NISOS

Webinar Brief

Managed Intelligence: Working Together to Stop Your Adversaries

Main Takeaways

In the private sector, the cybersecurity industry has hijacked the concept of threat intelligence. Cybersecurity vendors deliver threat data via platforms and feeds, which provides value, but falls short of actual intelligence because it lacks contextualization, refinement, and actionable recommendations. As the only Managed Intelligence™ provider, Nisos delivers finished intelligence to Fortune 500 companies.

Executive Summary

The enterprise threat landscape is rapidly evolving, and businesses of all sizes are pressed to find the threat intelligence they need to address their specific threat picture. Cybersecurity vendors have built a host of Cyber Threat "Intelligence" (CTI) offerings to fill this need.

While these solutions can deliver timely threat data, few vendors have the analytical capability to distill this data into actionable intelligence. Furthermore, cyber threats are just one example of everyday risks an enterprise must target to maintain business continuity, protect their brand, and ensure the safety of their people and assets.

As a Managed Intelligence provider, Nisos is uniquely positioned to help Fortune 500 companies address risk. In this webinar, Nisos outlined three of our core intelligence offerings: OSINT Monitoring & Analysis, Executive Shield, and Adversary Insights® RFI Subscriptions.

OSINT Monitoring and Analysis

OSINT Monitoring & Analysis (OMA) is an analyst-led, client-specific Managed Intelligence service that provides monitoring of technical and non-technical threats and sources of risk against clients across the surface, deep, and dark web. OMA subscriptions provide security teams with the intelligence they need to address threats across all six intelligence domains, including cyber, fraud, protective, reputation, platform, and third-party.

The OSINT Monitoring & Analysis Lifecycle parallels the intelligence cycle to provide our clients with in-depth, ongoing, Managed Intelligence. The Nisos team leverages automated feeds, a deep toolset, and manual checks (including social media platforms, forums, and dark web sources) to make it possible for our analysts to comb through tens of thousands of client mentions and threat indicators to surface only the most relevant and actionable intelligence.

Executive Shield

With Executive Shield, Nisos protects key personnel with intelligence gathered through periodic analyst-led investigations, automated reporting, and digital human intelligence. Executive Shield starts by identifying the executive's digital footprint and threat landscape by looking for concerning exposure and ongoing discussions of the target.

From there, the team works to reduce as much publicly exposed information as possible, going the extra mile to remove data from sites that can't be automated, minimizing the vulnerability of the executive. Finally, Nisos analysts inject "noise" into the PII system by adding an actual name with a hotel or coffee shop in a different city or a fictitious name with a real address.

Adversary Insights® RFI Subscription

Adversary Insights® RFI Subscriptions leverage Nisos analysts to act as an extension of your team, performing comprehensive research, analysis, and investigation tailored to your key concerns. Adversary Insights fuses a complete range of intelligence disciplines with robust data aggregation and collection capabilities across the surface, deep, and dark web.

Typical Adversary Insights Use Cases:

- Adversary unmasking and attributions
- Disinformation campaign investigations
- Fraud/abuse ecosystem analysis
- Threat actor-network analysis
- Social media characterization
- US/Foreign person pattern of life
- Breached credential and PII exposure checks

Adversary Insights® RFI Subscriptions are perfect for intelligence teams that need the expertise to address disparate security threats and don't have the resources, skills, or bandwidth to address issues adequately.

Nisos offers four report types as part of RFI subscriptions:

- **Spotlight -** Report focused on indicator research and collection with rapid analysis to establish if client's concern is a threat. This report is delivered within 1-2 business days.
- **Targeted -** Report provides research and analysis focused on a single problem or threat actor, leveraging broader datasets and analysis. This report is delivered within five business days (1 week).
- **Extended -** Report provides research, analysis, and correlation focused on a single problem or threat actor across platforms and personas. This report is delivered within ten business days (2 weeks).
- **Deep -** Report provides deep research, analysis, and correlation focused on a single problem or threat actor across platforms and personas, including their signatures and networks, supported by custom technology deployment and bespoke data collection. This report is delivered within 20 business days (1 month).

About Nisos

Nisos is the Managed Intelligence Company™. Our services enable security, intelligence, and trust & 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 cyberattacks, disinformation, and abuse of digital platforms. For more information visit: **www.nisos.com**

This briefing is not legal advice and is provided for general informational purposes only.