DIGITAL RISK AND THREAT MANAGEMENT

THREAT NG

Discover, Assess, Report, and Manage Threats Beyond the Perimeter

Manage Threats that Affect Your World Throughout the Open, Deep, and Dark Web

ThreatNG uncovers threats beyond the perimeter that exist across the open, deep, and dark web. The platform harvests, analyzes, and reports on Technical (Domain Information, Public Cloud Infrastructure, Certificates), Financial/Administrative (SEC Filings, Funding Rounds, Financial Reports, Lawsuits), Personnel (Sentiment, Layoffs, Social Media), and presence on the Dark Web. A comprehensive approach that provides a holistic and complete view of an organization's external technical and business attack surface.

DISCOVER AND INVENTORY

- Execute targeted Open, Deep, Dark Web data collection to bring to light all facets of your online Technical and Business Digital Footprint.
- Discover and refresh any time (all the time) the status of your:
  - Domains, Subdomains, Certificates, Publicly Available Email Addresses, Domain Name Permutations, and DNS Servers/Records.
  - Cloud Infrastructure (Amazon AWS, Microsoft Azure, and Google GCP) and Software
  - Public Code, Text Sharing Repositories, Technologies Implemented, and Website Archives Associated with Your Digital Footprint
  - Alternative Organization Names, Private Company Funding Information, Public Company Filings, Company/Layoff/News Chatter, and Lawsuits
  - Social Media Presence
  - Dark Web Mentions of Key People, Places, and Things (products, services, and brands)

ASSESS, EXAMINE, AND HIGHLIGHT

- On-demand, configurable, and thorough digital presence threat and risk assessment of your external Application/IT infrastructure (Technical Attack Surface) and public organizational data (Business Attack Surface). View your organization, subsidiaries, partners, and all entities in your ecosystem through a "real-world" adversarial "outside-in" perspective as ThreatNG uncovers and highlights:
  - Internet infrastructure issues, inconsistencies, and misconfigurations that impact business strategy, operations, and financials.
  - Rogue, unsanctioned, look-alike cloud resources and their contents that are open to the public.
  - Sensitive information within public code and text sharing repositories.
  - Technologies, applications, services, confidential/proprietary/sensitive data, and IoT entities uncovered by search engine queries (aka dorks).
  - Public strategic, operational, and financial issues, anomalies, non-compliant behavior.
  - Social media content for oversharing and exposures.
  - Archived web pages for sensitive information, Javascript endpoints, potential redirects, subdomains, and any misconfigurations that can be exploited by adversaries.

BENEFITS

IDENTIFY Internet-facing assets providing instant awareness of threats and risks across your external attack surface.

EXTEND threat, risk, and vulnerability management efforts beyond the perimeter, across disciplines, and into the open, deep, and dark web.

VALIDATE security controls and measures from the outside-in.

PROVIDE an adversarial view of your organizations, subsidiaries, partners, and third parties.

AUTOMATE the documentation of your external business (strategic, operational, & financial) and technical environment.

EDUCATE through guidance and explanations of digital presence, risk, and external attack surface concepts.

ELIMINATE Intelligence Silos. The platform serves as a "single source of the truth" of external assets that transcends functional silos and facilitates best security practices across your entire organization making "security everyone's job".

SAVE Time, Money, and Resources through the configurable asset discovery facility providing immediate and relevant information.

FACILITATE confidence with new initiatives, partnerships, vendor relationships, and acquiring new customers through knowing how secure everyone is from the outside-in.

HELP achieve compliance with applicable International, Government, Regulatory, and Industry Requirements.

DIGITAL RISK AND THREAT MANAGEMENT

CONTINUOUS VISIBILITY

- Configurable ongoing discovery sweeps, analysis, and reporting to stay on top of changes and developments throughout your:
  - Ecosystem of Organizations, Partners, Third Parties, and Supply Chain
  - Domains, Subdomains, and Certificates
  - Cloud Implementations
  - Public Code and Text Sharing Repositories
  - Technology Stack
  - Sentiment and Financial News
  - Social Media Presence
  - Dark Web Mentions
  - Website Archives and Contents
  - Search Engine Revelatory Information, Data, Infrastructure, and Resources
- Live Social Media, Domain Search Activity, and Security Industry News Feeds
- Intelligence Repositories (DarCache - Data Aggregation Reconnaissance Cache)
  - Continually updated, indexed, and vetted subject-specific data warehouses. Facilitate investigations through an easy-to-use "search engin-like" interfaceproviding instantaneous and relevant results.

REPORT AND SHARE

- Immediate digital risk and external attack surface "state of affairs" with data...
  - Available in adaptable form factors (PDF and CSV);
  - Presented with configurable levels of detail (Executive, Summary, Detailed, Delta); and
  - Sharable with existing IT infrastructure and enterprise management solutions through the ThreatNG API, Documentation, and Guide.

COLLABORATE AND MANAGE

- Engage and cooperate with team members to address and "close the loop" on external digital threats.
  - Correlation Evidence Questionnaire
    - Dynamically generated evidence-based questions to facilitate cross-functional (Technical, Strategic, Operational, and Financial) collaboration and management of external threats and risks. Each question is substantiated with discovery and assessment results.
  - Role-Based Access
    - Provide team members with privileges to platform capabilities to understand and manage findings.

DIGITAL RISK AND THREAT MANAGEMENT

EXTERNAL ATTACK SURFACE MANAGEMENT

Identify assets that are connected or exposed to the Internet and assess if adversaries can use them against you.

THIRD-PARTY RISK ASSESSMENT

Alignment of external assessment methodologies with third parties.

DUE DILIGENCE, ON-BOARDING, AND INTEGRATION

Perform practical, continuous, and consistent external assessments throughout all stages of the relationship lifecycle.

ONLINE SENTIMENT AND FINANCIAL MONITORING

Uncover potential risks, leaks, and exposures in public financial documentation, mentions, and chatter.

BRAND AND REPUTATION MONITORING

Inventory and analysis of all sanctioned, unsanctioned, and lookalike, and impostor brand appearances.

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.