Case Study

Employment Shield

Investigating Nation-state Employment Fraud

Nisos **uncovers North Korean state actors gaining employment** at major tech platform company

SITUATION

Employment fraud presents significant risks to businesses, leading to financial loss, security breaches, and damaged reputations. Fraudulent employees accessing sensitive information can undermine organizational trust, especially in remote work environments where vetting processes can be more challenging.

North Korean IT workers have been known to pose as non-North Korean nationals to infiltrate businesses, funneling funds to the DPRK's economic and security efforts. In 2022, the U.S. government issued warnings about North Korean IT workers using fake identities to secure jobs and fund illicit activities.

Fearing an insider threat, a Client and their legal counsel engaged Nisos to investigate several former employees who provided false documentation to obtain employment and exhibited suspicious behavior during their time with the company. Nisos was tasked to investigate the former employees to uncover any relationship with criminal or nation-state organizations.

Client counsel engaged Nisos to investigate potential links to criminal or nation-state actors and to provide guidance on responding to a security incident.

A team of Nisos experts analyzed the information provided by the Client, including background logs, email addresses, IP addresses, and social media accounts related to the subjects.

- **Nisos found the subjects used falsified identity documents,** and copied specific language from the resume of another, unrelated individual.
- Several application IDs connected to the subjects' email addresses and IP addresses used at login have **also been used by North Korean threat actors.**
- Despite claiming extensive work histories, **there is only a limited online presence for the subjects**, including a LinkedIn account, two GitHub accounts, and a Slack community.
- Nisos investigators **attributed two individuals** who were likely associated with the person of interest based on social media and US-based address association.

The individuals discovered are part of a growing effort by the DPRK to exploit remote work to fund the DPRK's weapons development programs, as well as steal intellectual property (IP) and other sensitive information on behalf the regime.

- **Legal and Law Enforcement Action**: The investigation resulted in actionable intelligence that supported law enforcement efforts to pursue legal action against the individuals involved.
- **Enhanced Security Response**: By working alongside legal counsel and law enforcement, Nisos supported the Client in reinforcing their security posture against future exploitation attempts.
- **Compliance:** By terminating the employment of the fraudulent employees, Nisos helped the Client to avoid sanctions and regulatory fines.

Case Study

Employment Shield

Nisos Uncovers Potential Employment Fraud Risks

Nisos investigation reveals an employee's **misuse of company resources for personal gain**

Employment fraud can take many forms, from conflicts of interest to misuse of company assets for personal gain. When employees have access to company resources, it's crucial for organizations to implement effective detection methods for compromised operations. Addressing these issues proactively not only protects an organization's assets but also ensures long-term integrity.

A Client who suspected that an employee might be using their position within the company to benefit for personal business ventures tasked Nisos to investigate.

The objective was to investigate any potential fraudulent activities, misuse of company resources, or conflicts of interest that could impact the Client's operations and business integrity. Through open source intelligence (OSINT) methodologies, the investigation aimed to gather sufficient evidence to guide the Client to take appropriate actions.

Nisos researchers applied a range of OSINT methodologies, including data aggregation, social media analysis, business registration research, and criminal record verification. The investigation aimed to provide a comprehensive view of the employee's professional and personal activities, focusing on potential conflicts of interest and fraudulent use of Client resources.

- **Undisclosed Business Ventures:** The employee was found to be involved in several personal business ventures that were not disclosed to the Client, their employer. Some of these ventures directly competed with the Client's business, suggesting a clear conflict of interest.
- **Misuse of Company Resources:** The investigation identified that the employee had accessed proprietary company systems on multiple occasions, often coinciding with activities related to their personal ventures.
- **Unreported Revenue Sources:** Financial records pointed to income linked to the employee's personal business activities, which had not been reported to the Client.

The investigation provided valuable insights into the employee's activities, revealing multiple potential areas of concern regarding employment fraud and misuse of company resources. This enabled the Client to make informed decisions about next steps.

While there was no direct, indisputable evidence of employment fraud, the findings strongly suggested that the employee was involved in personal ventures that could jeopardize the Client's business interests.

The discovery of conflicts of interest and the use of company systems for personal business highlighted substantial risks to intellectual property and company operations. Based on the findings, Nisos recommended further internal audits and reviews to confirm the extent of the misconduct and ensure the protection of the Client's assets.

Case Study

Employment Shield

Employee Assessments Reveal Potential Risks

Nisos investigation **identifies potential risks** through employee background and online activity

SITUATION

Employee risk assessments are critical for identifying threats to a company's security, reputation, and intellectual property. As businesses grow globally, especially in sensitive sectors, it's essential to evaluate employees for connections that could compromise organizational integrity. Assessing ties to foreign governments or questionable affiliations helps prevent risks like espionage, data theft, and compliance issues.

A Client approached Nisos with concerns over a specific employee who had shown signs of potential security risk, including possible connections to the Chinese Communist Party (CCP).

The objective was to conduct a comprehensive investigation to determine any links that might pose a risk to the organization's intellectual property or security posture.

INVESTIGATION

The employee's background was scrutinized, including their academic history, professional network, and online presence, to uncover any indirect associations or activities that could suggest a threat. The investigation aimed to provide a comprehensive view of the employee's risk profile, addressing concerns about foreign influence and potential impacts on corporate security.

- While no direct evidence of affiliation with the CCP was uncovered, the employee's academic background at Tsinghua University raised potential concerns regarding indirect influence.
- Several mainstream media mentions were found in Chinese news outlets that primarily focused on the employee's academic achievements. Engagement with CCP-friendly outlets and social media raised questions about potential ideological alignment, though no definitive evidence was found.
- Social media analysis showed the employee maintained an active presence across multiple platforms, with the most frequent activity on LinkedIn. Research found minimal interaction with CCP-related content, though a few instances of engagement with pro-China material may warrant further scrutiny.

IMPACT

The investigation did not uncover direct evidence of CCP ties but highlighted several possible red flags, particularly the employee's academic background and occasional engagement with CCP-friendly content. The employee's network included individuals in high-tech industries.

While no immediate action was deemed necessary, the findings suggested the need for continued monitoring, especially regarding the employee's professional network and social media activity. The Client concluded that ongoing monitoring was warranted and engaged Nisos for further analysis.

Case Study

Employment Shield

Protecting National Security Through Intelligence Investigations

Nisos uncovers unauthorized access to **controlled sensitive information** and mitigated potential risk

SITUATION

Employment fraud and unauthorized information access are critical challenges many organizations face today. As cyber-physical threats evolve, malicious actors increasingly exploit employment channels to access or share restricted data that could compromise national security.

Nisos was tasked with identifying an individual who had been behind the posting of a controlled unclassified military document on an online forum which posed a potential risk to the U.S. government.

Our investigation aimed to determine if the person responsible had access to controlled unclassified information and potentially classified data, and to assess any associated risks.

INVESTIGATION

Nisos analysts conducted a thorough investigation into the online activities and affiliations of the individual in question. Our experts traced the individual's online footprint, analyzing their interactions on forums, previous posts, and any professional affiliations that could suggest access to restricted information.

- **Unauthorized Document Posting:** The individual posted a controlled unclassified document related to equipment testing for an aircraft on a public forum. This post included sensitive details that, while unclassified, were restricted under distribution laws, raising red flags around potential regulatory breaches.
- **Military Background and Employment:** Our analysis attributed the post to a user with a military background, now employed in the private sector.
- **Recovered and Analyzed Content:** The Nisos team traced the origins of the document to the Defense Technical Information Center (DTIC). Posting the document on a public forum could be considered a violation of the International Traffic in Arms Regulation (ITAR) which constituted a serious breach of regulations.

IMPACT

Our findings confirmed the individual had access to controlled unclassified information from the DTIC, although we found no concrete evidence of access to classified materials stored on the Secure Internet Protocol Router Network, a network for secure, classified communication.

Although there was no evidence of access to classified information, the posting of restricted documents on a public forum posed potential security risks. Nisos recommended that further investigation may be required to determine the full extent of the individual's access to sensitive information and to mitigate any potential threats to national security.

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