Client Outcome

Engaging Protective Intelligence

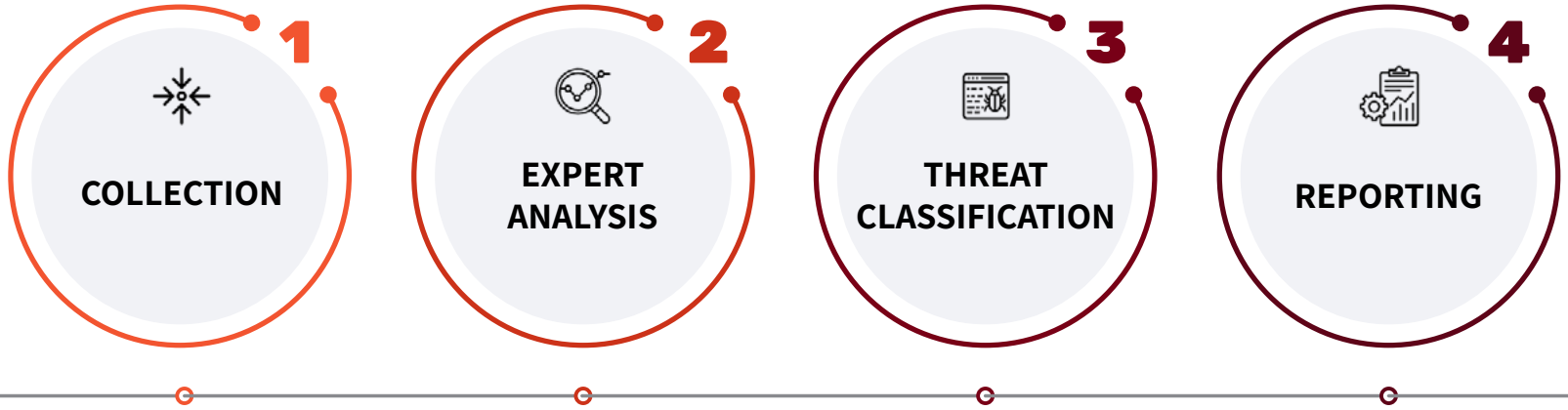
Nisos OSINT Monitoring and Analysis Service Identifies Bomb Threats Resulting in Law Enforcement Action

Overview: During routine digital protective intelligence monitoring of threats in the dark web, open web, and social media channels, Nisos identified several near-term physical security threats not previously identified by a large financial institution's security team or their previous intelligence vendors. Discovery by Nisos allowed the client to proactively defend their CEO, physical assets, and provide meaningful information to law enforcement.

Differentiated Approach: Nisos continually collects data to ensure we have coverage of deleted and updated or altered postings on social media. Our scope of a wide range of social media sites, discussion groups, hacking forums, and deep and dark web marketplaces provides an optimized view of threats to our clients, their physical locations, networks, and personnel. Instead of one large generic set of data, we collect from numerous small but deep data lakes that are specific and relevant to the client's intelligence requirements.

This exhaustive coverage of deleted posts in key social media channels allowed Nisos to discover bomb threats and direct threats to the executive team of our client. The severity and consistency of threats was enough for the client to request we pursue, identify and attribute individuals of on-going interest and refer our findings to law enforcement.

Our Process:



Our Process and Findings:

Step 1: Collect

- Nisos implemented recurring searches to monitor and alert for relevant terms and phrases associated with the client

Step 2: Expert Analysis

- Triaged alerts were analyzed to help identify plausible threats
- Profiles related to Persons of Interest (POIs) and Groups of Interest (GOIs) were examined for current and historical activity
- Newly developed personas were used to infiltrate the deep web, including private groups and forums, that automated systems are unable to penetrate and require human interaction

Step 3: Threat Classification

- Previously and newly identified POIs and GOIs were prioritized and added to a maintained Master Threat List for ongoing persona-based investigation and engagement

Step 4: Reporting

- Threat intelligence, including trends, active/latent threats, and new and existing POIs and GOIs, was shared with the client at regular intervals

Category	Findings
People and Groups	▪ User postings that implied an intent to call in a bomb threat to Client HQ for the purpose of disrupting operations ▪ Two additional posts indicating a desire to “bomb client company name” ▪ Numerous “people of interest” warranting tracking for any potential escalation ▪ Public and private groups on Reddit, Telegram, Discord, Facebook, and other forums sharing fanatical and threatening posts
Hacking Forum and Deep/Dark Web Mentions	▪ Client CEO’s social security number (SSN) was for sale on at least four deep web markets and determined likely listed by the same individual(s) ▪ Thread on a dark web forum requesting a link to a website accompanied by unfounded allegations that the client conducts illegal trading ▪ One user on the dark web forum Exploit[.]in posted a job seeking someone to perform takeovers of specific websites, including that of the client... No responses to the thread were found
Online Exposure and Sentiment	▪ Fluctuating volume of online mentions of the client ▪ Reddit having more and more users view the client as an enemy in their self-proclaimed “war”
Digital Threats	▪ Remote assistance page leaking information about support associates employed by the client ▪ Named firewall in a US city leaking the physical location ▪ Large quantities of DNS traffic resolved to IP addresses in named countries of interest in netflow samples taken quarterly ▪ Client’s employees with GitHub accounts identified and confirmed in hundreds of repositories... No client proprietary code was identified

Recommendations:

Nisos recommends the following best practices to:

- Reduce the likelihood of a compromise to the client's digital infrastructure,
- Identify and mitigate physical threats, and
- Minimize the client's overall threat landscape.

Credit Freeze/Monitoring

Mitigate theft of CEO's identity by executing a client-initiated full credit freeze and real-time credit monitoring service.

Exec Vulnerability Assessment(s)

Gain insight into vulnerabilities specific to key individuals and their close family and social network.

Executive PII Removal

Remove PII related to executives and other personnel from data marketers, data brokers, and people search sites.

Physical Asset Protection

Monitor and review versions and configurations of all equipment and the removal of references to physical addresses or employee names in public facing infrastructure.

GitHub/Collaboration Site Review

Examine employee GitHub as well as other collaboration sites related to its employees.

Periodic Netflow Review

Identify sources of anomalous DNS traffic.

Impact: As a result of our research and analysis, the client was able to gain a clearer understanding of online sentiment and threats from users on social media and the deep and dark web. The client used our intelligence to develop internal watch lists and coordinate with law enforcement to address physical threats, of which they were previously unaware.

Learn more about Nisos, the Managed Intelligence Company™ by visiting www.nisos.com. If you need immediate help, contact us: info@nisos.com or 703-382-8400.