Partnership Brief

Intelligence and Legal Partnerships

Managed intelligence and investigations in support of legal counsel

Nisos enables counsel to differentiate themselves through engagement with world-class investigation and intelligence experts.

Addressing clients' and partners' existing and emergent threats, we provide an unparalleled ability to investigate and draw context from data collected outside an organization's perimeter.

We regularly partner with law firms and inside enterprise counsel to address security concerns related to supply chain, third-party, M&A, investment risks, brand reputation, disinformation, data, systems, networks, trust and safety, and executives.

Transform Your Practice

Legal counsel from all practice areas want to retain and grow their practices and capabilities. A key factor in meeting that objective is having world-class experts assist them in mitigating risk for their clients. Having experts on hand to inform investigations, or to round out a client's security team, can make the difference between a fair result or a transformative result.

Nisos can help counsel arrive at results that surpass in-house capabilities, including: trade secret theft, intellectual property and brand reputation protection, regulatory compliance, key personnel and employee issues, insider threat, third party risk, and M&A due diligence.

Our Differentiated Approach

Nisos extracts and enriches client-specific data from our vast proprietary multi-source collection capabilities. Our process gives us unrivaled visibility into adversaries, deeper insights into threats, and allows the attribution and unmasking of adversaries **even if they aren't known actors that are using previously connected tactics, techniques, and procedures (TTPs).**

Multi-Source Core Capabilities Across All Solutions

Open Source Intelligence Research

Global coverage of surface, deep, and dark web sources using bespoke data collection and tools. We maintain significant coverage on most open and closed source social media platforms, and legally collect and aggregate many data breach and personally identifiable information (PII) datasets released on these platforms to conduct more detailed alerting and attribution.

Technical Signature Analysis

Adversarial-minded investigation of raw technical data, including off-network connection and context for on-network telemetry.

Threat Actor Engagement

Proprietary mis-attributable aged personas and infrastructure to engage in native language interaction on social media, open, and dark web forums.

Context for On-Network Telemetry, If Necessary

We conduct external threat hunting and forensics investigations on a variety of security events and incidents up to the point they become a breach. By combining our core capabilities with on-network forensics investigations, we bring actionable context, resolution, and remediation to security events both within and outside of a company's perimeter before a breach occurs.

Our Solutions
in Context for Counsel

Adversary Research and Attribution

Technical and analytic techniques within social media, breach data, recovered PII, and the dark web brings context behind the "who," "why," and "how" behind an attacker or threat. Use cases such as insider threat often involve attribution after monitoring and alerting efforts from investigations utilizing other services.

Our experts' abilities to draw conclusions and provide evidence can often extend counsel's ability to seek recourse from adversaries, whether through litigation or prosecution.

CASE STUDY >>

Outside Intel to Cyber Threats

External threat hunting for threats against the confidentiality, integrity, and availability of data, systems, and networks with the ability to conduct forensics investigations before a breach occurs.

CASE STUDY >>

Trust & Safety

Investigations and intelligence into fraud, abuse, and disinformation threats on platforms and marketplaces that derail consumer confidence.

CASE STUDY >>

Brand Reputation & Disinformation

Monitoring and reaction to negative sentiment or disinformation against a brand's products, assets, and employees.

CASE STUDY >>

Third-Party Risk and M&A Diligence

Investigations in support of diligence for third-party risk teams and M&A deal teams, including cyber maturity assessments, integration concerns, key man risk, and potential trade secret litigation.

CASE STUDY >>

Executive Protection

Combats threats to executive leadership, including the assessment of digital information that could be used to attack an executive, removal of PII, direct threat actor engagement, and attribution if necessary.

CASE STUDY >>