Third-Party / Supply Chain Exposure Assessment

Objective, evidence-based external risk scoring — no questionnaires, no self-reported answers, no cooperation required from the third party.

What it checks

- **External attack surface mapping — domains, resolved IPs, and IP/CIDR ranges.**
  - *Reveals what a vendor truly exposes to the internet, not just what they claim.*
- **TLS / certificate configuration analysis.**
  - *Flags weak encryption, expired certificates, and misconfigurations before they become a breach vector.*
- **DNS and email authentication hygiene (SPF / DMARC).**
  - *Measures how easily a supplier could be abused for phishing impersonation.*
- **HTTP security headers and cookie security analysis.**
  - *Produces an objective, machine-verifiable hardening score instead of a subjective checklist.*
- **WAF / CDN / cloud provider fingerprinting.**
  - *Verifies real protective controls are actually in place.*
- **Open mail-relay probing.**
  - *Detects whether infrastructure can be abused to send phishing or spam.*
- **Continuous threat-intel correlation — botnet / C2 infection, malicious TLS certificates, IP reputation blocklists.**
  - *Detects active compromise indicators, not just static weaknesses.*
- **Ransomware leak-site monitoring.**
  - *Surfaces signs that a supplier has already been breached, even before it becomes public.*
- **Persistent Knowledge Base, updated continuously.**
  - *Every previously assessed company is automatically re-checked against refreshed threat feeds, so you get alerted if a vendor becomes compromised later.*
- **Compliance-mapped findings (NIST CSF).**
  - *Results map directly into existing risk and compliance reporting.*

Key takeaway

Not a one-time snapshot or self-attestation form — *continuous, independently verifiable, evidence-backed monitoring of your supply chain's external exposure, including breach and dark-web signals, updated as new threats emerge.*

Objective. No questionnaires. No self-reporting.

Independently Verifiable Evidence from the open internet.

Continuous Monitoring Re-checks 24/7 as threats evolve.

Early Warning Detects exposure and breaches early.

Actionable Insights Risk scores aligned to *NIST CSF.*

PENTESTERRA

SUPPLY CHAIN EXPOSURE

Vendor Risk, Scored Without a Questionnaire

Objective, evidence-based external risk scoring for third parties and suppliers - no questionnaires, no self-reported answers, no cooperation required from the vendor. Built on the same engine as External Exposure Assessments, scoped to your supply chain.

0
Questionnaires sent - every signal is externally observed

24/7
Continuous re-checking as threat feeds update

NIST CSF+
Findings mapped to existing risk and compliance reporting

WHY NOW

A vendor questionnaire just came back clean - but questionnaires are self-reported. One compromised supplier with no direct network connection can still cost you the breach: shared credentials, shared SaaS access, a single infected laptop. Your last vendor incident probably didn't start with a "no" answer.

SIX LAYERS OF EVIDENCE

1. Attack Surface Mapping

Domains, resolved IPs, and IP/CIDR ranges - reveals what a vendor truly exposes to the internet, not just what they claim in a self-reported form.

- → Full domain and subdomain enumeration
- → Resolved IP and CIDR-range discovery
- → Cloud provider and hosting fingerprinting

2. TLS & DNS Hygiene

Certificate configuration analysis and DNS/email authentication (SPF/DMARC) - flags weak encryption and phishing-impersonation risk before they become a breach vector.

- → Weak encryption and expired-certificate detection
- → SPF / DKIM / DMARC posture
- → Open mail-relay probing

3. Web & Email Security

HTTP security headers, cookie analysis, and WAF/CDN/cloud fingerprinting produce an objective, machine-verifiable hardening score instead of a subjective checklist a vendor fills in themselves.

- → Security header and cookie configuration checks
- → WAF / CDN presence verification
- → Whether real protective controls are actually in place

4. Darknet & Threat-Actor Monitoring

The same continuously updated threat-intel KB used for your own domains is run against every tracked vendor - is this supplier already compromised, or being discussed by threat actors right now.

- → Darknet / criminal-forum mention signal per vendor
- → Known-malware and C2 infrastructure correlation
- → Ransomware leak-site and breach-news correlation, human-verified before flagged as confirmed

5. Continuous Monitoring, Not a One-Time Check

Vendor risk doesn't freeze the day you onboard a supplier. Once a company is added, its domains and IP ranges are automatically checked against every threat-feed update from that point forward - no one has to remember to re-run the scan.

- → Automatic backfill against every tracked vendor on every feed update
- → Notification the instant a new compromise indicator matches a tracked vendor
- → Re-checked on the same schedule as your own domains, not a slower vendor-only cadence

6. Compliance Mapping

Findings map directly into existing risk and compliance reporting, so vendor risk isn't a separate spreadsheet nobody looks at.

- → NIST CSF-aligned finding categories out of the box
- → Reuses the same evidence base as your own compliance assessments
- → One-click evidence export per vendor

KEY TAKEAWAY

Not a one-time snapshot or self-attestation form - continuous, independently verifiable, evidence-backed monitoring of your supply chain's external exposure, including breach and dark-web signals, updated automatically as new threats emerge.

WHAT IT CHECKS, AT A GLANCE

CHECK	WHAT IT REVEALS
External attack surface mapping	What a vendor truly exposes to the internet
TLS / certificate configuration	Weak encryption, expired certificates, misconfigurations
DNS and email authentication	How easily a supplier could be abused for phishing impersonation
Open mail-relay probing	Whether infrastructure can be abused to send phishing or spam
Darknet / criminal-forum monitoring	Whether this vendor is being discussed or targeted right now
Malware / C2 correlation	Active infection or compromise indicators, not just static weaknesses
Ransomware leak-site monitoring	Signs a supplier has already been breached, before it becomes public
Continuous re-check	Every tracked vendor re-scanned automatically on every feed update

Screen your first supplier list

No cooperation required from the vendor - start from a domain or company name.

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