FLAWFENCE

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

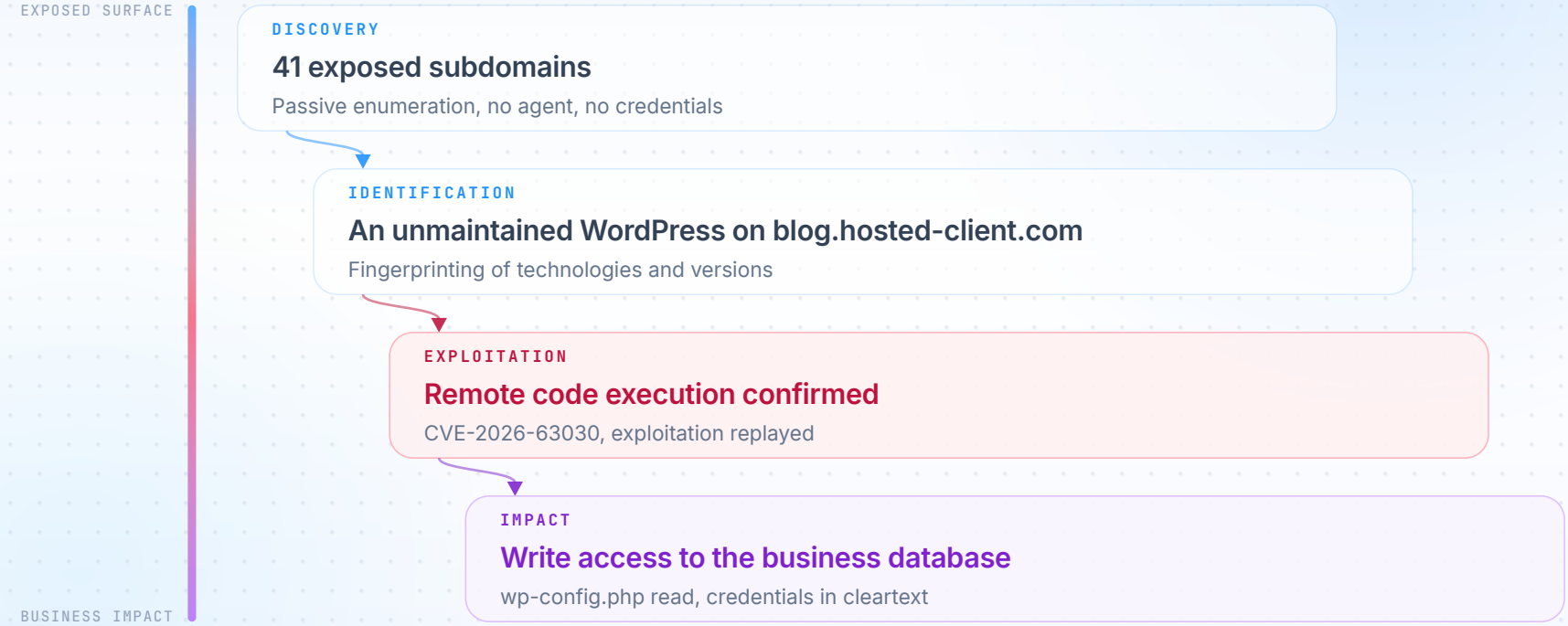
Admin console with no authentication

↳ Anonymous takeover of the application

XSS on the policyholder portal

↳ Silent theft of login credentials

Lessons learned: wp2shell crisis management



From building the PoC to the alert in a few **hours**

FRI. 17 JUL. 2026
WORDPRESS
wp2shell disclosed, patches published

SAME DAY
FLAWFENCE
Detection module rolled out

+ 1 H
FLAWFENCE
First vulnerable instances detected

THAT NIGHT
GITHUB
A working exploit goes public

SAT. MORNING
FLAWFENCE
Exploit replayed in the scan

SAT. MORNING +1H
FLAWFENCE
Alerts confirmed and sent

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.

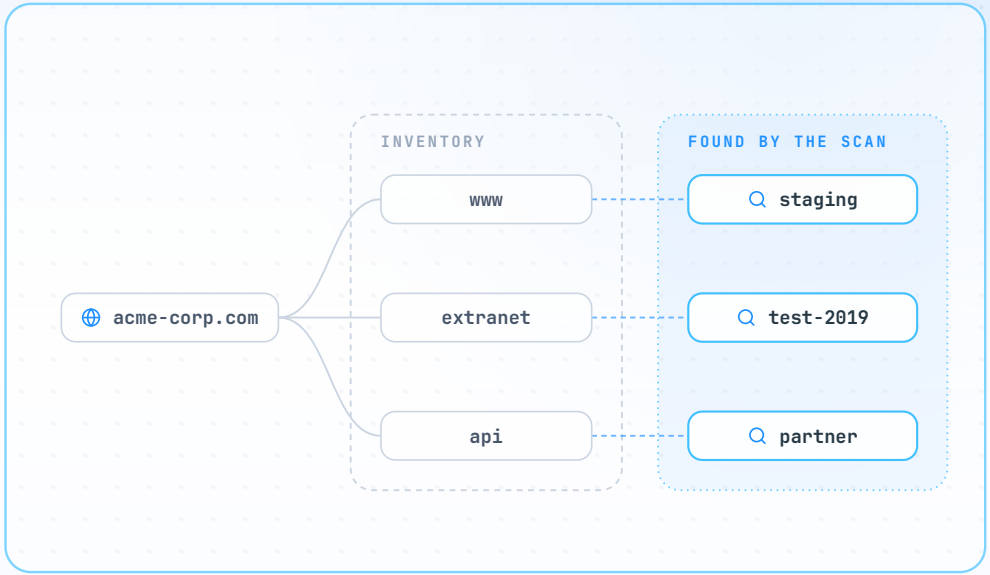
$4.99M

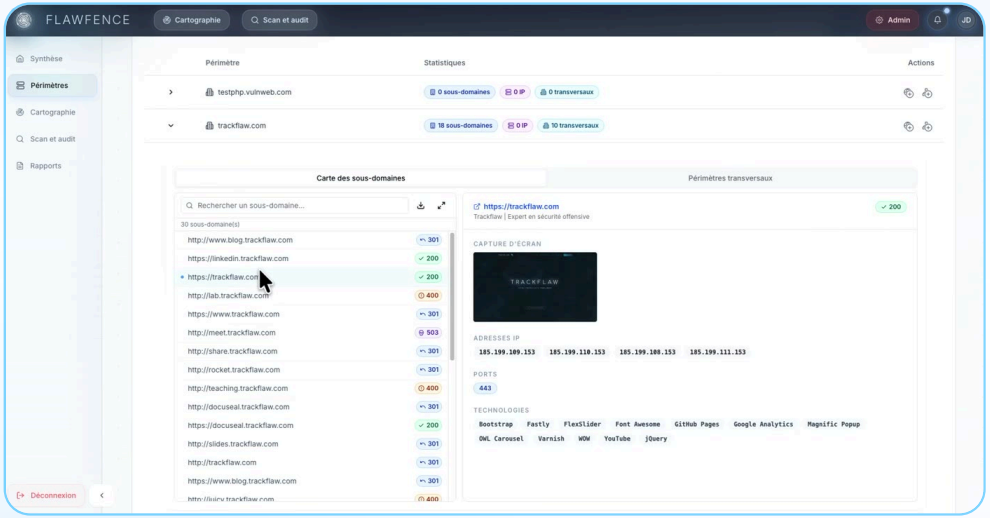
average cost of a data breach

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

01

Map

A staging subdomain missing from the inventory.

DNS · OSINT · WHOIS

02

Identify

A public Swagger describing the internal API.

Banner grabbing · Nuclei · Httpx

03

Exploit

A SQL injection confirmed by the data it returns.

Fuzzing · Agentic · DAST

04

Alert

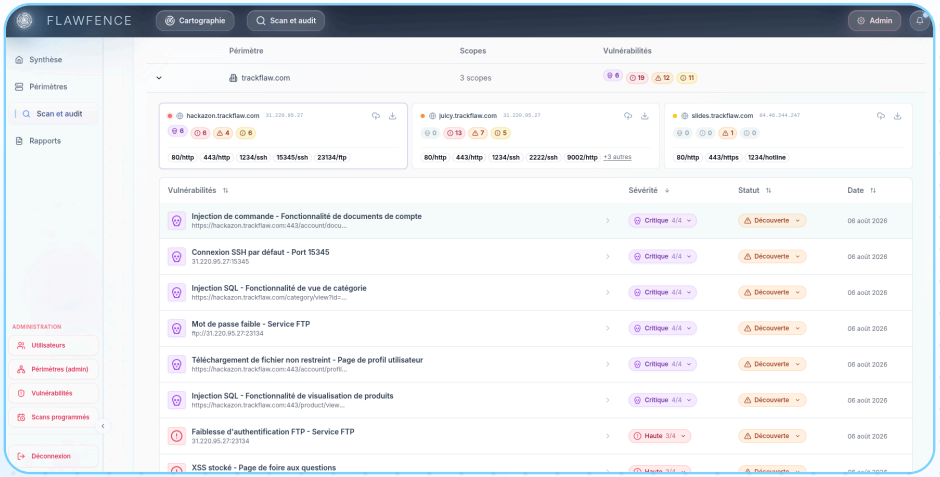
A critical alert in Slack, the same night.

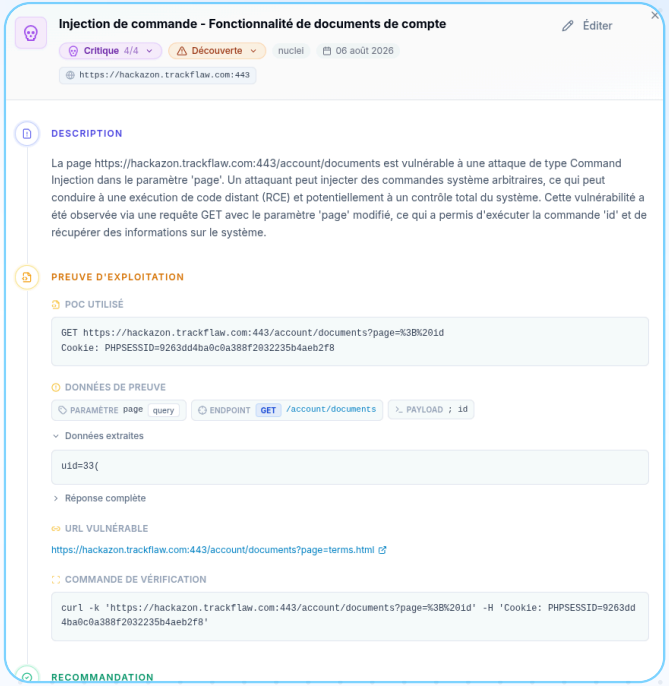
CVSS v4 · NIST 2 · SIEM

The technical detail of every link →

Proof of exploitation on every finding

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





Two measurements, **method** included

+30%

more subdomains discovered

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

+30%

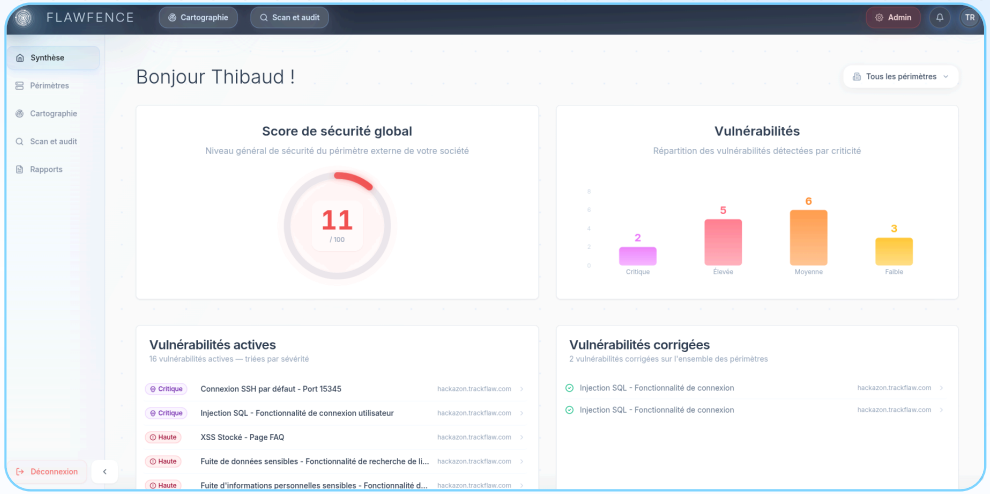
more exploitable vulnerabilities

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.