



Service Brief

Managed Intelligence™ Suite

Let Nisos be your threat intelligence partner.

For enterprise security teams with tight budgets, limited time, and expertise in short supply, Nisos fills a crucial gap by combining people, processes, and technology to deliver threat intelligence as a managed service.

The Nisos Managed Intelligence™ Suite allows security teams to offload complex threat intelligence efforts to an expert analyst team focused on your needs. Nisos analysts have the tools and experience to efficiently reveal critical open source intelligence from the surface, deep, and dark web to identify threats in your security shadows.

A Partner Focused on Your Intelligence Needs

Working as an extension of your team, Nisos provides intelligence focused on real-world threats specific to your organization. With Nisos as a partner, you can be confident in your ability to respond to advanced threats, even as your team evolves. You benefit from our broad experience and extensive toolset, so you'll always have the resources to fill knowledge gaps and address unique stakeholders' needs. Nisos analysts work with your team to respond to Requests for Information (RFIs) on your most pressing concerns and support ongoing security operations with monitoring and alerts.

Unmatched Open Source Collection Capabilities

Nisos gives security teams deeper, broader, and more comprehensive threat intelligence coverage. Using an extensive stack of third-party and proprietary tools, Nisos collects and maintains a vast collection of content to query for mentions related to your organization, its brand, key personnel, or assets.

Accelerated Analysis with the Nisos Intelligence Platform

Nisos analysts perform intelligence collection, correlation, analysis, and production using the Nisos Intelligence Platform. This secure internal platform gives analysts centralized access to data from over 30 licensed and curated intelligence feeds and collection tools.

The Nisos Intelligence Platform also enables Nisos analysts to rapidly query our vast and ever-growing proprietary database of over 20 billion lawfully-obtained records from breach compilations and dark web forums.

Threat Landscape Assessment

Comprehensive baseline assessment of your organization's threat profile

Managed OSINT Monitoring

External threat monitoring, investigation, and critical threat alerting

Adversary Insights® Investigations

Analyst expertise to identify and investigate risks and counter adversary threats

Executive Shield Digital

Digital risk assessment, monitoring, plus PII identification and removal

Nisos Managed Intelligence™ Suite

The Managed Intelligence Suite delivers comprehensive threat assessments, OSINT monitoring, digital executive protection, topical intel reports, and investigation support that helps your team stay ahead of threats. Nisos identifies security trends and equips stakeholders with the right intelligence at the right time. The Managed Intelligence Suite includes:

- **Threat Landscape Assessment**
 - One annual assessment
- **Adversary Insights® Investigation Suite**
 - Requested RFIs
 - Pre-scheduled intelligence reports
- **Managed OSINT Monitoring Suite**
 - Managed Surface & Deep Web Monitoring
 - Managed Dark Web Monitoring
 - Managed Technical Monitoring
- **Executive Shield Digital**
 - One individual

Threat Landscape Assessment

A Nisos Threat Landscape Assessment is an annual investigation that provides deep, finished intelligence on the digital and physical threats facing your organization, brand, or product. Threat Landscape Assessments provide unparalleled visibility beyond the perimeter. This includes critical insights into your security posture to help set intelligence priorities, identify collection strategies, track mitigation activities, and reduce risk.

Nisos assessments are uniquely comprehensive, addressing cyber and physical risks, including breaches and data leaks, technical indicators, vulnerabilities, disinformation, threats against people and assets, and more.

Key Use Cases:

- Assessment of external network hygiene, including asset discovery, potential undocumented public IP spaces, misconfigurations, and indicators of compromise.
- Analysis of the non-traditional business risk of the target organization, including potential suspicious financial activity, intellectual property theft, criminal activity, and threats of physical harm.
- Baseline for hunting active and latent threats and correlating findings across client requests, expert hypotheses, and landscape threat patterns.

Adversary Insights® | Managed Investigations

Managed Investigations provide timely, finished intelligence that addresses security threats by responding to client Requests for Information (RFIs). RFIs allow you to create tasks for Nisos to investigate specific threats relevant to your organization that use our curated toolset and an extensive, proprietary collection of breach data. There are two concurrent RFI workstreams:

Requested RFIs

- Spotlight Investigation: for quick-turnaround investigations into an urgent threat, or
- Targeted Investigation: for a detailed look at an emerging threat.

Pre-scheduled Intelligence Reports

- Choose up to four pre-scheduled Intelligence Reports delivered quarterly or monthly. Additional workstreams are available for purchase.

Intelligence Report Options Include:

Quarterly	Monthly	
Industry Landscape	Code Leaks	CVE Summary
Geographic Landscape	Compromised Account Credentials	Threat Actor Network Access
	Deep & Dark Web Mentions	Anomalous Network Traffic
	Tailored News Summary	3rd Party Focused Assessment

Managed OSINT Monitoring

Managed OSINT Monitoring delivers critical intelligence that helps you cut through the noise, identify critical threats to their organization, and respond confidently.

Managed Monitoring tracks social media content, dark web chatter, and technical indicators for signs of risk as part of the Managed Intelligence Suite. Your named Nisos analysts will analyze threats daily to determine credibility and urgency, alerting you to all threats that require immediate action.

Managed OSINT Monitoring, Continued

The Managed OSINT Monitoring Suite includes:

- **Surface and Deep Web Monitoring**

Targeted, systematic identification and monitoring of client-specific indications and warnings across social media, surface, and deep web.

- **Dark Web Monitoring**

External threat monitoring, investigation, and critical threat alerting for risks found in numerous dark forums, including but not limited to xss[.]is, raidforums[.]com, exploit[.]in, nulled[.]to, and hackforums[.]net.

- **Technical Monitoring**

Monitoring for purely technical use cases, including domain and typosquatting, using Grayhat Warfare, Shodan, BE, and more.

Executive Shield Digital

For clients who need greater visibility into threats against key personnel, Nisos Executive Shield Digital is a Managed Intelligence offering that provides comprehensive, analyst-led assessments and ongoing monitoring of an individual's digital risk profile.

Nisos' skilled analysts track and identify threat actors targeting your people across the open web, social and foreign media, the deep web, and dark web forums.

Executive Shield Digital delivers tailored intelligence distilled to drive clarity and action. The service includes:

- **An annual digital exposure assessment**
- **Ongoing monitoring of a select individual**
- **Quarterly Personally Identifiable Information (PII) reduction**

About Nisos®

Nisos is The Managed Intelligence Company™. Our customized, scalable services enable cybersecurity, corporate security, intelligence, and trust & safety teams to leverage a world-class intelligence capability tailored to their needs. We fuse robust data collection with a deep understanding of the adversarial mindset delivering smarter defense and more effective responses against advanced cyber attacks, disinformation, and abuse of digital platforms.

For more information: visit: www.nisos.com email: info@nisos.com call: +1-703-382-8400
follow: [LinkedIn](#), [Twitter](#), [Facebook](#), [Instagram](#)