



Your new **cyber** auditor

Continuous offensive auditing of your external surface.

✓ Compatible with NIST 2 / ISO 27001

📍 Built and hosted in Paris

🔥 Powered by Mistral AI

Flawfence at our **clients**

MSSP

French multicloud operator

IT transformation for its clients

White-label scans, continuously.

FIRST SCAN

2 critical

3 high

Code execution on a WordPress instance (wp2shell)

↳ A hosted client environment compromised

Exposed database credentials

↳ Business data open to tampering

END CLIENT

Employee benefits broker

Health, protection, retirement, employee savings

External and internal perimeters, outsourced services.

FIRST SCAN

1 critical

2 high

Admin console with no authentication

↳ Anonymous takeover of the application

XSS on the policyholder portal

↳ Silent theft of login credentials

Lessons learned: wp2shell crisis management

EXPOSED SURFACE

DISCOVERY

41 exposed subdomains

Passive enumeration, no agent, no credentials

IDENTIFICATION

An unmaintained WordPress on blog.hosted-client.com

Fingerprinting of technologies and versions

EXPLOITATION

Remote code execution confirmed

CVE-2026-63030, exploitation replayed

IMPACT

Write access to the business database

wp-config.php read, credentials in cleartext

BUSINESS IMPACT

From building the PoC to the alert in a few hours



The full wp2shell timeline →

A **snapshot**, at the price of monitoring

3 months

from scoping to debrief

€20k

per audit

1 / year

eleven months without visibility

They exploit **faster** than you patch

31%

of initial access starts with an exploited vulnerability

Verizon DBIR 2026, over 22,000 breaches. 20% a year earlier.

43 days

to remediate an actively exploited vulnerability

Verizon DBIR 2026, median time to fix, CISA KEV catalog. 32 days a year earlier.

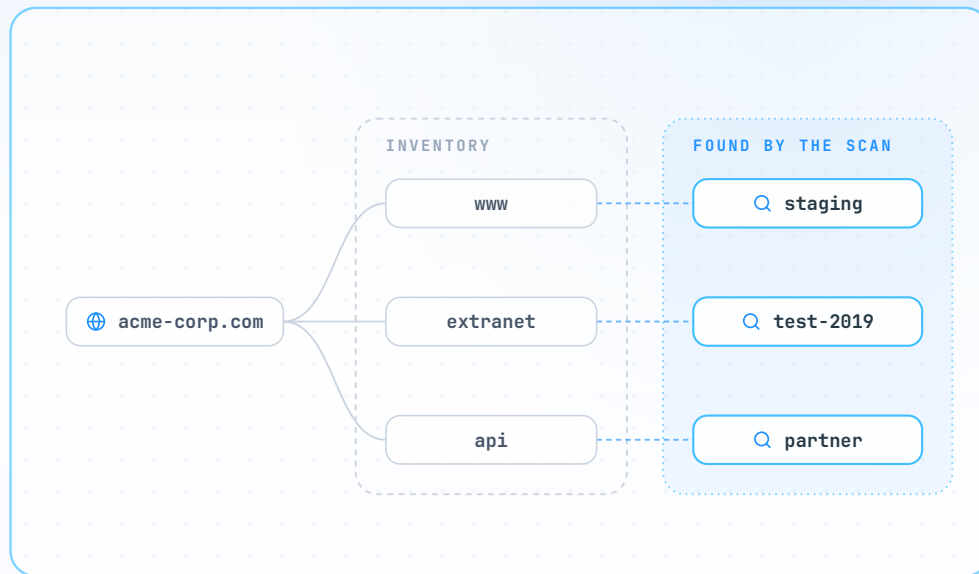
\$4.99M

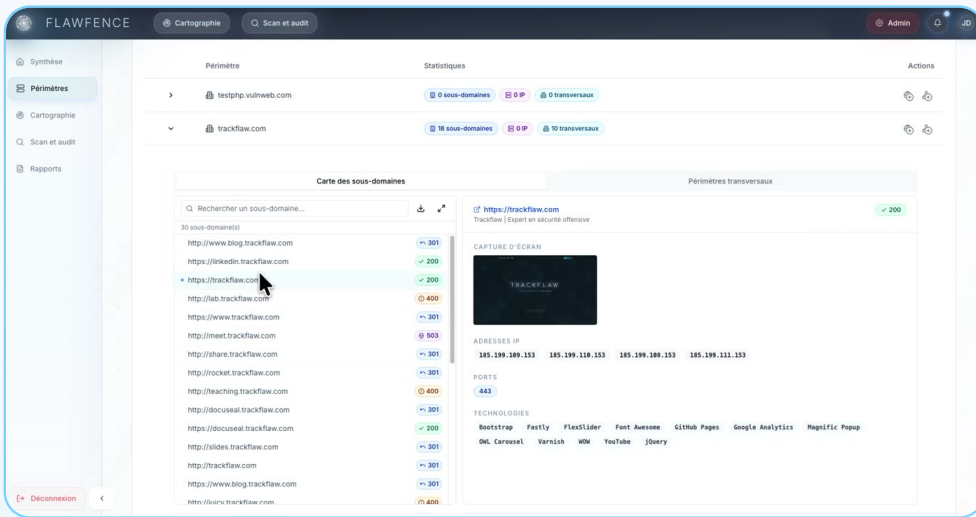
average cost of a data breach

IBM Cost of a Data Breach 2026, 602 organizations. Up 12% in one year.

Your inventory is not your **perimeter**

- ✓ A staging environment opened for a demo
- ✓ A test subdomain nobody shut down
- ✓ A partner service still pointing at you



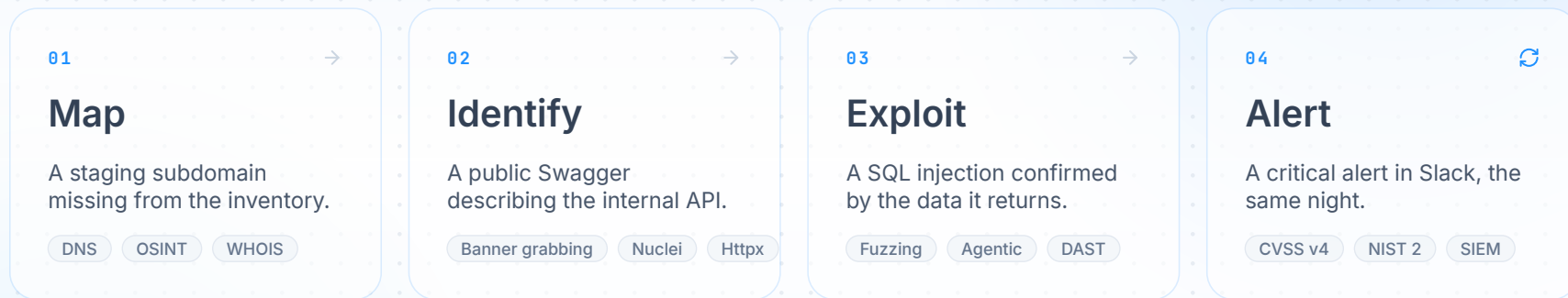


An auditor that never sleeps

A work email, nothing to install.

- ✓ The perimeter rebuilds itself
- ✓ First report in under 24 hours
- ✓ The scanning never stops

Four links, replayed on a loop



The technical detail of every link →

Proof of exploitation on every finding

- ✓ Nothing reported without confirmed exploitation
- ✓ Replay the test before opening a ticket

The screenshot shows the FLAWFENCE interface with a sidebar on the left containing 'ADMINISTRATION' and 'Utilisateurs'. The main area displays a table of vulnerabilities for the target 'trackflaw.com'. The table has columns for 'Vulnérabilités', 'Sévérité', 'Statut', and 'Date'. The first vulnerability is 'Injection de commande - Fonctionnalité de documents de compte' with a severity of 'Critique 4/4', status 'Découverte', and date '06 août 2026'. Other vulnerabilities include 'Connexion SSH par défaut - Port 15345', 'Injection SQL - Fonctionnalité de vue de catégorie', 'Mot de passe faible - Service FTP', 'Téléchargement de fichier non restreint - Page de profil utilisateur', 'Injection SQL - Fonctionnalité de visualisation de produits', 'Faiblesse d'authentification FTP - Service FTP', and 'XSS stocké - Page de foire aux questions'.

The screenshot shows the detail page for the vulnerability 'Injection de commande - Fonctionnalité de documents de compte'. It includes a 'DESCRIPTION' section explaining that the page is vulnerable to a Command Injection attack. The 'PREUVE D'EXPLOITATION' section shows the 'POC UTILISÉ' (GET request to /account/documents?page=38k291d) and 'DONNÉES DE PREUVE' (PARAMÈTRE: page, query; ENDPOINT: /account/documents; PAYLOAD: 1d). The 'URL VULNÉRABLE' is https://hackazon.trackflaw.com:443/account/documents?page=terms.html. The 'COMMANDE DE VÉRIFICATION' is curl -k 'https://hackazon.trackflaw.com:443/account/documents?page=K3BK201d' -H 'Cookie: PHPSESSID=9263dd4ba9c0a388f2032235b4aeb2f8'. The 'RECOMMANDATION' section is at the bottom.

Two measurements, **method** included

+30%

more subdomains discovered

tesla.com, subdomains with an active DNS A record.

+30%

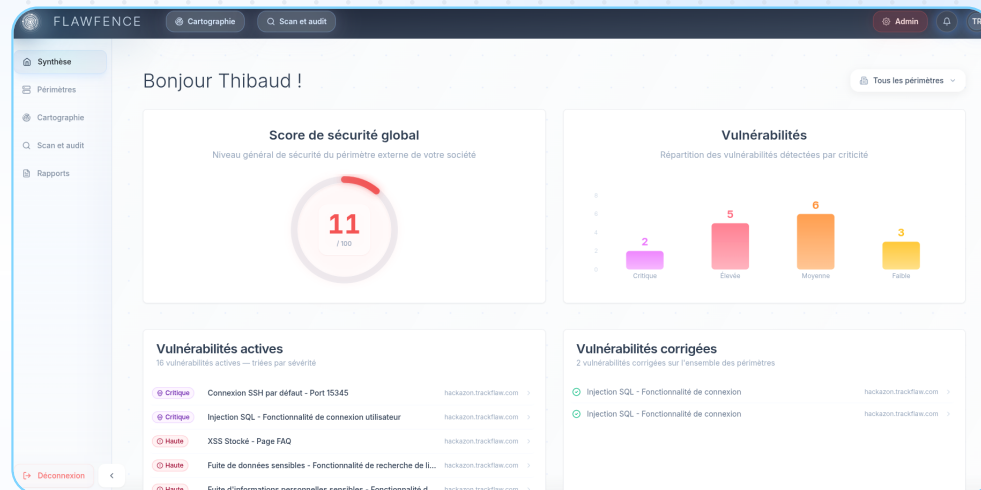
more exploitable vulnerabilities

Anonymous scan, default configuration, hackazon platform.

Bug bounty on YesWeHack [See the counter →](#)

One report for your teams, another for your **board**

- ✓ NIST 2 compliant PDF report
- ✓ Immediate alerts on critical findings
- ✓ Remediation prioritized by exploitability



French, from the team to the hosting



Hosted in Paris, data stays in France



Mistral AI models for the analysis



NIST 2 and ISO 27001 compliant exports

An audit once a year, or **continuously**

The one-off audit

€20k per audit

The usual format, repeated every year.

- ✓ Scoping, testing, debrief
- ✓ A report dated the day of the tests

Flawfence

From €5,000 excl. VAT per year

The perimeter rebuilds itself, scanning runs 24/7/365.

- ✓ Continuous offensive scanning
- ✓ Proof of exploitation on every finding
- ✓ Immediate alerts on critical findings
- ✓ NIST 2 compliant reports

Pricing scales with the size of the perimeter.

Let us look at your **perimeter**

A demo, no commitment.

Request a demo →

Run a free preview

Passive preview, no sign-up.