NISOS

Webinar Brief

Scaling Intelligence Collection Across Open Source and Social Media

Main Takeaways

Open source intelligence (OSINT) is more than just scraping social media, press, and open source information. OSINT should be redefined as the following:

- **Direct threat actor engagement with adversaries:** sock puppet accounts engaging with other personas in open or closed forums.
- **Commercially available open-source research:** business data, social media, press, advertising subscriptions, breach data, etc.
- **Technical signature analysis:** passive DNS, mobile, netflow, malware samples, anything that can be commercially collected on the wire.

Executive Summary

Regardless of the use cases across physical, cyber, or fraud security, collection management is critical to identifying priority intelligence requirements (PIRs) that are important to the business that will reduce risk. Following collection management, a living platform (JIRA, MDC, etc) is also critical for collection requirements, data, and analysis. These boards should be updated on a regular basis and will often change.

Scaling Open Source Intelligence for Cyber Threat Intelligence

Open source intelligence is a critical piece of not only the “story-telling” framework that matches priority intelligence requirements with answers the stakeholders are seeking, but also provides critical context and enrichment to technical data being matched with internal telemetry.

Common problems being solved include:

- Vulnerability Management
- Security Operations
- Application Security
- Business Stakeholders concerned with Intellectual Property Protection
- Investigations including Incident Responses are general concerns addressed by CTI and OSINT

An onion-layered approach to reviewing threats can be specific to:

- Organization
- Peers
- Industry
- Regions
- Targets of opportunity, such as ransomware as a service

Another way to review threats are either as *most common and probable* courses of action or *most dangerous* threats and courses of actions.

Scaling Open Source Intelligence for Physical Security

- Executive Protection
- Travel Security
- Global Investigations
- Mergers and Acquisitions
- Vendor and Supplier Diligence
- Physical Asset Security
- Geo-Political Risk
- Environmental Risk

Open source intelligence is critical for transitioning from "trends" or vague threats, followed by alerting on OSINT that is actionable and meaningful. For example, a threat actor who vaguely states "I want to harm X executive" on social media is far less worrisome than an online persona speaking in slang that they want to target an executive's actual location. Stacking collection requirements and OSINT sources is important for being able to execute against this type of threat so analysts aren't drowning in meaningless alerts.

Categorizing organization-specific threats and how they pivot from mainstream social media to alternative platforms such as Telegram can be effective ways to prioritize a variety of threat actors.

Scaling Open Source Intelligence for Fraud

The 70/20/10 model is common in the fraud landscape. Seventy percent (70%) of collection against abuse reports should be blocked through automation; twenty percent should be reviewed, and 10 percent should be escalated to stakeholders for more thoughtful analysis and disruption. Distributed Denial of Service (DDoS), phishing, account takeovers, weaponization, and reconnaissance on a platform are common business problems being solved in fraud. Open-source intelligence is a critical piece of contextualizing the bottom thirty (30%) of threats.

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.