Service Brief

On Demand Threat Research

FOR CYBER DEFENSE

Proactive and preventative investigations that reveal threat actor context and risk correlations

Imagine having the level of coverage and visibility outside your digital perimeter as you do within when a security event occurs...

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

Enterprises have funded in-house teams to address cybersecurity defense, with technology and a level of expertise to keep many bad actors out of their environment.

What they do not have is what Nisos provides: deep intelligence expertise and multi-source collection capabilities that deliver “outside the firewall” insight into threat actor behavior, motivations, plans, and intentions that exist outside of your environment.

As the attack surface continues to widen and manifest on the digital plane, you benefit by having a go-to expert resource to address complex challenges.

Our Approach

Cyber threat intelligence should not only inform a security operations center’s prioritization of the most critical cyber risks to the business; they should also have the capability to investigate any cyber threat globally.

We combine threat intelligence with investigative prowess outside your perimeter to bring short-fuse actionable intelligence priorities for the SOC, threat hunting, vulnerability management, red team, application security, security engineering team, and business units.

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

Nisos On Demand Threat Intel is Different.

We designed our short-fuse on-demand threat intelligence to extract client-specific data from our vast multi-source collection capabilities to perform expert analysis, rather than the traditional product threat intelligence approach of collecting large digital datasets and creating a search capability for keywords. This differentiates our intel in two ways. First, we fuse external telemetry with internal data proactively to determine the proper controls to be able to get back to business quickly. Second, we attribute the adversary, if necessary.

Services

Threat information is not “intelligence” until it becomes contextualized and actionable. Responding to your organization’s threats allows you to better prepare, prevent, mitigate, and attribute to specific actors looking to take advantage of resources and weaknesses, including advanced persistent threats, fraud actors, and insiders.

Below are areas where our short-fused investigations generally tend to focus with the intent to detect and avoid an incident when possible, address control gaps for mitigation, and potentially attribute the adversary.

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 on-demand threat intel investigations, enabling 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