NISOS

Webinar Brief

Digital Executive Protection: Reduce Risk and Stop the Attacks

Executive Summary

When combatting online threats to executives, employees, facilities and assets, the typical response from executive protection teams consists of physical, procedural, and technical security protocols (guns, guards, gates).

It’s almost impossible, and often unnecessary, to provide 24x7 physical protection for every online threat. Determining the online risk profile and validating intent and viability are critical to identifying genuine and problematic threats.

Online Personal Identifiable Information (PII) Proliferation

PII continues to be available online from multiple sources, such as people search sites that aggregate information from major data brokers. Legally publicly available information including, but not limited to, utility records, voting records, property records, and campaign donations are scraped, aggregated, and sold on the internet. Other commonly “scraped” PII comes from posts within social media accounts and data breach information and can be bought on the dark web.

Removing PII from Chan boards, dox sites, and Kiwi Farms (formerly known as CWCki Forums) is difficult. It is important to proactively monitor sites for the purpose of understanding what information remains available. It is also important to understand that removing it once will not prevent it from resurfacing or being reposted.

To establish an effective digital executive protection strategy, you must be prepared for the technology challenges of keyword matching, evaluating metadata from content, and detecting relevant images.

Anyone with a Life to Live Has a Pattern of Life

Executives, their family members, and their close associates are often targets of exploitation and their PII is routinely weaponized for malicious purposes. There are two approaches to helping protect these individuals:

- manually reducing the quantity of online profiles and presence through PII reduction techniques, and
- training executives in online best practices that help them self-monitor for risky behavior.

Information that contains personal selectors (phone numbers, email addresses), personal data (date of birth, social security number), and personal characteristics (name of high school, pet names, route they take their kids to school) are often used as a means to facilitate harassment and fraud campaigns.

Context and Collaboration is Critical

Executive vulnerability assessments should not focus exclusively on easily accessible PII. Assessments should also identify information that can be used to facilitate a variety of threat types. This comprehensive approach requires collaboration with executive teams to distinguish how a harassment campaign could differ from a fraud campaign.

For example, a disgruntled former employee may target a holiday party that is posted online, whereas PII on the internet could lead to a stolen identity used to apply for a fraudulent mortgage or credit cards.

Collaboration between executive teams, executive protection teams, partners, law enforcement, and vendors is critical to establishing a smart defense against malicious actors.

The Case for Unmasking an Attributing Adversaries

In closing, it should be noted that attribution and unmasking may ultimately lead to the strongest deterrence and the ultimate cessation of malicious activity.

Examples of this working effectively include:

- Contacting the perpetrator, their family members, or their employer and identifying the activity and requesting it be stopped
- Conducting a law enforcement “knock and talk”
- Rolling back anonymity by filing civil lawsuits and sending cease and desist letters
- Working with law enforcement to prioritize prosecution

For more information or to check out our latest webinars, visit www.nisos.com/library.

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 cyber attacks, disinformation and abuse of digital platforms. For more information visit: **www.nisos.com**