NISOS

Service Brief

Adversary Insights® Investigations Suite

Elevate your security program with answers to your intelligence questions and custom risk reporting.

Organizations face escalating threats, disgruntled insiders, financially motivated hackers, cyber-criminal gangs, state-sponsored actors, and even corporate espionage firms. Intentional and malicious disclosures occur daily.

Security teams are charged with the monumental task of finding, fixing, and reducing the impact of these threats on the organization's brand, personnel, and assets.

Nisos' Adversary Insights Investigations Suite is a subscription service that provides timely, finished intelligence to help security teams anticipate threats and undertake security investigations. As a Managed Intelligence service, Nisos provides and manages the people, processes, and technologies required to identify, stop, and prevent increasingly sophisticated adversaries.

A Partner Focused on Your Intelligence Needs

Working as an extension of your team, Nisos provides intelligence focused on the material 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' concerns.

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 proactively collects and queries 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 leading, 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.

Multi-Source Intelligence

Intel developed from Nisos' curated collection of investigative tools and difficult-to-access data from the open, deep, and dark web.

Nisos Expert Analysis

Broad intelligence expertise that includes depth in multiple intelligence disciplines plus technical and investigative experience.

Right-Sized and Actionable Reporting

Relevant research and actionable analysis that facilitates rapid and precise response to client inquiries.

Prioritized Recommendations

Detailed reports with recommendations that include prioritized actions, next steps, and key considerations specific to each client.

Analyst Engagement and Client Success

Nisos experts are at the center of each engagement. As a Nisos client, you have access to a Lead Analyst and a Client Success Director who are focused on your intelligence needs. Client Success Directors have, on average, over 10 years of intelligence experience and serve as your point of contact for troubleshooting, contracting, and administrative needs. Client Success Directors also ensure intelligence deliverables meet your expectations and they are available to assist you throughout the lifetime of your Nisos engagement.

Unlimited Investigations

Nisos analysts work with your team to address your most pressing security concerns. They respond to Requests for Information (RFIs) and support your ongoing security operations. You may request an unlimited number of sequential investigations into specific threats and concerns.

The Adversary Insights Investigation Suite includes two types of investigations:

- **Spotlight RFI**
  This report type focuses on simple queries, including yes/ no answers of limited complexity. The insights from this report may lead to additional investigations or confirm that there is no need for concern. Spotlight Reports typically require two business days to complete.
- **Targeted RFI**
  This report type goes more in-depth to answer questions when fast turnaround and pointed, specific answers are required. Targeted Reports typically require five business days to deliver.

Intelligence Reports Catalog

In addition to answering your intelligence-related questions about a specific threat, situation, concern or priority unique to your business, you can also select reports from the Nisos Intelligence Reports Catalog. These reports provide topic-specific information on risks to your organization and help keep your teams abreast of evolving attacker methodologies, tools, and tactics. Our growing catalog includes reports around the following subject and more.

Pre-scheduled Intelligence Reports Catalog

- **Industry Landscape**
  A report providing insights into actors, attacks, and TTPs observed within a client's industry.
- **Geographic Landscape**
  A report providing insights into actors, attacks, and TTPs observed within a geographic area.
- **Code Leaks**
  A report showing any proprietary code and sensitive items such as API keys and passwords exposed on code-sharing sites or publicly accessible code repositories.
- **Compromised Credentials**
  Discovery and identification of employee or customer credentials compromised through malware, account takeover, or overlapping exposure from third party breaches due to password reuse.
- **Deep & Dark Web Mentions**
  Discovery and identification of actors discussing attacks, ways to conduct fraud, and coordinating efforts against an organization.
- **News Summary**
  Triage and distribution of open source news articles tailored to the client's concerns and requirements.
- **CVE Summary**
  Triage and a summary roll-up of recently disclosed vulnerabilities and exploitation discussed in OSINT.
- **Actors Claiming Network Access**
  Identification and assessment of actors making claims or advertising network access to a client, vendor, or supply chain partner, along with identification of postings on ransom and extortion leak sites.
- **Anomalous Network Traffic**
  Analysis of internet traffic observed ingressing and egressing an organization's network to identify abnormal traffic that may be undetected with traditional security controls.
- **Third Party Focused Assessment**
  A tailored assessment to identify specific organizational, geopolitical, or technical risks of a vendor or supply chain partner.

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