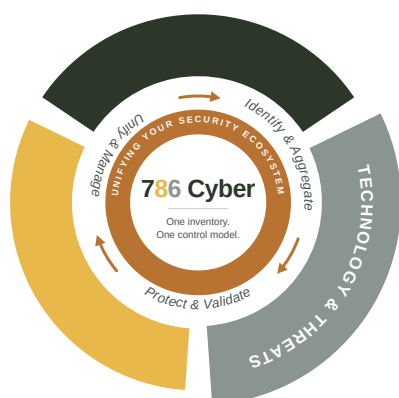


Know your exposure. Manage the risks that matter to your business.

Vulnerabilities, cloud posture, application exposure and external threat signal — scored by what is actually likely to be exploited, and explained in plain English.

A list of four thousand findings is not security work, it is a filing problem. This pillar takes the inventory built in Environment & People, works out what is genuinely exposed, ranks it by real-world exploit probability rather than raw severity, and tells you in plain English what to do about each one.



Prioritised by what attackers **actually exploit** — not by what scores highest.

Severity tells you how bad a vulnerability would be. Exploit probability and known-exploited status tell you whether anyone is bothering. We score with all three, against your own assets, so the queue is short enough to actually finish.

3

scoring inputs — CVSS,
EPSS, CISA KEV

12+

intelligence and scanning
sources

0

findings without a plain-
English explanation

WHAT IT DOES — AND WHAT CHANGES WHEN IT DOES

CAPABILITY	WHAT IT GIVES YOU	WHAT CHANGES
Internal CVE matching	Your own software and operating-system inventory matched against the National Vulnerability Database, continuously.	You learn what is vulnerable across your estate without buying, deploying and maintaining a separate scanner.
Exploitability-based prioritisation	Every finding scored with FIRST EPSS exploit probability and CISA Known Exploited Vulnerabilities status alongside CVSS severity.	Your team works a queue of the handful that matter this week instead of triaging thousands that never will.
Plain-English explanation per finding	What it is, why it matters to you specifically, and what to do — written for a competent generalist, not a specialist.	The person who can actually fix it no longer needs a security analyst to translate first.
Web application scanning	OWASP ZAP baseline passive scanning, plus a consent-gated active scan when you want to go deeper.	You stop paying annually for a scan that tells you what a continuous one would have told you in March.
Cloud posture	Prowler-based configuration checks across your cloud accounts — public storage, weak policies, exposed services.	The misconfigured bucket is found by you, on a Tuesday, rather than by somebody else at a worse moment.
External exposure discovery	What the internet can see of you, drawn from Shodan and Censys and matched to your own asset list.	The service someone stood up for a project in 2023 and never took down stops being invisible.
Domain and certificate monitoring	New certificates, new subdomains and lookalike domain registrations, watched continuously.	You catch the phishing domain while it is still being set up rather than after it has been used on your customers.
Threat intelligence and reputation	Open-source intelligence feeds and domain and IP reputation, prioritised against your actual assets rather than the internet at large.	Threat intelligence becomes something you act on rather than something you subscribe to.
Testing & Validation	Real active reconnaissance against your own estate — DNS, IP and application-layer tooling, admin-gated and run only with explicit per-session consent.	You can prove a control works on demand, and the result stays out of your automatic score so the score keeps meaning something.

Where it fits, and what to read next

For everyday security

A prioritised queue of what to fix first, scored by exploit probability and known-exploited status rather than severity alone, with a plain-English explanation attached to every finding.

For compliance

Every finding maps to the control it evidences, so vulnerability and cloud-posture work doubles as audit-ready proof for the frameworks that require it. The work you were doing anyway starts counting twice.

Testing & Validation — deliberately kept out of your score

Active reconnaissance sits inside this pillar, alongside the continuous capabilities rather than mixed into them. Its results are shown clearly and never feed the automatic posture score — a test you chose to run at a moment you chose is not the same evidence as continuous monitoring, and blending the two would make the score look better and mean less.

THREE MOTIONS IN THIS PILLAR — CONTINUOUS, NEVER A STEP

IDENTIFY & AGGREGATE

Findings from our scanners and yours — external exposure, web application scans, cloud misconfiguration, internal CVE matching, pen test reports — collected against the same assets.

PROTECT & VALIDATE

Every finding validated against NVD, EPSS and CISA KEV, weighted by asset importance and the controls already in place, explained in plain English. Consented active testing when you choose to run it.

UNIFY & MANAGE

One prioritised queue across four posture lanes, each scored on its own terms — never one blended number — with the fix, the owner and the control it affects.

THE POINT PRODUCTS THIS COVERS

- Vulnerability management (VM) — Vulnerability Prioritisation
- Cloud posture (CSPM) — Cloud Posture
- Web app scanning (DAST) — Web Application Scanning
- External attack surface (EASM) — External Attack Surface
- Threat intelligence (CTI) — Threat Intelligence & Reputation
- Pen-test tooling — Testing & Validation

BUILT ON OPEN STANDARDS YOU CAN CHECK

- NVD and CPE for internal CVE matching
- FIRST EPSS exploit probability and CISA KEV
- OWASP ZAP for web application scanning
- Prowler for cloud posture
- Shodan, Censys, VirusTotal, crt.sh, DNSTwist
- AlienVault OTX, URLhaus, RDAP, Spamhaus, AbuseIPDB

Point it at one domain and see what comes back

Add a single domain on the free trial and the external exposure view populates the same day — certificates, subdomains, exposed services and lookalike registrations, scored and explained. Most organisations find at least one thing they had forgotten they owned.

[Start free for 14 days — no card](#)
[Book a walkthrough](#)
786cyber.com

FURTHER READING

Environment & People data sheet

Know what you have — the inventory every finding on this page resolves back to.

Policy & Process data sheet

Prove it — how a fixed vulnerability becomes evidence against a control.

Testing & Validation data sheet

The consent model, the admin gate, and why results stay out of the score.

786 Cyber Platform Overview

The four-page introduction: three pillars, twelve point products, one platform.