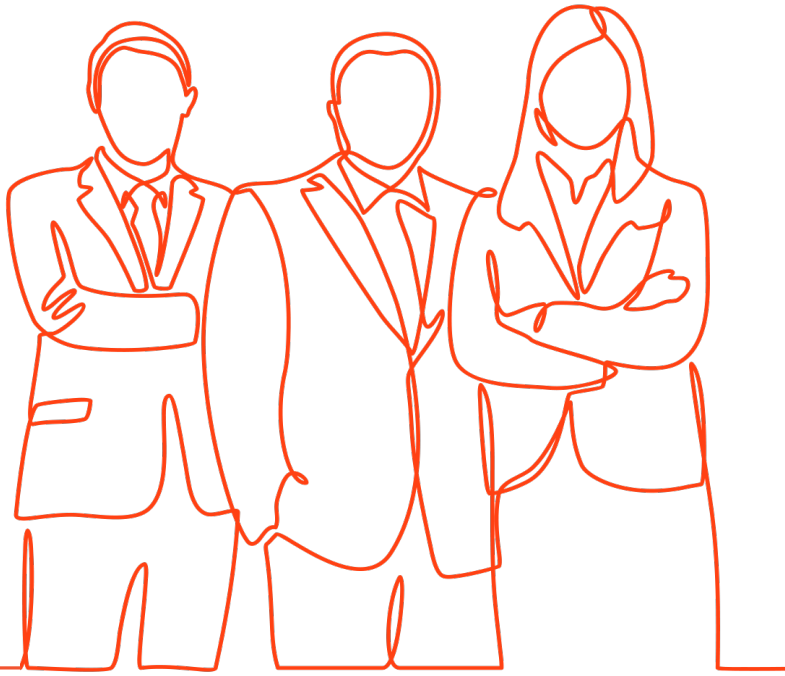
Solution Brief

Executive Shield

FOR CORPORATE SECURITY

Threat assessments to address doxxing, stop fraud, and reduce real physical security risks to high visibility people

When online adversaries target your executive team members and their families, Nisos Protective Intelligence can help you identify, assess, validate, and mitigate threats.



For businesses looking to gather greater adversary insight and develop protection for VIPs, executives, their families, and other important individuals, Nisos can help mitigate threats and recommend actions that can be taken to reduce digital footprints.

Using threat monitoring and attribution methods, Nisos tracks and identifies threat actors on social media, extremist forums, and within the dark web targeting your people.

Common "Solutions"

Traditional corporate security tools and collection mechanisms focus on **data sources and analysis** relating to physical security, putting less emphasis on threats developing within the digital space. Typically, they **do not engage** with malicious actors online, **monitor** their activities at scale across various platforms, or **alert** in a time-sensitive manner.

Nisos Executive Shield is Different.

Maximize the protection of key personnel with customized, actionable research that is gathered through OSINT, analyst-led investigations, automated reporting, and digital human intelligence.

How it Works:

We collect and analyze data across numerous social media channels, extremist forums, data leak sites, and dark web platforms. Routinely engaging with threat actors to maintain our credibility, we are able to maintain relevance and stay apprised of potential threats before they're acted upon. Learn about our Social Media Monitoring and Analysis Capability.

We constantly collect various forms of breach data, personally identifiable information (PII) publicly available on the internet, and subscribe to many major data brokers that aggregate PII on individuals and companies. This allows us to quickly validate and research information from a much larger database than our peers. Learn about the Nisos Information Database.

Why it's Better:

Nisos extracts and enriches client-specific data from our vast multi-source collection capabilities to perform expert analysis. Other companies simply perform a traditional product threat intelligence approach by collecting large digital datasets and creating a search capability for keywords. They provide you with data.

Our process gives us unique visibility into adversaries, enables deeper insights into attacks, and allows attribution of adversaries even if they aren't known actors using previously connected tactics, techniques, and procedures (TTPs).

We provide you with finished intelligence.

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

Capabilities

Vulnerability Assessment

Identify exposed PII of key personnel and their families and provide recommendations and support to reduce digital exposure. We leverage OSINT tradecraft and access to discreet datasets to produce a thorough picture of risk and vulnerability.

PII Reduction

Using commercially reasonable efforts, we comprehensively remove PII for executives and family members from publicly available databases and brokers. We document what data cannot be removed for legal and policy reasons and generate a results report demonstrating the percentage of digital reduction.

Online Monitoring

We periodically monitor and provide notifications of threatening social media mentions and comments targeting executives and family members. We focus intently on threat actor activities that mention or organize efforts to physically target executives. Below are activities that can be routinely monitored:

- 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
- Threats to company employees, executives, assets, or facilities
- Compromised account credentials
- Posting of "Dox," digital dossier or personal details for a "C" Level Executive on Social
- Indicators and warnings
- Executive Vulnerability Assessment and PII Reduction
- Adversarial campaign, petition, or divestiture commentary

The results of Online Monitoring may lead to a RFI to dive deeper and engage directly with an adversary or provide attribution. While these services are not included in Online Monitoring, they are available via an Adversary Insights Retainer, where we investigate questions around the credibility, identification, location, and background of a threat.

Deliverables

Nisos provides on-demand-based and subscription-based monitoring that enables you to take action and protect your people, your business, and your assets. Increase your insights into real risk with rapid, 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