFC 4033-4035). Signature cryptographique des réponses DNS. Prérequis ANSSI.

En clair : Une signature infalsifiable sur les réponses de l'annuaire Internet : elle garantit que l'adresse renvoyée pour `votresite.fr` vient bien du vrai domaine et n'a pas été falsifiée en chemin pour détourner vos visiteurs.

MFA / 2FA — Multi-Factor Authentication. Préférer TOTP/FIDO2 à SMS (SIM-swapping). Microsoft : -99,9 % compromissions compte.

PKI — Public Key Infrastructure. Gestion cycle de vie certificats (CA, RA, CRL, OCSP). Standard X.509.

mTLS — Mutual TLS. Authentification client+serveur par certificat. Standard service mesh (Istio, Linkerd).

SBOM — Software Bill of Materials (SPDX, CycloneDX). Obligation contractuelle US Executive Order 14028. Recommandé NIS2.

Zero Trust — Modèle NIST SP 800-207. Never trust, always verify. Microsegmentation + identity-aware proxy.

En clair : On cesse de considérer le réseau interne comme sûr : chaque accès est re-vérifié (identité, appareil, contexte), comme un immeuble où le badge est recontrôlé à chaque porte plutôt qu'une seule fois à l'entrée.

À propos de Sedona AI

Pour les équipes sécurité — Sedona Radar orchestre 45+ outils open-source enrichis par 14 sources de threat intelligence. Le pipeline reproduit la méthodologie d'un pentester externe expert, à l'échelle automatisée.

Stack technique

- **Scanners actifs** — Nmap, Nuclei, ZAP, SQLmap, testssl.sh, Nikto, WhatWeb, Wapiti, dnsx, httpx, subfinder, amass, naabu, gowitness.
- **Threat intelligence** — NVD, CISA KEV, FIRST EPSS, MITRE ATT&CK, CERT-FR, HavelBeenPwned, AbuseIPDB, GreyNoise, Shodan InternetDB, AlienVault OTX, URLhaus, Tranco, crt.sh, Have I Been Squatted.
- **Conformité** — OWASP Top 10 (2021 & 2025), CIS Controls v8, ANSSI Hygiène, NIS2, ISO 27001, ReCyF.

Méthodologies de référence

- **PTES** (Penetration Testing Execution Standard) — 7 phases.
- **OWASP Testing Guide v4.2** — surface web.
- **NIST SP 800-115** — guide technique d'évaluation de sécurité.
- **ANSSI — Guide d'hygiène informatique** (42 mesures).

Équipe

- **Vincent Coderch** — CEO.
- **Angel Venzac** — CTO. Architecture pipeline, scoring engine, infrastructure.

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

© 2026 Sedona AI — Tous droits réservés. Ce document est généré automatiquement par Sedona Radar. La reproduction ou la diffusion non autorisée est interdite.

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.