FLAWFENCE

Votre nouvel **auditeur cyber**

L'audit offensif de votre surface externe, en continu.

Compatible NIST 2 / ISO 27001 | Construit et hébergé à Paris | Propulsé par Mistral AI

Flawfence chez nos **clients**

MSSP

Opérateur multicloud français

Transformation du SI de ses clients

Scans en marque blanche, en continu.

PREMIER SCAN

2 critiques | 3 élevées

Exécution de code sur un WordPress (wp2shell)
↳ Environnement d'un client hébergé compromis
Identifiants de base de données exposés
↳ Données métier altérables

CLIENT FINAL

Courtier en protection sociale

Santé, prévoyance, retraite, épargne salariale

Périmètres externe et interne, services externalisés.

PREMIER SCAN

1 critique | 2 élevées

Console d'administration sans authentification
↳ Prise de contrôle anonyme de l'application
XSS sur le portail assurés
↳ Vol silencieux des identifiants

Retour d'expérience : gestion de crise wp2shell

SURFACE EXPOSÉE

IMPACT MÉTIER

DÉCOUVERTE

41 sous-domaines exposés

Énumération passive, sans agent ni identifiant

IDENTIFICATION

Un WordPress non maintenu sur blog.client-heberge.fr

Empreinte des technologies et des versions

EXPLOITATION

Exécution de code à distance confirmée

CVE-2026-63030, exploitation rejouée

IMPACT

Accès en écriture à la base de données métier

wp-config.php lu, identifiants en clair

De la construction du PoC à l'alerte en quelques **heures**

VEN. 17 JUIL. 2026
WORDPRESS
wp2shell divulguée, correctifs publiés

LE JOUR MÊME
FLAWFENCE
Module de détection déployé

+ 1 H
FLAWFENCE
Premières instances vulnérables détectées

DANS LA NUIT
GITHUB
Un exploit fonctionnel devient public

SAM. MATIN
FLAWFENCE
Exploitation rejouée dans le scan

SAM. MATIN +1H
FLAWFENCE
Alertes confirmées et envoyées

Chronologie complète de wp2shell →

Un **instantané**, au prix d'une surveillance

3 mois

du cadrage à la restitution

20 k€

par audit

1 / an

onze mois sans visibilité

Ils exploitent plus **vite** que vous ne corrigez

31 %

des accès initiaux passent par une faille exploitée

Verizon DBIR 2026, plus de 22 000 brèches. 20 % un an plus tôt.

43 jours

pour corriger une faille activement exploitée

Verizon DBIR 2026, délai médian, catalogue KEV de la CISA. 32 jours un an plus tôt.

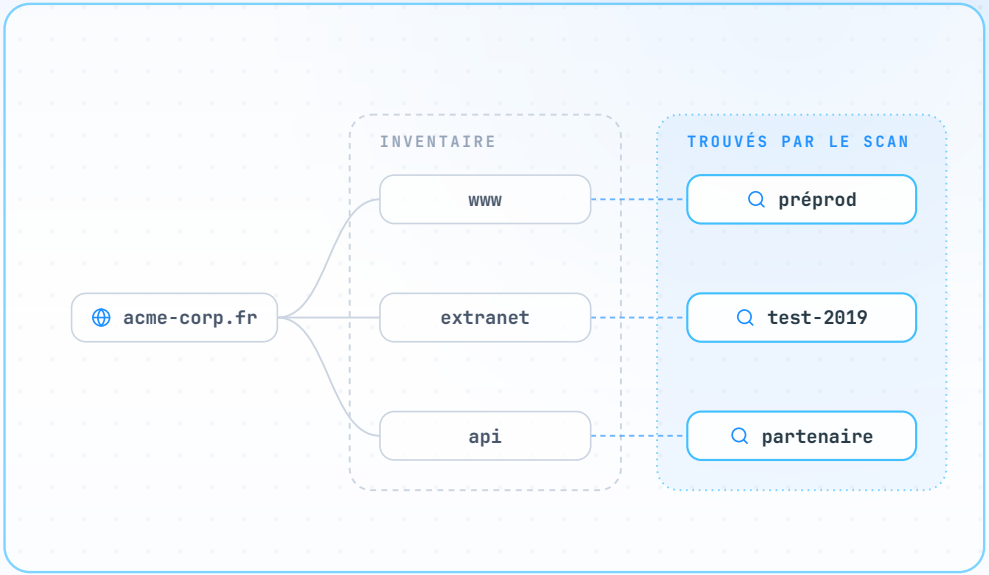
4,99 M$

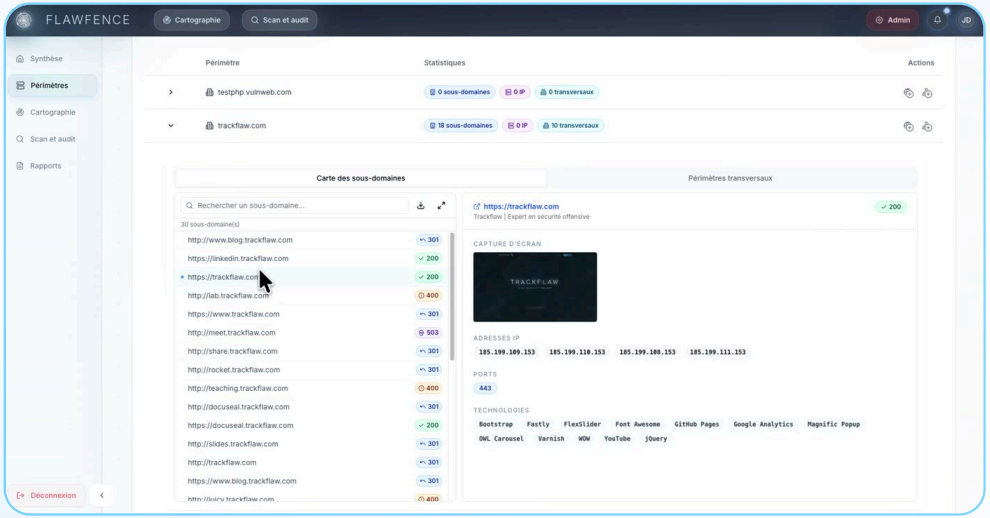
coût moyen d'une violation de données

IBM Cost of a Data Breach 2026, 602 organisations. En hausse de 12 % sur un an.

Votre inventaire n’est pas votre **périmètre**

- Une préproduction ouverte pour une démo
- Un sous-domaine de test jamais éteint
- Un partenaire qui pointe encore chez vous





Un auditeur qui ne **dort** pas

Un email professionnel, rien à installer.

- Le périmètre se reconstitue seul
- Premier rapport en moins de 24 h
- Le scan ne s'arrête plus

Quatre maillons, rejoués en boucle

01

Cartographier

Un sous-domaine de préproduction absent de l'inventaire.

DNS · OSINT · WHOIS

02

Identifier

Un Swagger public qui décrit l'API interne.

Banner grabbing · Nuclei · Httpx

03

Exploiter

Une injection SQL confirmée par la donnée renvoyée.

Fuzzing · Agentique · Dast

04

Alerter

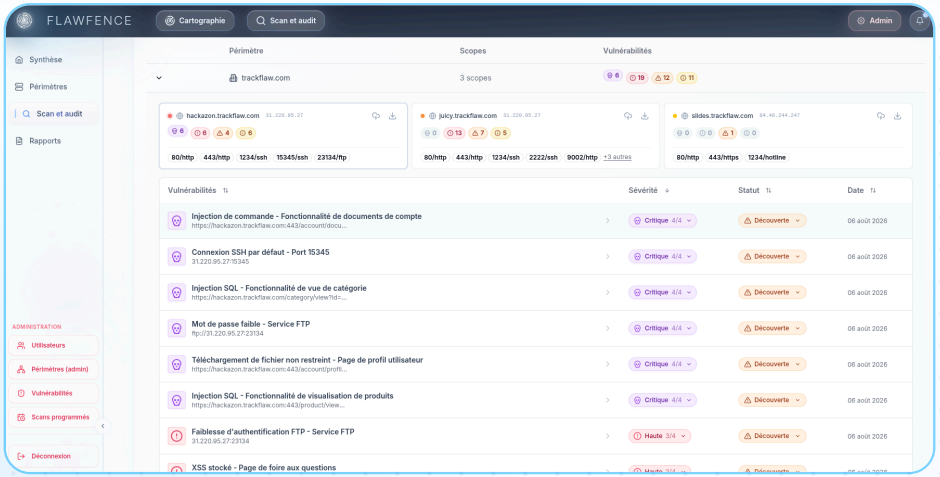
Une alerte critique dans Slack, la nuit même.

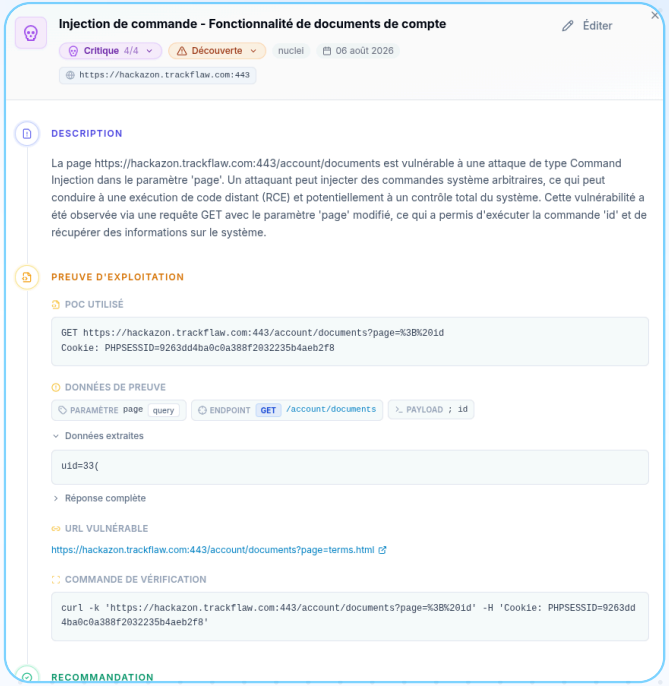
CVSS v4 · NIST 2 · SIEM

Le détail technique de chaque maillon →

Une **preuve** d'exploitation par vulnérabilité

- Rien de remonté sans exploitation confirmée
- Le test se rejoue avant d'ouvrir un ticket





Deux mesures, **méthode** comprise

+30 %

de sous-domaines découverts

tesla.com, sous-domaines avec un enregistrement DNS A actif.

+30 %

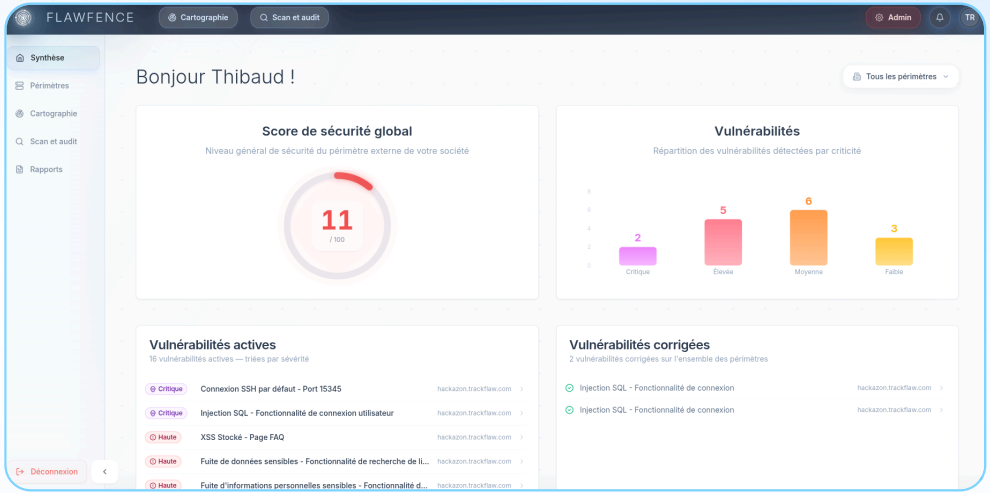
de vulnérabilités exploitables

Scan anonyme, configuration par défaut, plateforme hackazon.

Bug bounty sur YesWeHack Voir le compteur →

Un rapport pour vos équipes, un autre pour votre **direction**

- Rapport PDF conforme NIST 2
- Alerte immédiate sur les critiques
- Remédiation priorisée par exploitabilité



Française, de l’équipe à l’hébergement

- Hébergement à Paris, données en France
- Modèles Mistral AI pour l’analyse
- Exports conformes NIST 2 et ISO 27001

Un audit par an, ou toute l'**année**

L'audit ponctuel

20 k€ par audit

Le format habituel, refait chaque année.

- Cadrage, tests, restitution
- Un rapport daté du jour des tests

Flawfence

À partir de 5 000 € HT par an

Le périmètre se reconstitue seul, le scan tourne 24/7/365.

- Scan offensif continu
- Une preuve d'exploitation par vulnérabilité
- Alerte immédiate sur les critiques
- Rapports conformes NIST 2

Tarif selon la taille du périmètre.

Passons à votre **périmètre**

Une démonstration, sans engagement.

Demander une démonstration →

Lancer un aperçu gratuit

Aperçu passif, sans inscription.