Service Brief

Event-Driven Intel Investigations

Multidimensional security fact-finding that delivers insights into adversary behavior

If your organization is facing a security emergency from fraudsters, nation states, organized crime, terrorists, hacktivists, insiders, extremists, online belligerent, or competitors, you need Nisos' unparalleled intelligence matched with our investigative expertise.

Quick reaction, event-driven intelligence investigations from Nisos allows you to ensure business continuity, confidentiality, integrity, and availability, simultaneously attribute malicious actors if necessary, take subsequent administrative or legal action, and get back to business quickly.

Despite funded enterprise in-house teams whose job it is to address the many facets of security (cybersecurity, trust and safety, fraud, executive protection, disinformation, physical security, and brand reputation) many teams do not have the data collection, visibility, intelligence capability, and investigations capacity like Nisos.

Our Approach

Rather than the traditional threat intelligence approach of responding to breaches, collecting large cyber security datasets, and searching for outliers or trends to connect to forensics findings, Nisos extracts client-specific data from our vast multi-source, "outside the firewall" collection capabilities to then perform expert analysis.

Flipping the script gives us unique visibility into numerous types of adversaries, not just traditional tracked adversaries. This enables insights to attacks and attribution of adversaries even if they aren't knowing actors using previously connected tactics, techniques, and procedures (TTPs).

Nisos Intelligence Investigations are Different

We possess a differentiated set of collected data that, when paired with our expert adversarial mindset, provides intelligence to detect, disrupt, and prevent adversary operations. Most importantly, while Nisos can use our external telemetry to attribute actors with client-specific internal telemetry, often we thrive on not having an "internal network starting point".

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

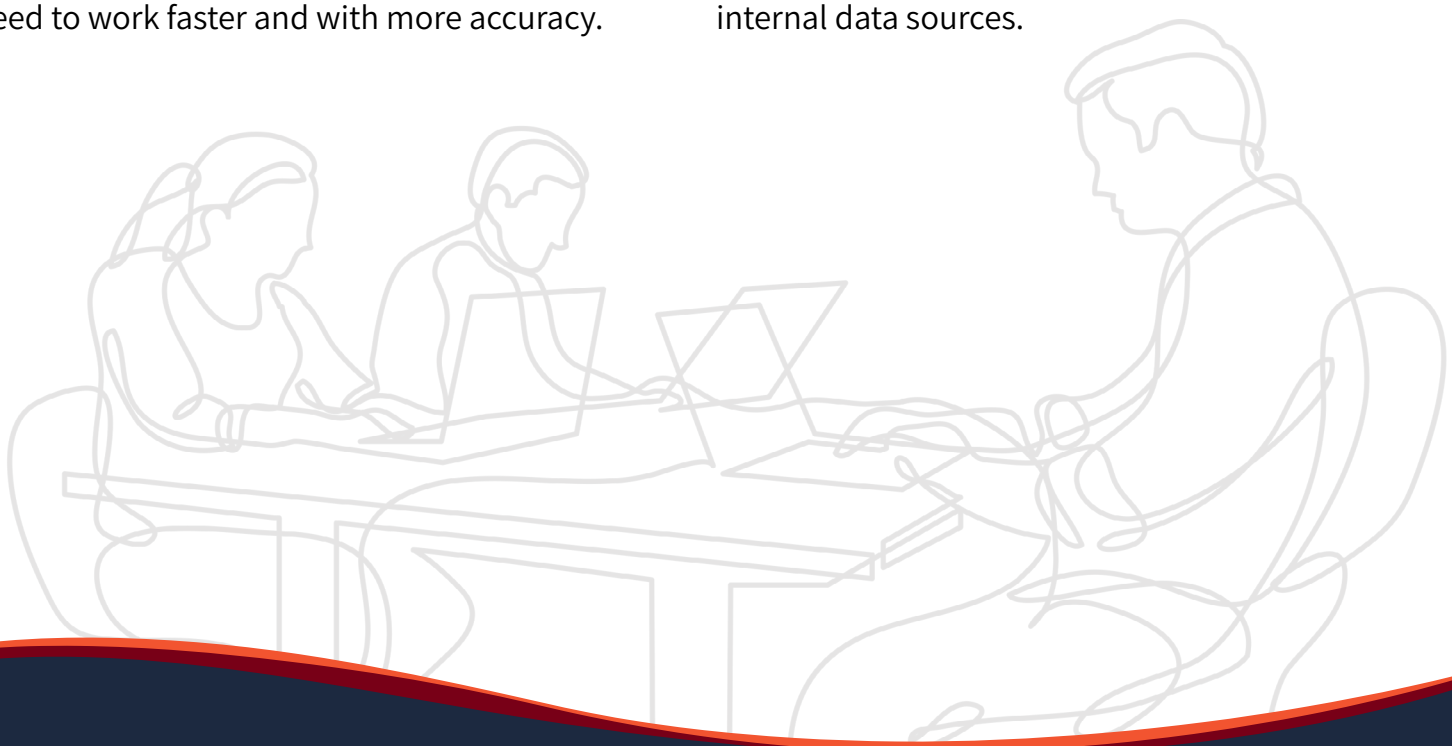
Businesses
- Business Registrations
- Corporate Filings
- Corporate Profiles
- Public Records

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

How it Works:

If you have a security event relating to digital adversaries that requires immediate attention, we can get started immediately. 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 arm your internal team with the intelligence they need to work faster and with more accuracy.

If you have a security event that's already underway, we can help augment or take over an investigation. If your security team is short on resources, doesn't have the bandwidth, or lacks the necessary expertise to stop adversaries, Nisos can help by combining our external telemetry and placing it into context with your internal data sources.



Common Adversary Challenges

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

To defend against cyber crime, espionage, 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.

For security professionals seeking adversarial context for actionable outcomes, Nisos takes a comprehensive approach to meeting the challenges of fighting and stopping threat actors with more diverse information and analysis enhanced by our multilingual capabilities and global linguistic expertise.

Here are a few of the things we do to protect you from e-crime and fraud:

Nisos 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.	Technical techniques in social media data	Data breach announcement
Threat actor engagement	Sensitive/confidential/IUP document disclosure	Infrastructure attribution	Using GeoIP data to identify individuals and physical locations
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

For continued reading on cyber, ecrime and more, **check out our case study library >>**

Common Adversary Challenges

Counter Disinformation and Brand Reputation Attacks

The cyber domain brings significant risk to reputation, brand, employees, products, and workplaces. While the risks associated with disinformation and reputation attacks are not new, they are increasing in both volume and scope. Well-funded and technically sophisticated adversaries 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, political, competitive, and activism perspectives.

When an issue is identified, we determine the actors propagating it and the outlets and methods they are using. For coordinated inauthentic behavior, we will reveal the technical signatures of their approach and determine telemetry to identify and enable you to shut down the spread and the threat actor.

Here are a few of the things we do to protect you from brand reputation and disinformation attacks :

Nisos Activities

Indicators and warning as seen in media, social media and geolocation information	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	Summary of disinformation narratives propagated by key offenders	Attribution of disinformation accounts & outlets
Social network analysis of accounts with correlations highlighted	Outlet registration & tracker correlations highlighted	Name, brand, visual identifier, or platform misuse or abuse
Rogue, impersonated application discovery and reverse engineering	Direct threat actor engagement and trust development, including gaining access to closed forums and within social media groups	Heat maps for crime and geopolitical hotspots for foreign market expansion
Potential damaging workplace commentary	Domain name issue – Cyber/Typo-Squatting	Boycott activity or organizing related to the client
Sites/pages associating the brand with objectionable content (pornography, hate speech, racism, extremism)	Unauthorized social media account(s) or company-account impersonation	Identification of potential insider threats including incident response support

For continued reading on Brand Reputation >>

Common Adversary Challenges

Provide Executive Protection

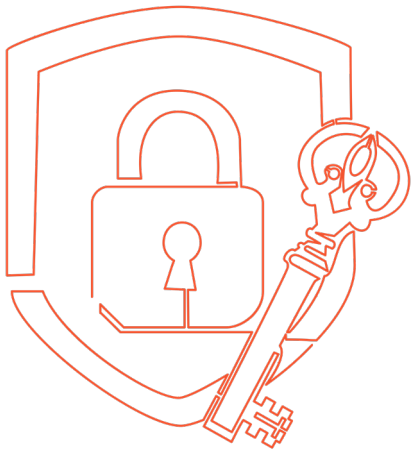
For businesses looking to gather greater insight and develop protection for VIPs, executives, and their families, Nisos can help mitigate threats and recommend actions that can be taken to reduce digital online footprints. Using monitoring and attribution methods, Nisos tracks and identifies threats on social media and within the dark web targeting your people.

Here are a few of the things we do to protect key personnel:

Nisos 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	Digital identity reduction, proactively removing executive PII from data brokers
Doxing response: insights when a digital dossier or personal details for a “C” level executive surface on social media, paste sites, IRC, or the Dark Web	Indicators and warning	Executive vulnerability assessment
Compromised account credentials	Threats to company employees, executives, assets, or facilities	Adversarial campaign, petition, or divestiture commentary

For continued reading on Executive Protection >>



Deliverables

Nisos helps you take action and protect your people, your business, and your assets with rapid and curated responses to your intelligence questions and concerns. Situation reports are available on demand. When relevant, native language translation by a subject matter linguist is available for on-demand and researched content.

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