NISOS

Service Brief

Adversary Insights Retainer^{SM}

Intelligence for client-driven inquiries and rapid-response so you'll always be prepared

Nisos deploys our experts and advanced methodologies to empower your organization with actionable insights tailored to counter the ever-maturing adversary.

Fraudsters, nation states, organized crime, terrorists, hacktivists, insiders, and competitors are potentially targeting you. These bad actors use their skill to evolve rapidly, hide themselves, and exploit your knowledge gaps.

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 insight into threat actor behavior, motivations, plans, and intentions which exist outside of your environment.

As the attack surface continues to widen, you benefit by having a go-to expert resource to address complex challenges. Enterprises know the "intelligence" they receive from their existing cyber security stack does not address the questions they have or provide the answers they need to identify, stop, and prevent increasingly sophisticated adversaries.

When you need to know who is doing what against your business, why they are doing it, how they are doing it, and when they might try something similar again, Nisos is here with our diverse intelligence analysis capabilities.

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

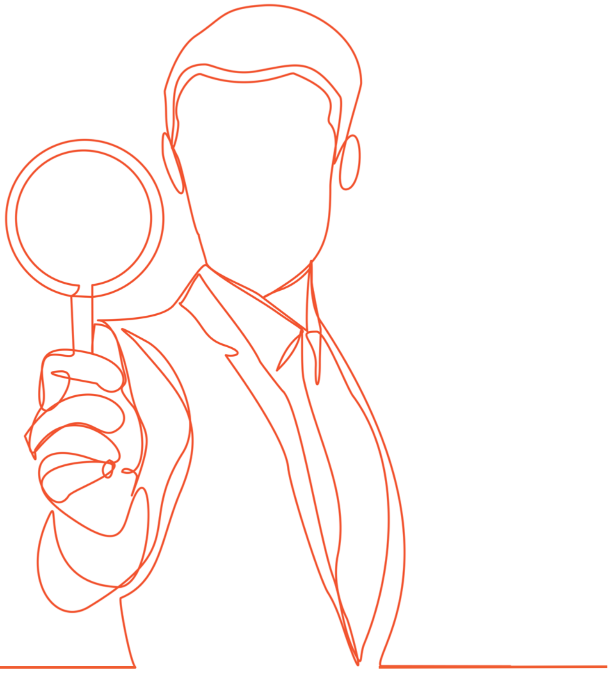
Persons & Groups

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

Real Attribution

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.

Nisos can also attribute actors, enabling you to pursue legal or law enforcement measures against the perpetrators and resume normal business operations.



How the Retainer Works:

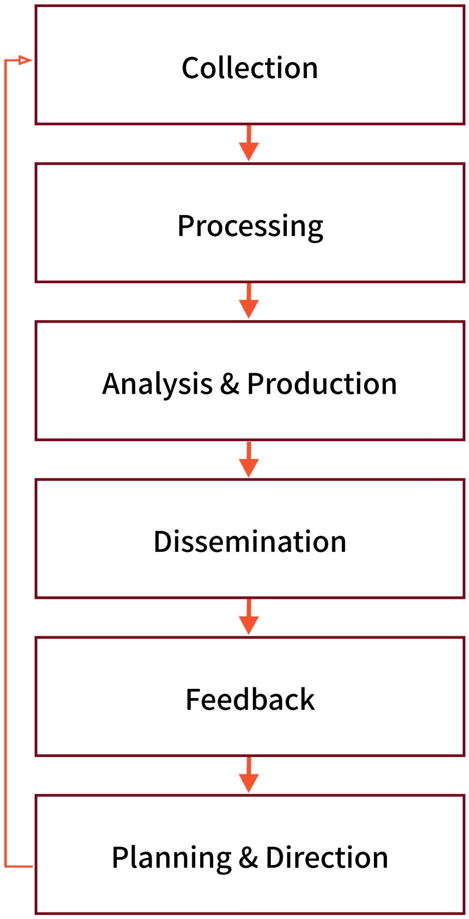
When you engage Nisos under your Adversary Insights Retainer, you gain access to unparalleled custom research that delivers ongoing actionable insights.

That means that if you send us RFIs, taskers, or questions about adversaries, you get expert insights - fast. 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.

We Deliver Intelligence and Research in the Ways You Need it

We are focused on helping you investigate and attribute adversaries. Depending on your present and evolving needs, Nisos can scale to fit your requirements.

The Intelligence Lifecycle



Collection

Processing

Analysis & Production

Dissemination

Feedback

Planning & Direction

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 proactively and reactively to protect you from e-crime and fraud:

Proactive 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
- 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

Reactive Activities

- Threat actor engagement
- Sensitive/confidential/IUP document disclosure
- Infrastructure attribution
- Using GeoIP data to identify individuals and physical locations
- 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 proactively and reactively to protect you from disinformation attacks:

Proactive Activities

Indicators and warning as seen in media, social media and geolocation information

Discussions/threats observed in Dark Web/IRC/messaging networks and underground forums

Social network analysis of accounts with correlations highlighted

Potential damaging workplace commentary

Claimed relationships or impersonations posted online by parties/sites other than those officially whitelisted

Summary of disinformation narratives propagated by key offenders

Outlet registration & tracker correlations highlighted

Domain name issue – Cyber/Typo-Squatting

Adversarial campaign, petition or divestiture negative commentary, stealing IP

Attribution of disinformation accounts & outlets

Heat maps for crime and geopolitical hotspots for foreign market expansion

Boycott activity or organizing related to the client

Reactive Activities

Name, brand, visual identifier, or platform misuse or abuse

Sites/pages associating the brand with objectionable content (pornography, hate speech, racism, extremism)

Rogue, impersonated application discovery and reverse engineering

Unauthorized social media account(s) or company-account impersonation

Direct threat actor engagement and trust development, including gaining access to closed forums and within social media groups

Identification of potential insider threats

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 proactively and reactively to protect key personnel:

Proactive Activities

Alerting of potential/actual disruptive activities (boycotts) targeting, in proximity to, or focused on individuals and their physical locations

Executive vulnerability assessment

Illegitimate registration of social media accounts and domain names

Compromised account credentials

Indicators and warning

Reactive Activities

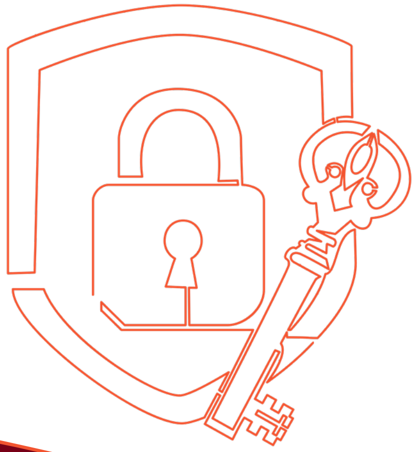
Digital identity reduction

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

Threats to company employees, executives, assets, or facilities

Adversarial campaign, petition, or divestiture commentary

For continued reading on Executive Protection >>

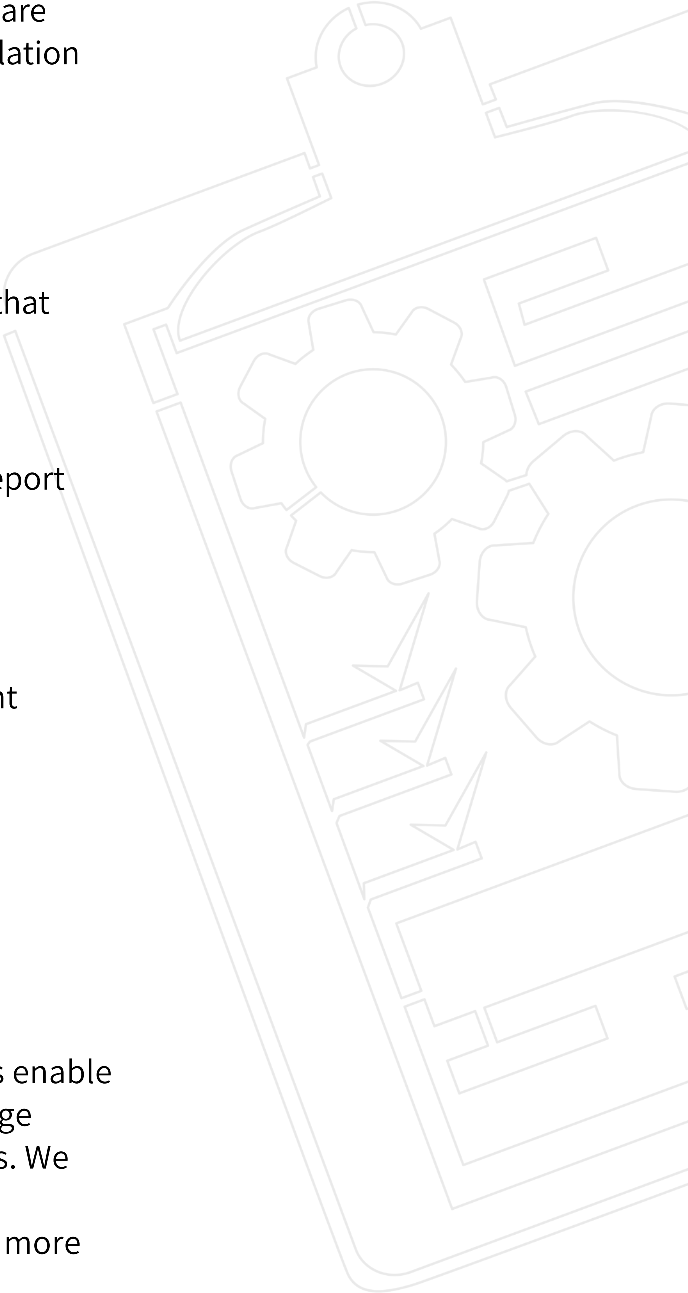


Deliverables

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