NISOS
Webinar Brief

Using Open Source and Threat Intelligence to Identify and Remediate Corporate and Physical Threats

Main Takeaways

The primary disciplines within a corporate security program are:

- Executive protection
- Physical asset protection
- Travel security
- Reputation to the brand and interests
- Global investigations
- Regulatory and environmental risk specific to the business
- Geopolitical risk
- New market entry analysis
- Supply chain resiliency

While open-source intelligence analysis and collection strategies answer many of these disciplines, they are often fragmented and rely on disparate, non-integrated platforms. Security leaders need to assure business executives' collection strategies are ethical and legal, and therefore, outcomes and output become the primary focus.

Open Source Intelligence Coverage to Chief Security Officers

Open source tools are critical to support all of these programs in a variety of ways, including:

1. **Open-Source Research and Analysis:**
   - Keyword alerts and analysis to give predictions of what's happening in the future.
   - Geolocational, event-driven, open-source intelligence specific to an area that predicts how quickly an incident can be remediated.
   - Creative research, scraping, collection of data breaches, closed and dark web forums.

2. **Technical Signature Analysis:**
   - Technical data sets such as mobile data, Netflow, and passive DNS to enrich content such as threatening emails or social media against executives.

3. **Direct Threat Actor Engagement:**
    - Engaging with threat actors to extract more context to the problem that needs to be solved.

Collection and Intelligence Strategies

The corporate security teams are still not bringing information together in a single platform, and are dependent on individual tooling. Corporate intelligence teams need to provide a collection strategy that has overlapping efforts against the mandates covered in the nine disciplines above:

- Collect against the mandate set by the board of directors and provide clarity in a murky environment to reduce risk.
- Breakthrough siloed business areas and brought them together based on the risk picture. Ensuring the right questions between business units is an essential function of the corporate security team.
- Try and provide next week's intelligence and news today for executives. Constantly making better intelligence consumers out of executives is an evolving process for even mature security teams.

Three Core Areas to Model a Collection and Intelligence Strategy

- **Information Requirements:** What do customers need to know, and when do they need to know it?
- **Framework and Structure:** Tactical and strategic plan that discusses requirements to collect and understand the outcomes for success.
- **Relationship and Deals:** Companies and vendors contracting for data or finished intelligence answers to understand if a security team needs more data (aka fire hoses) or more magnifying glasses (technology and people that derive the answers from data).

Executive Buy-In For Corporate Security Programs

The best corporate security programs are similar to entrepreneurs trying to sell their programs to business executives. This means the security leaders need to know the business and speak the executive's business language. Security needs to get out of the mindset of control and enforcement and transition to business enablers through ethical and legal collection strategies.

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.