PENTESTERRA

SUPPLY CHAIN EXPOSURE

Are Your Suppliers Already Compromised?

Vendor risk scored without questionnaires - externally observed evidence, not self-attestation. Same engine as External Exposure Assessment, scoped to your supply chain.

IN SHORT

Objective, evidence-based risk scoring for vendors and third parties - 6 layers of externally observed signals, from attack surface to criminal-forum presence - no questionnaires, no cooperation required from the vendor.

0
Questionnaires sent - every signal is externally observed

24/7
Continuous re-checking as threat feeds update

NIST CSF+
Findings mapped to your existing risk and compliance reporting

THE SITUATION TODAY

WHO YOU ARE

You're the vendor risk, procurement, or security lead of an organization that needs to assess supplier and third-party exposure without relying on self-reported questionnaires.

WHAT HAPPENED

A vendor questionnaire just came back clean - but questionnaires are self-reported. A compromised supplier with no direct network connection can still cost you the breach: shared credentials, shared SaaS access, a single infected laptop.

WHY IT HURTS

Your last vendor incident probably didn't start with a 'no' answer on a questionnaire - questionnaires measure stated intentions, not real exposure.

WHERE YOU WANT TO GET TO

DESIRED OUTCOME

You want to know, with objective evidence, which vendors are actually exposed or already compromised - not just which ones answered a questionnaire well.

THE SOLUTION

A Supply Chain Exposure Assessment service: 6 layers of externally observed evidence - attack surface, TLS/DNS hygiene, web/email security, darknet monitoring, continuous monitoring, compliance mapping - no cooperation required from the vendor.

WHY IT'S DIFFERENT

You're not buying another vendor questionnaire to send out. You're working with [YOUR COMPANY NAME] - a certified provider with a long track record in information security. You've likely worked with us already, directly or through someone you know. And every tracked vendor is automatically re-checked on every threat-intel update - not just when someone remembers to resend a questionnaire. The same evidence base is reused across your compliance assessments.

CONCRETE PROOF

The result is a complete, ready-to-deliver PDF report with every vendor's exposure documented across 6 layers of evidence. If gaps come up, we propose additional services: external exposure assessment, vulnerability assessment, penetration testing.

6 Layers

Surface, TLS/DNS, web/email, darknet, monitoring, compliance

No Cooperation Needed

The vendor doesn't have to do anything

Scale

From a single vendor to a whole portfolio

WHAT'S ACTUALLY INCLUDED

6 layers of externally observed evidence - not a questionnaire to send the vendor.

Attack Surface Mapping

Domains, resolved IPs, CIDR ranges - reveals what a vendor truly exposes to the internet, not just what they claim.

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

TLS/DNS Hygiene and Web/Email Security

Certificate configuration, DNS/email authentication, security headers, WAF/CDN fingerprinting.

- Weak encryption and expired-certificate detection
- SPF/DKIM/DMARC posture
- Open mail-relay probing
- WAF/CDN presence verification

Darknet and Threat-Actor Monitoring

The same continuously updated threat-intel base used for your own domains, run against every tracked vendor.

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

Continuous Monitoring and Compliance Mapping

Vendor risk doesn't freeze the day you onboard a supplier.

- Automatic re-check of every vendor on every feed update
- Instant notification on a new compromise indicator
- Finding categories aligned to NIST CSF
- One-click evidence export per vendor

PENTESTERRA

SUPPLY CHAIN EXPOSURE

WHAT YOU GET

- ✓ A complete PDF report with every vendor's exposure across 6 layers of evidence
- ✓ External attack surface mapping for every vendor
- ✓ Correlation with ransomware leak-sites, breach news, and criminal forums
- ✓ Finding categories mapped to NIST CSF
- ✓ Continuous monitoring with alerts on new compromise indicators

HOW IT WORKS

1

We upload the vendor list

A single vendor or a whole portfolio - no cooperation required.

2

We collect the evidence

6 layers of externally observed signals, automatically.

3

We verify the signals

Every compromise indicator is confirmed by an analyst.

4

We deliver the report

A complete PDF with risks prioritized per vendor.

Find out which vendors are already exposed or compromised

A complete report, ready to present to clients, auditors, or your board.

Request your Supply Chain Exposure Assessment →

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