PENTESTERRA

SEE THE REAL RISK

ATTACK SURFACE | REAL EXPOSURE | PROVEN SECURITY

AUTOMATE.
VALIDATE.
STAY AHEAD.

External Exposure Assessment

Know what's exposed. Before attackers do.

Fast, comprehensive and evidence-based assessment of your external exposure across domains, infrastructure, technologies, and third-party dependencies.

SCALE
50K+ targets

FAST
Seconds to minutes

NON-INTRUSIVE
Passive & light active checks

From single companies to global supply chains — at scale.

WHAT WE CHECK

Attack surface mapping
Domains, subdomains, resolved IPs, ASN, cloud providers and services.

Vulnerability intelligence
Known CVEs, KEV, EPSS scoring and real exploitability context.

Web & service security
Open ports, exposed services, HTTP headers, TLS/SSL analysis, misconfigurations, default setups.

Data leaks & dark web
Breach data, leaked credentials, mentions in underground sources.

Email & phishing risk
SPF, DKIM, DMARC, open relays, email security posture.

Technology & infrastructure
Tech stack detection, CDN/WAF, cloud exposure, cloud metadata (e.g. IMDSv2).

Malware & threat intelligence
Active malware, C2 infrastructure, IOC matches, ransomware connections.

Compliance insights
NIS2, DORA, GDPR and more — mapped to real findings.

TURN DATA INTO ACTION

Risk scoring
Clear, prioritized risk scores for every target.

Actionable insights
Evidence-based findings with remediation guidance.

Beautiful reports
Shareable PDF reports for clients, teams or vendors.

Continuous monitoring
Track changes and get alerted when new risks emerge.

Supplier risk screening
Assess third-party and supply chain exposure.

Built for scale
From tens to 50,000+ companies — fast and reliable.

WHY PENTESTERRA

REAL EXPOSURE
Not just theoretical risk — we show what's actually reachable and exploitable.

ALL-IN-ONE
Combines external exposure, threat intel, compliance and supplier risk in one platform.

BUILT FOR PROFESSIONALS
Designed by security experts for real-world use, not checkbox compliance.

MORE VALUE
Faster, deeper and more actionable than traditional ratings or passive tools.

A CLEARER VIEW.
A SAFER TOMORROW.

START ASSESSING →

EXPOSE
UNDERSTAND
MITIGATE
GROW

Know If a Company Is Already Compromised

Import a whole sector, supplier book, or country and triage every company in seconds to minutes each - exposure, compromise indicators, threat-actor interest, a compliance baseline, and OSINT, aggregated from every Pentesterra module that has evidence on it.

50,000+
Companies importable and triaged in a single batch

Agentless
Nothing installed on your - or your suppliers' - infrastructure

24/7
Automatic recheck when the threat-intel KB updates

WHY NOW

A supplier just made headlines, or a customer is asking for evidence before they'll sign. Without visibility into what's actually exposed, one overlooked subdomain or leaked credential can become a ransomware entry point - and by the time it shows up in the news, triage is too late.

HOW IT WORKS

Bulk Triage, Not One Domain at a Time

Import 50,000+ companies in one pass - a whole sector, supplier book, or country. Each one is checked in seconds to a few minutes, not the days a manual review or a full pentest would take.

- → Bulk CSV import, batch scanning at real scale, no artificial per-request cap
- → Per company: exposure, compromise, compliance, OSINT - one pass
- → Filter thousands down to "high risk", "not yet scanned", "confirmed compromise"
- → Progress tracked server-side, visible and cancellable from any session

Compromise & Threat-Actor-Interest Signals

Beyond "is a port open" - is this company already compromised, or actively interesting to attackers right now. Every tracked target is cross-checked against a continuously updated threat-intel KB, not a one-time lookup.

- → Open mail relay, phishing susceptibility, known-malware / C2 indicators
- → Employee credential and session exposure pulled from infostealer logs
- → Ransomware leak-site and breach-news correlation, human-verified before it's shown as confirmed
- → Darknet / criminal-forum mention signal - is this company being discussed or actively targeted right now

One Company, Every Module's Evidence

A company can have several domains, IP ranges, and CIDR blocks, and evidence about it can come from anywhere in the platform - External Exposure Assessments pulls it together under one record.

- → Per-module coverage shown explicitly: assessed, not yet assessed, never silently blank
- → Drill straight through from a company summary to the underlying module's own evidence
- → Web Pentest and Vulnerability Management findings feed the company's exposure score
- → OSINT, DevGuard, Phishing Simulation results all roll into the same record

Attack Surface, Checked the Passive Way

Domains and services are checked against common attack classes using passive and semi-passive methods - no active exploitation, no port-scanning noise on infrastructure you don't operate.

- → DNS/email hygiene, TLS, security headers, cookies, WAF/CDN/cloud fingerprinting
- → Opt-in safe-active checks (VPN/firewall portal exposure, open-relay test) - never on by default
- → Same engine covers your own domains and your suppliers' or prospects'
- → Explicit about what a passive check cannot see - never implies broader coverage than it has

Compliance Baseline From Real Evidence

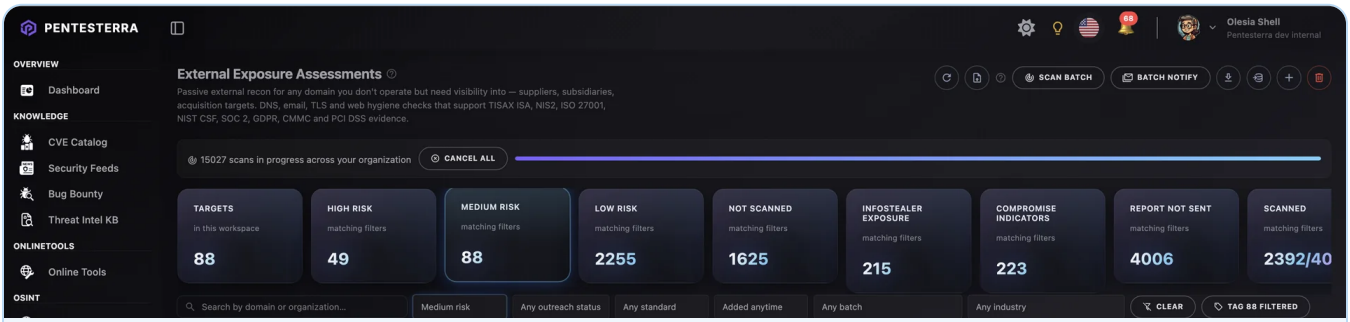
A baseline compliance read generated from what was actually found - not a self-attested questionnaire. One-click evidence reports for the frameworks that matter.

- → NIS2, DORA, GDPR, ISO 27001, NIST CSF, SOC 2, CMMC, PCI DSS, TISAX ISA coverage
- → One-click per-supplier PDF evidence pack, built for the auditor's actual question
- → Coverage percentage shown honestly - a compliance signal, not a certification
- → Never a legal conclusion from country/industry alone - always overridable

Continuous Monitoring, Not a Point-in-Time Report

A scan result is a snapshot; a threat feed keeps moving. Every tracked company is automatically re-checked the moment the knowledge base updates - not just when someone remembers to re-run a scan.

- → Automatic backfill against every already-tracked company on every feed update
- → Notification the instant a new compromise indicator matches a tracked company
- → Batch outreach notices with per-recipient open/click tracking
- → A whole country or sector analyzed and notified within hours, not weeks



Every tracked company by risk tier, coverage, and compromise indicators - with a live, organization-wide view of scans in progress.

PENTESTERRA VS. MANUAL VENDOR REVIEW

DIMENSION	MANUAL / QUESTIONNAIRE-BASED	PENTESTERRA
Scale	One vendor questionnaire at a time	50,000+ companies, seconds to minutes each
Discovery scope	One domain you already know about	Full domain/IP/CIDR footprint, cross-module evidence included
Compromise detection	Manual OSINT / vendor questionnaires	Continuous cross-reference against a live threat-intel KB
Breach signal	Found by chance, months later	Ransomware leak-site + breach-news correlation, flagged for review
Freshness	Re-checked only at renewal / annual review	Auto-rechecked the moment the KB updates
Cross-module view	Every finding lives in a separate tool/ report	One company record aggregates OSINT, DevGuard, VM, Pentest, Phishing
Authorization needed	Scanning/pentest sign-off before you can start	Passive/semi-passive - no authorization required to begin
Footprint	Your domains only	Your domains, your suppliers', your prospects' - same workflow

STATED PLAINLY

If a target only exposes a domain behind NAT, a proxy, or a CDN, an infected host inside that organization's internal network is invisible to any external scan. This is a fast, mostly passive external-exposure check, not a substitute for an internal network assessment.

Triage your first 100 companies

Point Pentesterra at a supplier list, a sector, or your own domain footprint.

info@pentesterra.com
pentesterra.com/external-exposure-assessments