Service Brief

Intelligence Team as a Service

FOR CORPORATE SECURITY

Collaborative subscription-based engagement providing robust intelligence and analysis

Nisos enhances your corporate security teams, enabling you to consume and operationalize data collected from various sources to disrupt attacks, stop adversaries, and improve defenses.

Imagine having a digital investigative team that provides consistent and constant monitoring in the security disciplines of physical security, trust and safety, executive protection, and fraud.

Traditional corporate security tools and collection mechanisms focus on data sources and analysis relating to physical security while putting less emphasis on the intersection with digital space. They do not have the ability to engage with malicious actors online, monitor their activities at scale, or alert in a time-sensitive manner.

A traditional security vendor ecosystem provides leads, but realistically, you need more context to create intelligence that you are obligated to respond to in order to properly investigate and attribute actions to actors.

Our Approach

Security intelligence should inform an enterprise's prioritization of the most critical corporate security threats to the business. In other words, corporate security intelligence should inform and have coverage beyond human-centric investigations and social media analysis alerts of SIGACTs (significant activities). They should have persistent, digital access and placement in places that matter to your business that allow actionable insights to illuminate unknown potential risks.

Nisos extracts client-specific data from our vast multi-source collection capabilities to then perform expert analysis, rather than the traditional product threat intelligence approach of collecting large digital datasets and creating a search capability for keywords. Flipping the script gives us unique visibility into adversaries, and enables insights into attacks and attribution of adversaries even if they aren't knowing actors using previously connected tactics, techniques, and procedures (TTPs).

Nisos Intel Team for Corporate Security is Different.

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

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, belligerents threatening executives, and insiders.

How it Works:

When you engage Nisos under your Intelligence as a Service subscription, you choose which collection and analysis solutions you want routinely monitored in order to gain access to unparalleled custom research that delivers ongoing actionable insights.

Our robust analytic methodology, combined with our suite of tools to collect, store, enrich, and integrate data from a wide variety of sources helps us to arm your internal team with the intelligence they need to work faster and with more accuracy.

Resource available on nisos.com

If further research or requests for information (RFIs) are needed, depending on the request, we may need to create an additional Adversary Insights Retainer℠.

Corporate Security Monitoring

Defend and Respond to Cyber Crime, Espionage, E-Crime, and Fraud

In order to defend against espionage, e-crime, and fraud, you must detect threats with greater speed, accuracy, and effectiveness. In addition, and most importantly, the intelligence must be tailored to combat global threats occurring at scale against your organization. Here are a few of the things we do proactively and reactively to protect you from e-crime and fraud:

Proactive and Reactive Activities

NetFlow and mobile data access, monitoring, and outside-the-firewall analysis	Search for sensitive data on code-sharing and repository sites including Github, Sourceforge, etc.	Review of known compromised libraries, publicly available docker images, and attacks against cloud providers (AWS, GCP, Azure)	Discussions/threats observed in Dark Web/IRC/messaging networks and underground forums
Gain access to closed forums and marketplaces	Questionable asset use: Proxy, TOR Node, etc.	Sensitive/Confidential/IUO Document disclosure	Data breach announcement
Phishing and spoof sites	Detecting spam	Virus/botnet infection	Malware hosting/distribution
Suspicious domain registration	Compromised company account credentials	Malicious/scanning behavior	Open source media analysis
Origination and amplification of DDOS attacks	Command and control activity	Ransomware detected	Hosting of phishing activity

Respond to Disinformation and Brand Reputation Attacks

The cyber domain brings significant risk to reputation, brand, employees, products, and workplaces. While the risks associated with reputation attacks are not new, they are increasing in both volume and scope. Adversaries, supported by a healthy budget and increasingly sophisticated technical means, continue to inflict damage upon their targets.

Nisos provides attribution for threats to your brand and assets. Our approach utilizes our robust multi-source collection capabilities with analysis from fraud, financial, geopolitical, competitive, and activism perspectives. When an issue is identified, we determine the outlets and actors propagating it. For coordinated activity, we also will reveal the signatures of their approach and then apply telemetry to identify patterns and shut down the spread and the threat actor.

Nisos Activities for Disinformation and Brand Reputation Attacks

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*	Claimed relationships or impersonations posted online by parties/sites other than those officially whitelisted	Adversarial campaign, petition or divestiture negative commentary, stealing IP	Discussions/threats observed in Dark Web/IRC/Messaging Networks and Underground Forums
Heat maps for crime and geopolitical hotspots for foreign market expansion	Domain Name Issue – Cyber/ Typo-Squatting	Potential damaging workplace commentary	Boycott activity or organizing related to the client
Summary of disinformation narratives propagated by key offenders	Attribution of disinformation accounts and outlets	Social network analysis of accounts with correlations highlighted	Outlet registration and tracker correlations highlighted
Name, brand, visual identifier, or platform misuse or abuse	Unauthorized social media account(s) or company-account impersonation	Sites/pages associating the brand with objectionable content (pornography, hate speech, racism, extremism)	Rogue, impersonated application discovery, and reverse engineering

Provide Executive Protection

For businesses looking to gather greater insight and develop protection for VIPs, executives, and immediate families, Nisos can help mitigate threats and recommend actions that can be taken to reduce digital online footprints. Using monitoring and attribution methods, Nisos tracks and identifies threats on social media and within the dark web targeting your people. Here are a few of the things we do proactively and reactively to address your needs:

Proactive and Reactive Activities

Alerting of potential/ actual disruptive activities (boycotts) targeting, in proximity to, or focused on individuals and their physical locations	Illegitimate registration of social media accounts and domain names	Posting of “Dox,” digital dossier or personal details for a “C” Level Executive on Social Media, Paste Sites, IRC, or the Dark Web	Adversarial campaign, petition, or divestiture commentary
Indicators and warning	Threats to company employees, executives, assets, or facilities	Executive Vulnerability Assessment	Compromised account credentials

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