NISOS

Webinar Brief

Why Flexibility is the Key to Threat Intelligence Success

Main Takeaways

- Cyber Threat Intelligence (CTI) provides valuable context during Incident Response (IR) processes by helping to identify attacker agendas, progress, and potential ways to reduce damage.
- Nisos Managed Intelligence™ services offer tailored analysis to help clients identify larger fraud operations that may be affecting their organizations.
- Cyber and physical security threats are often linked, which makes online monitoring crucial to protecting personnel and facilities within an organization.
- Organizations can use Open Source Intelligence (OSINT) and Threat Intelligence to better understand risks to personnel and specifics around cybersecurity hygiene.

Executive Summary

Threat intelligence teams lead the charge in safeguarding organizations from cyber threats, but staying ahead of the curve is no small feat. Depending on the size of an organization, its digital footprint, and the need for speed, these teams must build or retain a managed service with investigative capabilities that can scale with their company's needs.

Cyber Threat Intelligence for Incident Response and Insider Threat

Incident Response (IR) is a cyclical process similar to the intelligence process and involves looking for the most accurate information to make decisions. The kind of intelligence you are looking for will change depending on where you are in your response process.

Cyber Threat Intelligence (CTI) teams provide context during the IR process around what companies need to be looking for next, such as details on attackers' agendas or progress during an operation. CTI teams also recommend ways to increase friction for attackers, thereby reducing potential damage.

Best practices for using intelligence to create a more resilient security infrastructure include analyzing likely attackers and their tactics, techniques, and procedures (TTPs). Remediation activities, such as loading new domains or IPs into a proxy may help disrupt an attacker and reduce damage to the company.

Fraud Investigations for Trust and Safety Teams

Trust and Safety teams frequently have visibility into their own services and platforms, but they struggle to know what's happening outside their environment. This is why a holistic approach is best for helping understand the complexity and the spread of an exploit.

When it comes to emerging threats, companies need visibility into specific information which tailored analysis can provide. These types of insights are time sensitive and a flexible solution can help with modifying existing policies and procedures or creating new ones to bolster safety for the organization and its customers.

Addressing Real-Time Threats to Personnel and Facilities

Threat Intelligence can be used effectively by security operation teams to protect personnel and facilities. There is often a link between cyber and physical threats. Regularly monitoring and reporting online threat activity as it fluctuates in volume is critical because of the potential cyber threats have in escalating into physical risks. Contextualization is key to validating threats to people and organizations.

Monitoring and Responding to Geopolitical Events

Geopolitical events often create a ripple effect felt by other countries and by other industries. Fake news and disinformation can spread quickly, especially when related to political events. Disinformation can spread quickly thanks to social media and mainstream news outlets. Investigation of disinformation activities can help determine how individuals are coordinating these activities and how this might affect a client's global business operations.

Threat Intelligence and OSINT Highlight Business Risk

Open Source Intelligence and Threat Intelligence can provide organizations with a better understanding of personnel risks, different companies they might be involved with, and their cybersecurity hygiene. Social media platforms and other OSINT tools can be used to identify connections to sanctioned entities, and additionally, help to highlight other risks that may be associated.

Cyber leaders must be prepared to help answer a multitude of questions - from how they should use threat intelligence to respond to incidents and insiders to how they can support Trust and Safety teams to battle fraud. Addressing real-time threats to people, organizations, facilities, and brands can be best managed through assessments and monitoring with investigations and rapid assessments when needed.

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.