

TPRM



Third-Party Risk Management

Cyber intelligence for supplier risk and dependencies

Assess supplier exposure, map observable fourth-party dependencies and prioritize portfolio risk through technical evidence and collaborative remediation.



Suppliers, service providers, fourth parties and shared digital dependencies



Independent assessment

Assess suppliers near real time from available intelligence, without initial supplier participation.



Dependency visibility

Review observable fourth parties and shared-provider concentration across your portfolio.



Collaborative remediation

Invite suppliers to review findings. Add questionnaires and coordinate risk reduction.

Evidence for supplier-risk compliance

NIS2, DORA and other international regulations require covered organizations to assess and monitor cyber risk across their supplier ecosystem. Coinnect TPRM supports these requirements with independent intelligence assessments, ongoing monitoring and technical evidence for supplier due diligence, risk prioritization and remediation. This evidence complements the wider governance, controls and contractual measures required for compliance.

Technical capabilities

Connect supplier exposure to observable dependencies and remediation status. Review the technical findings behind portfolio risk scores and priorities.

Supplier exposure evidence

Domains, IPs, exposed services and observed technologies for each supplier. Review asset-linked CVE context, configuration indicators and exposed-data signals.

Portfolio risk prioritization

Compare supplier risk scores with the affected-asset evidence behind them. Review criticality and shared-provider concentration to focus oversight where it matters.

Questionnaires & campaigns

Complement intelligence with supplier questionnaires and compliance campaigns. Review responses alongside technical evidence during due diligence.

Fourth-party dependencies

Identify observable cloud, hosting and IT providers used by suppliers. Map shared dependencies to reveal technology and provider concentration across the ecosystem.

Monitoring & breach signals

Track exposure changes, exposed credentials and breach or ransomware intelligence. Use alerts and portfolio reports to support ongoing supplier oversight.

Collaborative remediation

Invite suppliers to review findings and provide context. Coordinate remediation and track improvements through the workflow and available technical evidence.

Optional EASM module

External Attack Surface Management

Add EASM to monitor your own organization alongside supplier risk. Review external assets, observed technologies and asset-linked exposure indicators through the same intelligence approach.

Organization exposure

Discover domains, IPs and cloud-facing services. Inspect CVE context and exposed-data signals linked to the organization's assets.

Shared security priorities

Use risk scores, AI-assisted explanations and alerts to coordinate review. Follow exposure changes and support remediation across organization and supplier views.

