NISOS

A Practical Guide from Nisos®

Threat Intelligence Buyer's Guide - Executive Protection

To stay ahead of risks to your executives, you need intelligence about emergent threats whenever and wherever they arise. This buyer's guide will outline alternatives for executive protection solutions and highlight the things to consider when building a program.

Executive Summary

Corporate security and executive protection teams have an important job when it comes to defending and protecting company VIPs and key personnel. The responsibility for protecting those individuals typically falls to physical security teams, who have limited visibility into threats in the digital space. Yet, often the first sign of an impending attack appears on social media, extremist forums, and the dark web.

Today's executives and their families are more exposed than ever. Sixty-nine percent of executives report a dramatic increase in physical threats.[1] Unsurprisingly, executives are 12x more likely to be targeted in a cyber-attack.

Threats to a CEO and their families can have the most impact on business continuity of all the physical risks businesses experience.[2] Despite all the evidence of this risk, few corporate security teams have the resources to identify threat actors targeting key personnel across digital channels.

Digital Footprint Dangers

FOCUS	DESCRIPTION
Pattern of Life Exposure	Details an executive shares via social media, interviews, and other digital channels make it easier for threat actors to establish a pattern of life facilitating stalking, surveillance, and harassment.
Doxxing	Doxxing refers to the intentional publishing of an individual's sensitive or protected identifiable information on the open internet. Doxxing is increasingly used to blackmail, threaten, and intimidate executives.
Credential Theft	C-suite credentials represent one of the most prized targets for hackers. Executives suffer from the same poor cyber hygiene as their subordinates. Password reuse and risky online site engagement are not uncommon.
Business Email Compromise	Attackers can dupe employees by posing as an executive or emailing a finance department member with an urgent request for a funds transfer. Despite cybersecurity education, employees continue to fall for these attacks.
Opinion Outrage	Expressing opinions on controversial issues can make executives the target of activists or hacktivists. Issues that may not relate to the business can cause outrage and motivate attacks.
Personally Identifiable Information (PII)	Unintended exposure of personal information continues to create a risk to executives. A wide range of data like utility records, voting records, property records, campaign donations, and more helps enable threat actors.
Impersonation and CEO Fraud	Fraudulent email, phone calls, text messages, and in some cases, deep-fake videos are used to prey on employees and associates of executives.

Executive Exposure is Exploding

In a data-driven world, the data of an employee or - even a private citizen reflects upon their employer. It can benefit the employer through goodwill and positive association, but it can also be useful to criminal organizations and threat actors.

What we buy, what we eat, our frequently visited locations, relationship status, and details about our close circle of friends are all valuable to a determined adversary.

What is PII?
Personally identifiable information is any data that makes it possible to directly or indirectly infer an individual's identity. Examples of personally identifiable information include:

Name	Full name, maiden name, mother's maiden name, or alias
Personal Identification Number	Social security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, financial account number, or credit card number
Address Information	Home address, work address, extended family address
Contact Information	Personal phone number, email address
Personal Characteristics	Identifying photographs, fingerprints, or handwriting
Biometric Data	Retina scans, voice signatures, or facial geometry
Vehicle Ownership	VIN number, license plate, or title number
Asset Information	Internet Protocol (IP) or Media Access Control (MAC) addresses

There are over 540 legal data brokers operating in the United States. Each of these data brokers collects and stores a massive amount of personally identifiable information (PII).[3]

- On average, 350 companies hold a person's PII
- 83% of an average user's data is held by a company they interacted with only once
- 32% of an individual's digital footprint required no account creation
- PII record exposure has increased 150% in the last two years
- The average employee provides PII to eight new companies per month
- As a result of their highly visible role, executives have on average, 15 to 20 percent more PII exposure than their employees.[4]

Keys Steps to Identify and Mitigate Executive Risk

EXPOSURE ASSESSMENT

New and increasingly sophisticated news and social media platforms increase the exposure of individuals and, if not properly monitored and managed, can do irreparable damage to an individual's reputation and impact organizations associated with them.

An exposure assessment will document the scope of an executive's digital footprint, identify active threats and concerning web chatter, and provide a thorough sentiment analysis to establish a baseline for assessing the individual's risk profile.

PROACTIVE THREAT MONITORING

Monitoring for threatening social media mentions and comments targeting key personnel and family members makes it possible to avert risks related to:

- Potentially disruptive activities targeting, in proximity to, or focused on individuals and their physical locations
- Illegitimate registration of social media accounts and domain names
- Threats to company employees, executives, assets, or facilities
- Compromised account credentials
- Posting of "Dox," digital dossier or personal details for a "C" Level executives on social media
- Indicators and warnings
- Executive vulnerability and PII exposure
- Adversarial campaign, petition, or divestiture commentary

SCREENING OF KEY PERSONNEL

Bringing new staff on board, whether through hiring or acquisition, can introduce new risks to an organization. An individual's online presence, social media activity, and breach history can reveal opportunities for attack.

An initial assessment of the individual risk profile allows clients to properly scope, analyze and mitigate risk before bringing them onboard.

PII REDUCTION AND REMOVAL

Over time, the amount of an individual's PII on the internet increases. Normal activity, leaks, breaches, and other exposure add to the information available.

PII removal reduces the exposure of key personnel by identifying and eliminating sensitive information across internet databases and sources.

Three Types of Executive Protection

Today's Executive Protection Intelligence offerings are typically provided via a software platform or by a consultancy that provides custom services focused on physical protection use cases. In order to effectively defend executives against risks, organizations need visibility into emergent threats wherever possible. Proper threat intelligence that reflects the convergence of physical and cyber domains is crucial to defending key personnel, averting crises, and avoiding security events.

EXECUTIVE PROTECTION SOFTWARE

Cybersecurity vendors have addressed the growing demand for visibility into threats against executives by developing artificial intelligence solutions that can rapidly scrape the open and dark web to identify threatening content, credential theft, and PII exposure.

Typically integrated into a SIEM or other management platform, these solutions can rapidly detect evidence of a breach. However, these technology tools and platforms often focus on speed while sacrificing accuracy, credibility, and depth for speed.

Pros:

- Highly automated
- Large data set
- APIs make integration simple

Cons:

- Lacks contextualization and correlation
- Data is not client-specific
- Thousands of alerts issued a day

Types of Executive Protection... continued

EXECUTIVE PROTECTION CONSULTANCIES

Corporate security teams often turn to consultants to help them manage the physical security of key personnel. Given the existing relationships, adding digital security to consultant offerings is appealing.

The right consultants can provide guidance on how to reign in your executive team's digital footprint and may even help with some takedowns of PII, but in general, consultancies are about providing moment-in-time advice for specific business challenges.

Pros:

- Client-specific
- Typically have strong familiarity with protective security use cases
- Less noise than software/platforms

Cons:

- Highly manual (slower to detect and respond)
- Costly
- Less experience in digital/cyberspace use cases

NISOS EXECUTIVE SHIELD Executive Protection as a Managed Service

Nisos Executive Shield is a Managed Service that helps protect key personnel with credible, reliable intelligence gathered through OSINT monitoring, analyst-led investigations, automated reporting, and digital human intelligence.

The scope of the service spans the protective, reputation, and cyber intelligence domains as reflected on social media, the surface, deep, and dark web.

Managed Intelligence services are a natural choice for businesses struggling to stay ahead of their complex threat landscape because they combine the best of software and consultancies. Managed Intelligence providers work as an extension of your team, providing businesses with targeted intelligence about your key personnel that goes beyond the simple scraping of the web.

Executive Shield is delivered by Nisos' expert team of analysts. The Pandion team uses their specialized skills in OSINT intelligence collection, research, and analysis to build custom queries tailored to client-specific risks and proactively tune them to ensure credible, actionable intelligence, threat identification, and mitigation.

	Software	Consult	Nisos
Open Web	■	■	■
Social Media	■	■	■
Dark Web	■	■	■
Public Records	■	■	■
Civil and Criminal Data	■	■	■
Domestic Media	■	■	■
PII Reduction (Automated)	■	■	■
Closed Forum		■	■
Foreign Media		■	■
Domain Monitoring		■	■
Threat Actor Engagement			■
PII Poisoning			■
PII Reduction (Manual)			■
Cost	$	$$$	$$

Sources:

1. https://www.wsj.com/articles/surge-in-physical-threats-during-pandemic-complicates-employee-security-efforts-11607432400
2. ONTIC 2022 State of Protective Intelligence Report
3. Privacy Rights Clearinghouse
4. Executive Personally Identifiable Information (PII): Managing Leadership Personal Information Risks - DeleteMe

Explore Nisos

Analyst-Led Threat Intelligence

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 or email info@nisos.com