ThreatNG empowers your organization to quickly uncover, manage, and monitor third-party risks to fulfill due diligence, onboarding, and offboarding requirements for Third Party Risk Management (TPRM). **Enter a third party's domain name into our platform to discover, assess, report, and monitor their risks.**

Identify and **Evaluate** all parties, products, and services involved: Vendors, Partners, Contractors, & Consultants.

Assess Risk based on all externally available Technical, Strategic, Operational, and Financial data.

Address Risks and **Create Controls** to facilitate informed Procurement and Documentation of relationships.

Continuously Monitor all parties throughout the entire relationship life-cycle from start to finish.

Discover, Identify, Evaluate, and Assess Third Parties, Nth Parties, Products & Services

Discover & Identify

Discover and Identify all Parties in your digital ecosystem (Your Organization, Third Parties, Nth Parties) and Interconnected Technologies: Cloud Resources & Environments, SaaS, PaaS, IaaS, APIs, and more.

Evaluate & Assess

Evaluate and Assess all parties for ethical, reputational, and cybersecurity risks they may pose to your organization.

- ❑ ESG (Environment, Social, and Governance) Indicators
- ❑ Undesired Strategic, Operational, and Financial Exposures
- ❑ Susceptibility to Cybersecurity Threats

Report & Review Third-Party Risk

Risk from All Angles

Obtain an in-depth and holistic way to view yourself and your Third Parties.

Cyber Risk

Security industry best practices External Attack Surface and Digital Footprint risk assessment rating.

Susceptibility & Exposures

Gauge the susceptibility and exposure to Phishing, Ransomware, Application Hijacking, Subdomain Takeover, Data Leaks, and Brand Damage.

Communicate & Understand at All Levels

Executive and Detailed Technical Reporting

Across all the following areas of assessment:

- ❑ Domain Intelligence
- ❑ Cloud & SaaS Exposure
- ❑ Sensitive Code Exposure
- ❑ Online Sharing Exposure
- ❑ Sentiment & Financials Indicators
- ❑ Web Archives
- ❑ Search Engine Exploitation
- ❑ Dark Web Presence
- ❑ Social Media Presence

Verify Third-Party Risk

Engage Stakeholders & Verify Findings

Investigate and verify findings through dynamically generated results-driven questionnaires. Fueled by ThreatNG's Correlation Evidence Questionnaire (CEQ), a customized questionnaire is generated to facilitate effective and time-saving third-party risk assessments. The CEQ provides questions in the context of impacted functional assets and pillars (Technical, Strategic, Operational, and Financial) to facilitate seamless communication and collaboration across departmental silos.

Address Risks & Create Controls

Team Visibility & Empowerment

Provide visibility to all critical stakeholders for effective delegation of remediation efforts through the platform's role-based access controls and integrations.

Holistic Approach Fuels Effective Policy Development

Create Risk Policies, Controls, and Appetite through informed Ratings (Cybersecurity, Exposure, and ESG), Detailed Assessment Areas, and further bolstered by the ThreatNG Correlation Evidence Questionnaire (CEQ) Results. All ratings and findings are substantiated and explained through the continuously updated ThreatNG Knowledgebase containing detailed descriptions, risk-level assignments, reasoning, recommendation, and external references.

Continuous Monitoring from Start to Finish

Configurable ongoing discovery sweeps, analysis, and reporting to stay on top of changes and developments throughout the defined ecosystem.

Continuously Monitor

❑ Deviations from Baseline Policies and Risk Appetite
❑ Changes in ESG Indicators
❑ Risk and Exposure Levels
❑ Changes in Digital Presence and Interconnected Technologies

Confidently Offboard Third-Parties from Your Digital Presence

Confirm the severance of a party relationship throughout your entire technology footprint, digital presence, and third/nth party ecosystem through initial and ongoing discovery sweeps, analysis, and reporting.

About ThreatNG

ThreatNG is redefining digital risk protection and external attack surface management with a platform of unmatched breadth, depth, and capabilities in managing technical and business threats across the dark, deep, and open web. Living up to the company mantra ("Security Centric; Not Security Exclusive"), ThreatNG provides a configurable solution to target, discover, and assess digital assets across a definable ecosystem of organizations, subsidiaries, partners, third parties, supply chain, and customers. Bolstered and maintained by the open source intelligence (OSINT) experts at DarcSight Labs, ThreatNG empowers organizations of all types and sizes to uncover, understand, and manage their external digital threats