Service Brief

Intelligence Team as a Service

FOR CYBER DEFENSE

Collaborative subscription-based engagement providing robust intelligence and tier 3 cyber intel analysts

Nisos enhances your cyber threat intelligence programs, enabling you to consume and operationalize data collected from various sources to inform cybersecurity operations, improve defenses, disrupt attacks, and stop adversaries.

Traditional security tools are typically designed to manage events, indicators, and alerts. They do not automatically curate intelligence and discover insights specific to your organization in collected data. A traditional security vendor ecosystem provides indicators, but realistically, you need more context to create intelligence that you are obligated to respond to in order to properly investigate anomalies and attribute actions to actors.

Our Approach

Cyber threat intelligence should inform a security operations center's prioritization of the most critical cyber risks to the business. In other words, true intelligence informs you in a way that a traditional security stack cannot.

Data enriched into actionable intelligence informs and establishes priorities for the SOC, threat hunting, vulnerability management, red team, application security, security engineering team, and business units. Nisos uses customized intelligence gathering and analysis to investigate as a team which threats are targeting you. analysis capabilities.

Intel Team as a Service is Different

Maximize your organizational security with tier 3-level analyst-led diligence investigations that combine automation and human intelligence to deliver actionable information that is customized to your unique challenges.

Nisos Collection & Analysis Stack

Network & Telephony
- Anonymous Infrastructure
- DNS and WHOIS
- Internet Netflow (90%+ of IPV4)
- Mobile and IP Geolocation
- Threat Feeds

Web & Social
- Deep and Dark Web
- Foreign Media
- Historical Web Content
- Open Web
- Social Media

Human
- Closed Forum
- Deep and Dark Web

Media
- Domestic News
- Foreign Media

Adversaries
- Activist
- Disinformation
- E-Crime
- Nation State
- Political

Breach
- 20+ billion records of legally acquired datasets including PII, selectors, and information/credentials

Businesses
- Business Registrations
- Corporate Filings
- Corporate Profiles
- Public Records

Persons & Groups
- Biographical
- Civil and Criminal Actions
- Email and Identity
- Investigative Databases
- Public Records

Services

Threat information is not *"intelligence"* until it becomes contextualized and actionable. Understanding the threats to your organization allows you to better prepare, prevent, attribute, and respond to specific actors looking to take advantage of resources and weaknesses, including advanced persistent threats, fraud actors, and insiders.

Cyber Threat Intelligence Enrichment

Nisos works with your security operations team as your tier 3 intelligence extension to enrich existing data and selectors and provide expert insight to make threat information actionable. When your SOC determines an event is malicious, we provide the added context to mitigate the attack and improve defenses. When you have suspicious events, Nisos provides the intelligence to determine if they are benign or malicious, and to react accordingly.

Beyond event response, we also augment current understandings with external threat hunting, which is a process of connecting external telemetry, including netflow, with organizational data, including internal data where necessary. We are also capable of taking over an investigation when the internal team does not have the skillset or the time.

Threat Monitoring

Empower your team to improve your security posture. Even the most sophisticated adversaries leverage internet resources during attack planning. With monitoring, you can better prevent and prepare for attacks with insight into imminent risk from threat actor activity and reveal evidence of compromise.

Nisos monitors for indicators of attack or compromise, including traffic pattern analysis from global netflow data, monitoring threat actor infrastructure, message groups, and internal domain leaking (such as DNS and certificates.)

We also conduct deep web, dark web, and forum analysis to identify credentials, intellectual property, or other sensitive data disclosed or for sale, as well as analyze threat actor chatter.

By monitoring threats that are specific to you, we are able to focus, prioritize, and triage so you can improve your cybersecurity defenses and mitigate avoidable risks.

Key Areas We Assist

Indicators of Compromise and Selector Enrichment

- Infrastructure being used by the actor
- Information about other organizations possibly affected by the attack
- Tool and TTP attribution
- Actor attribution
- Showing value from intel feeds

Internal Domain Leakage

- DNS queries and domain registrations
- Certificate abuse

Public Channels on the Dark Web

- Pastebin, GitHub, Leaked Identities
- Dark Web Monitoring
- Leaked data dumps, forums, and chat rooms, and OSINT

Additional Data Collection and Research Analysis Investigated

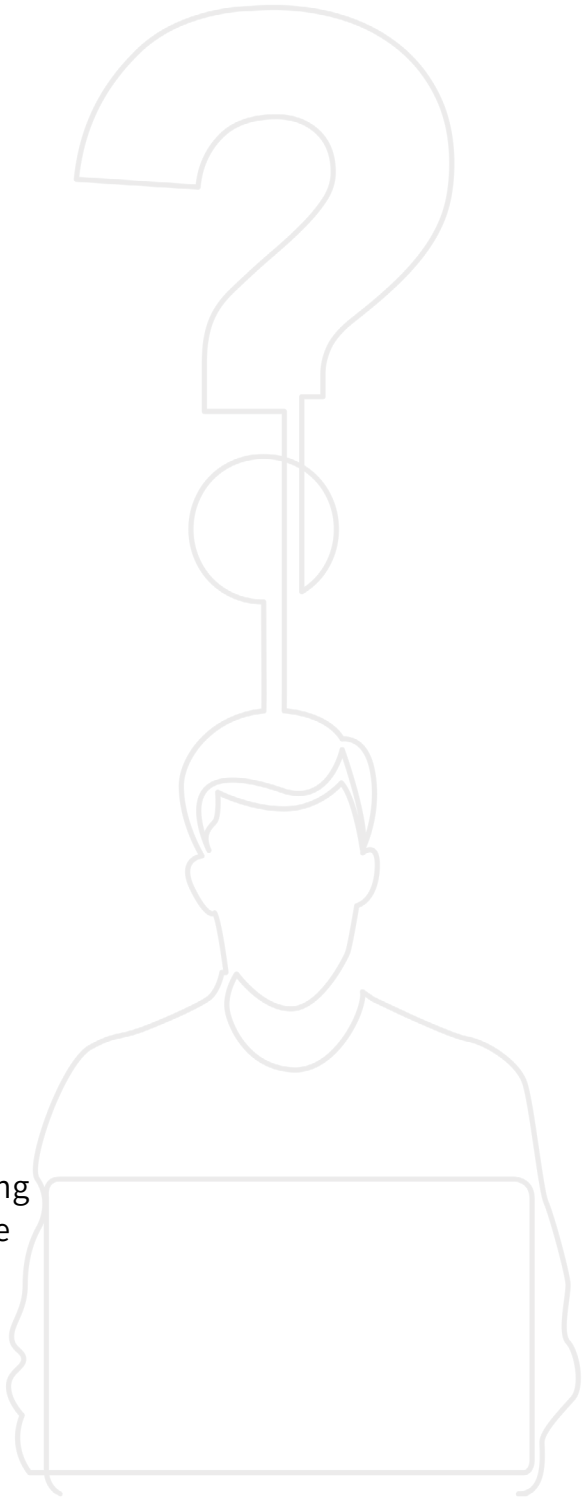
NetFlow/outside-the-firewall analysis	Sensitive information disclosure	Data breach announcement	Honey tokens, canary files, etc.	Direct threat actor engagement
Review of known compromised libraries, compromised publicly available docker images, and attacks against cloud providers (AWS, GCP, Azure)	Indicators and warnings as seen in media, social media, and geolocation information *Gab, Reddit, Parler, Bitchute, Telegram, WhatsApp, 8kun, 4chan, Twitter, FB, Dark Web Forums, Blogs, IRC*	Search for sensitive data on code-sharing and repository sites, including Github, Sourceforge, etc.)	Discussions/threats observed in Dark Web/IRC/messaging networks and underground forums	Technical techniques in social media data
Develop trust within Dark Web hacking communities	Geolocation of IP address	Malicious TLS cert identification	Ransomware detected	Compromised company account credentials
Phishing and spoof sites	Receiving spam	NetFlow analysis of suspect or anomalous IPs	Origination and amplification of DDOS attacks	Malware hosting/ distribution
Questionable asset use: Proxy, TOR Node, etc.	Virus/botnet infection	Gain access to closed forums and marketplaces	Command-and-control activity	Using mobile data to identify individuals and physical locations
NetFlow access	Suspicious domain registration	Ability to interact in any foreign languages	Malicious/scanning behavior	Open source media analysis
Client mention/ discussion by a Known Threat Actor	Hosting of phishing activity	Rogue, impersonated application discovery	Claimed relationships or impersonations posted online by parties/sites other than those officially whitelisted	Indicators of criminal or derogatory information related to Client executives

Deliverables

Nisos provides subscription-based monitoring, which enables you to take action and protect your people, your business, and your assets with rapid and curated responses to intelligence questions and concerns.

Reports available:

- **Fast Inquiry:** an on-demand request for information that includes a curated response to a specific intelligence question from a client
- **Situation Briefing:** an on-demand summary status report of an ongoing situation or activity monitored by Nisos researchers and analysts
- **Spot Report:** a supplemental brief used to quickly communicate time-sensitive intelligence for significant events impacting a client



About Nisos

Nisos is the Managed Intelligence™ company. Our services enable security, intelligence, and trust and 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 response against advanced cyber attacks, disinformation, and abuse of digital platforms.

For more information visit: nisos.com
email: info@nisos.com | 703-382-8400