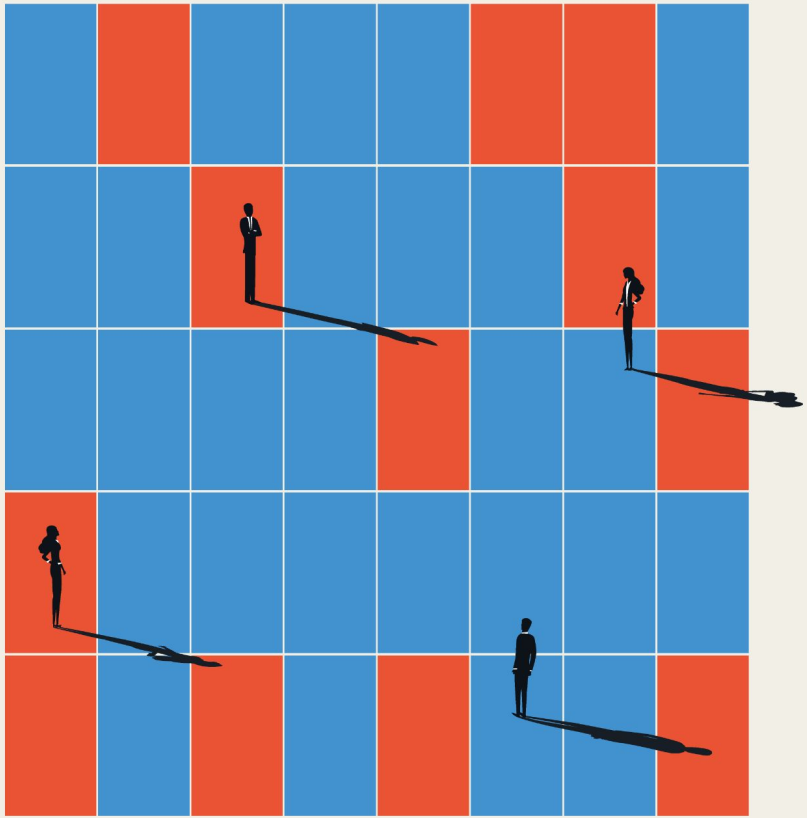
Case Study

Executive Protection

Mitigating Threats to Executives and Their Families

Nisos **uncovers significant threats targeting an executive and their family** from a financial services enterprise



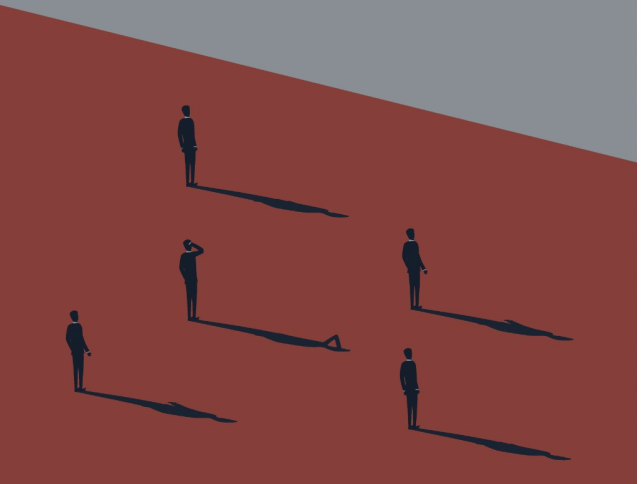
SITUATION

Identity theft and fraud are serious security issues that can plague executives and companies. Due to the wide availability of Personally Identifiable Information (PII) online, proactive measures need to be taken to protect high-profile individuals and their families.

A Client within the financial sector tasked Nisos with identifying vulnerabilities associated with a C-level executive after attempts of fraud and identity theft targeting the executive's family member.

The primary objective was to assess the risks associated with breached information, accounts for sale, physical location data, and their overall digital footprint.

INVESTIGATION



Looking to protect the executive's and the company's sensitive data, the Client tasked Nisos to assess the risks associated with the executive and their family member.

Nisos conducted a comprehensive analysis and found that both the executive and the family member had moderate risk profiles.

This assessment was based on several factors:

- Wide availability of physical addresses and contact information.
- Public images and family information shared on social media profiles.
- Inclusion of PII in breach data.

IMPACT

Assessing the extent of risk to the executive identified that the vulnerabilities for the C-level executive also extended to their spouse and children. This required a holistic approach to ensure the security of the entire family.

The vulnerabilities Nisos uncovered included:

- The executive's family members' social security number (SSN) was **found for sale on a dark web marketplace.**
- Both the executive and the family members' **PII was present on numerous websites** that required no payment or login credentials to access.
- A recent data breach of a financial institution was identified as a potential contributor to the fraud experienced. However, it was noted that the more likely cause was a threat actor **acquiring information through a deceptive phone call.**

Case Study

Executive Protection

Protecting CEO from Targeted Harassment

Nisos identifies **escalating harassment against a CEO** by recognizing threats, enhancing security, and safeguarding personal information

SITUATION

Executive harassment is an escalating risk in today's digital landscape, where threat actors can exploit multiple channels to target high-profile individuals. These campaigns can jeopardize personal safety and organizational security, making protective intelligence essential for mitigating threats.

A Client's CEO became the focus of persistent harassment from an unidentified individual. The aggressor used personal and business phone numbers, email addresses, and social media accounts to intimidate the executive.

As the harassment escalated, concerns grew around the CEO's safety and the risk of sensitive information exposure. To address these risks, the Client turned to Nisos to identify the perpetrator and help mitigate threats.

INVESTIGATION

Our protective intelligence and cyber threat mitigation expertise netted learnings that the client's team were unable to achieve on their own. Using advanced investigative tools, we conducted a comprehensive analysis to identify vulnerabilities and immediate threats targeting the CEO.

- **Executive Threat Assessment**: Our team conducted a thorough assessment to locate weaknesses, such as easily accessible personal information and vulnerable communication channels, that could be exploited by threat actors.
- **Proactive Mitigation Strategies**: Based on our findings, we advised on protective measures, including removing publicly available PII, strengthening communication security, and implementing ongoing monitoring to preempt future threats.

IMPACT

Nisos reduced the current and future risk to the executive, and by extension the Client's business.

With our support, the Client was able to develop swift and effective strategies to safeguard the CEO and their associates, helping to ensure their security.

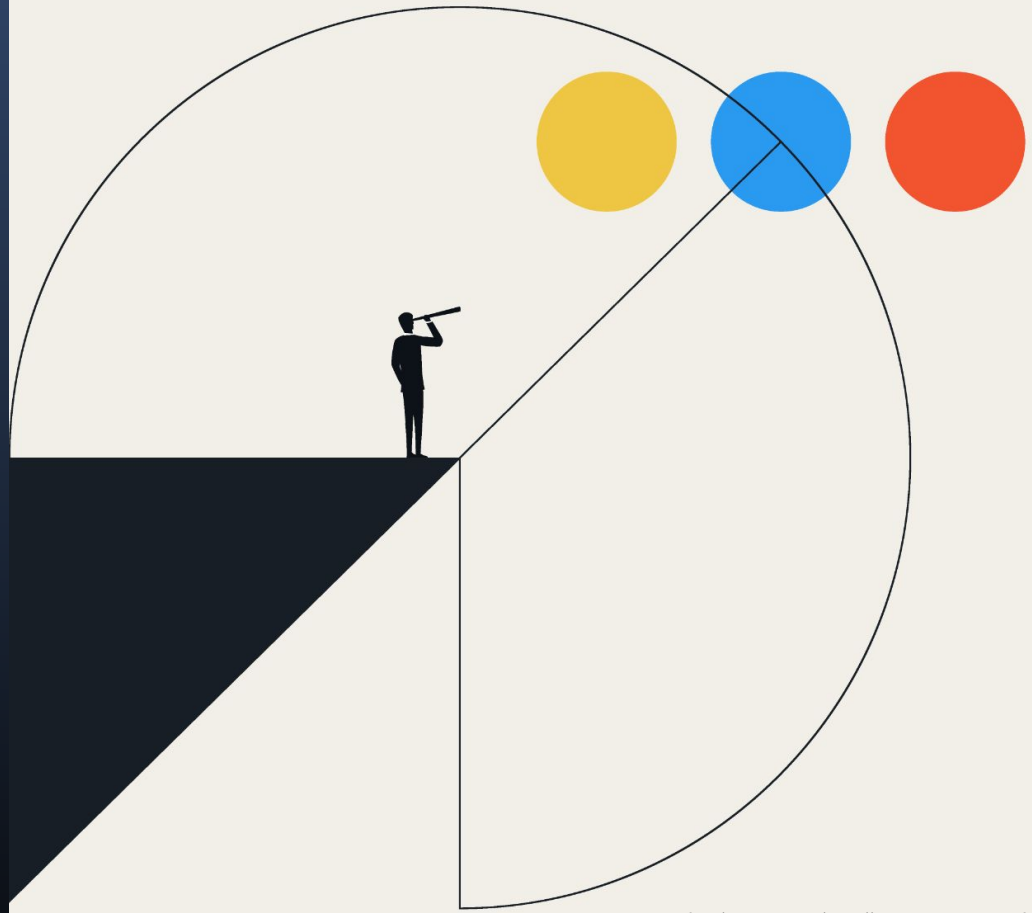
We continue to monitor the digital landscape - including the deep and dark web for the CEO's PII and emerging risks to help the Client's team stay one step ahead of threats and protect their executive team.

Case Study

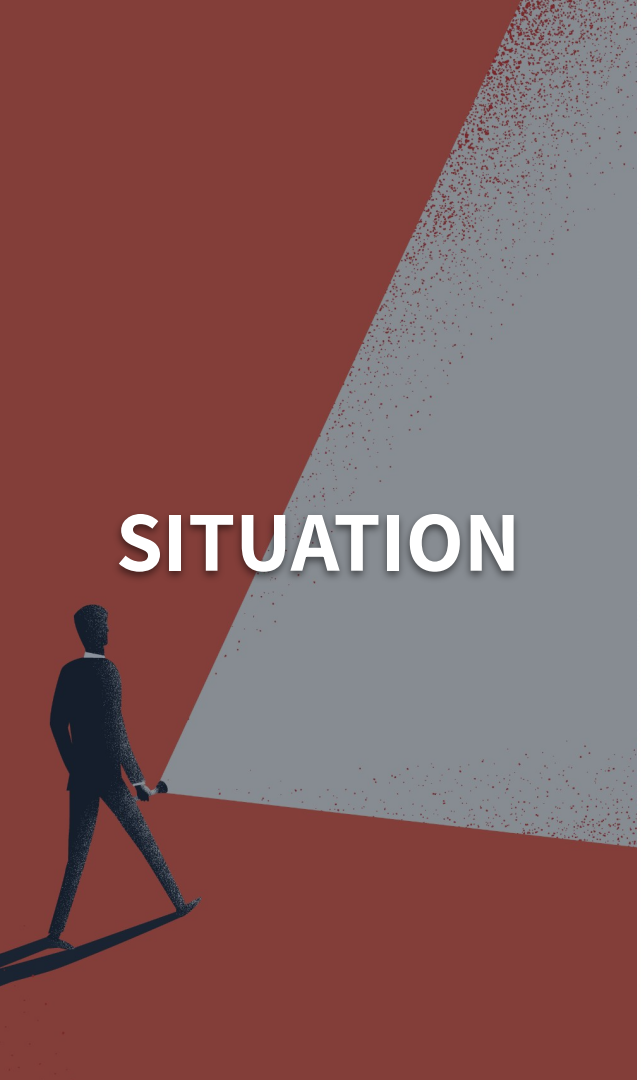
Executive Protection

Identifying and Protecting CEO from a Bomb Threat

Nisos' expert intelligence uncovered **hidden threats, and identified imminent risks** missed by a Client's security team



SITUATION



Physical security threats pose a significant risk to executives and their teams, with the potential to disrupt operations, harm key personnel, and damage an organization's reputation. Detecting these emerging digital threats and shutting them down before they become physical threats is crucial for protecting leadership and maintaining business continuity.

During routine monitoring of dark web, open web, and social media channels, for a Client, Nisos identified several imminent physical security threats to the CEO. These threats had evaded detection by both the Client's internal security team and their previous intelligence vendors. Nisos was tasked to identify the origin of these threats and assess the risk to the Client's teams.

INVESTIGATION

Nisos collected and monitored data across the digital ecosystem for visibility into deleted, updated, or altered content. Our data sources included social media sites, discussion groups, hacking forums, and deep and dark web marketplaces. Analyzing this data provided a comprehensive perspective on the threats targeting the Client's physical locations, networks, and personnel.

Our human-driven investigation involved a multi-step process in which we triaged alerts, and analyzed profiles related to Persons of Interest (POIs) and Groups of Interest (GOIs).

We uncovered bomb threats directed at the Client's executive team in deleted posts on social media channels. The severity and frequency of these threats prompted the Client to engage Nisos to attribute the individuals responsible, and ultimately refer the findings to law enforcement.

Identifying patterns and prioritizing threats based on their likelihood of materializing, we provided the Client with actionable intelligence, so they could respond quickly to proactively mitigate the risks before they could escalate into a real-world security incident.

IMPACT

The timely identification and mitigation of these threats prevented potential harm to the Client's executives and team, safeguarding both their physical security and the organization's reputation.

Nisos enabled the client to take a number of actions to shut down the threat, reduce their risk, and mitigate future threats.

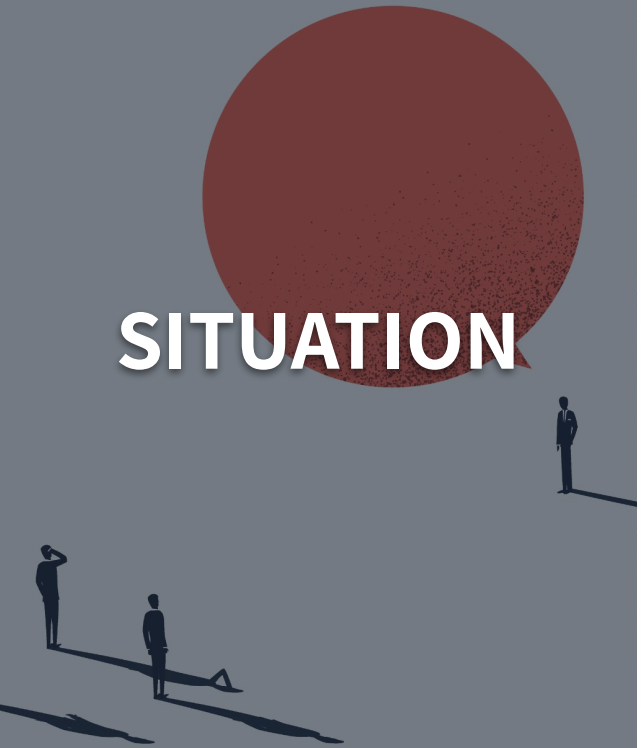
- **Pursue action with law enforcement and develop internal watch lists to proactively and reactively address physical threats:** Nisos identified bomb threats and direct threats to the client's executive team, and provided the Client with actionable intelligence.
- **Implement monitoring services, a periodic netflow review, and freeze executive's credit:** Nisos discovered the sale of the CEO's social security number on deep web markets and uncovered potential attempts to compromise the Client's digital infrastructure.
- **Swiftly protect executive team from threats:** Nisos made specific recommendations to reduce the likelihood of compromise to the Client's digital infrastructure, enhancing the Client's security posture and resilience against emerging threats.

Case Study

Executive Protection

Monitoring for Threats to Executives

Nisos provides overwatch for a major gig economy platform **whose CEO was the target of planned protests**



SITUATION

Executives and key personnel of controversial brands may find themselves targets of protests and harassment, online and in person, instigated and organized behind digital closed doors.

When a Client was alerted to ongoing chatter on social media channels organizing a protest at their CEO's residence, they were concerned that the event could turn violent, and contacted Nisos to assess the risk.

Nisos discovered social media pages created by a fringe political organization that promoted events targeting the Client and their executives. In addition to the one flagged by the Client, other events were being organized by the group also targeting the Client's employees.

INVESTIGATION

Nisos monitored the social media pages of several fringe political organizations targeting the Client. No mentions of the organizations were discovered on the deep or dark web, suggesting the accounts were new, and not part of public leaks.

Although the threat actors posts about the protest event received little interaction, the organizers hosted a public video meeting several days before the event to prepare potential participants.

Nisos assessed that the event was unlikely to turn violent given the lack of violent rhetoric, and minimal interaction with the social media posts themselves. A closer examination of the individuals managing the social media pages revealed that most shared a common background and education.

As a result of our work:

- The Client and their CEO had a full understanding of the planned protest, and confidence that it was unlikely to cause any physical risk to themselves or their family.
- The Client was made aware of other political organizations generating chatter about the Client, and their relationship to the initial organization.
- As a preventative measure, Nisos was asked to continue to monitor social media, and the deep and dark web for evidence of similar threats.

Let's **Connect**

Nisos is the Managed Intelligence Company®. Our services enable security, intelligence, and trust and 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.
Learn more at **nisos.com**.

For more information:

visit: www.nisos.com
email: info@nisos.com
call: +1-703-382-8400
follow: LinkedIn