NISOS

Marketing Research

Insider Threat Intelligence Solutions Trend Analysis

September 2025

Table of Contents

Executive Summary **3**

Definition of Insider Threat **3**

Insider Threat Examples **3**

Workplace Conflicts 3

Polywork 4

Data Collection 6

Financial Pressures 7

Insider Threat Platform Solution **8**

Conclusion **8**

Executive Summary

Identifying potential insider threats requires vigilance and proactive monitoring of key behavioral, technical, and organizational indicators. Nisos' open-source intelligence investigations have increasingly complemented inside-the-firewall telemetry with externally focused risk and threat visibility at scale.

Nisos routinely partners with enterprise clients to investigate individuals with heightened risk profiles or reveal the identities of individuals responsible for insider threats. We identify and map networks advertising insider access or recruiting insiders at companies on mainstream and alternative social media platforms, cloud-based messaging applications, and dark web forums. Our investigations also include identifying threat actors who create fake identities to obtain employment with companies, which can lead to insider risk issues if not detected and investigated during the hiring phase of the employee lifecycle.

The following analysis details insider-threat risk indicators based on findings from our insider threat intelligence solutions. We also discuss our new platform, Ascend™, which enables our clients to quickly assess and mitigate potential insider risks.

Defining Insider Threat

Insider threat refers to a security risk that originates from within an organization, such as an authorized person abusing their access to and knowledge of an organization's resources, including personnel, facilities, information, equipment, networks, and systems, to harm that organization. This harm can include malicious, complacent, or unintentional acts that negatively affect the integrity, confidentiality, and availability of the organization, its data, personnel, and facilities.[1] Most of our client work has focused on malicious insider threats and supporting client security teams with outside-the-firewall intelligence solutions.

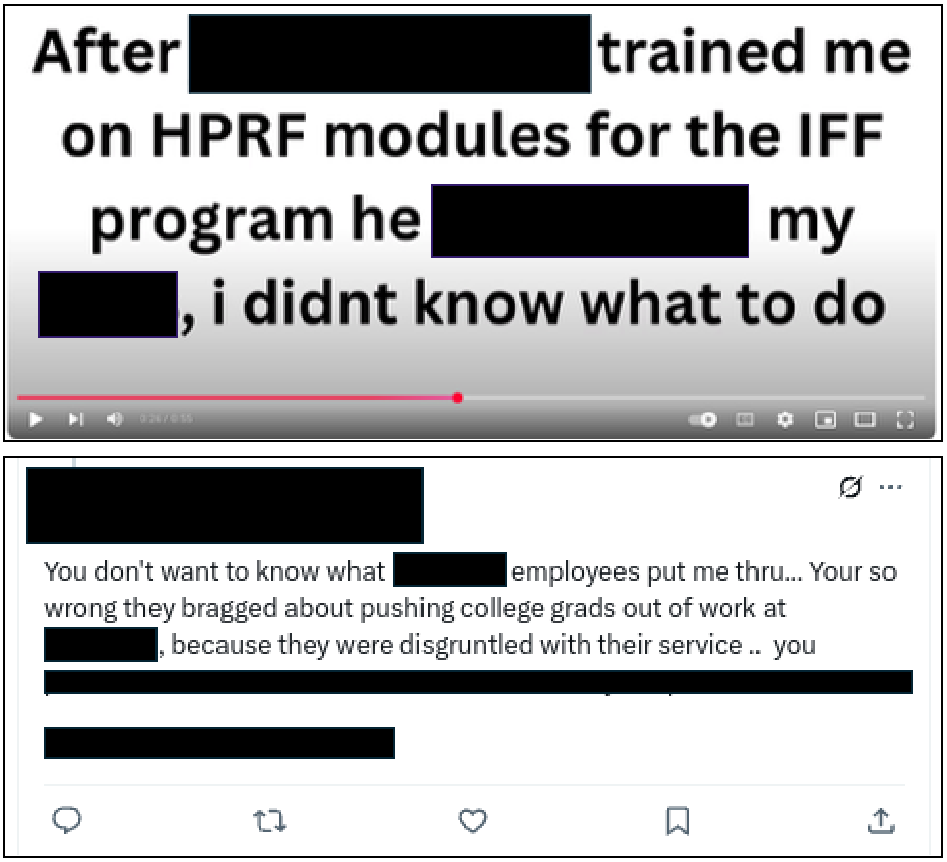
Insider Threat Indicators

Drawing from our detailed investigations into insider threats, Nisos has identified critical risk indicators surfaced in the digital realm that frequently signal the presence of an insider threat. These include workplace conflicts, undisclosed polywork arrangements, suspicious data collection activities, and employees under significant financial pressure. These indicators represent a sample of the comprehensive risk factors we continuously monitor through our sophisticated insider threat intelligence solutions, helping organizations proactively identify and mitigate internal vulnerabilities before they escalate.

[1] https://www.cisa[.]gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats

Workplace Conflicts

Individuals identified as insider threats frequently posted on social media about growing tensions with management or coworkers. These posts often occurred following negative performance reviews. In the following examples, individuals openly posted about their interactions with their supervisor and coworkers. Nisos combines expert-led investigation with outside-the-firewall intelligence collection to attribute social media accounts. This approach gives security teams insights to take action.



After [redacted] trained me on HPRF modules for the IFF program he [redacted] my [redacted], i didnt know what to do

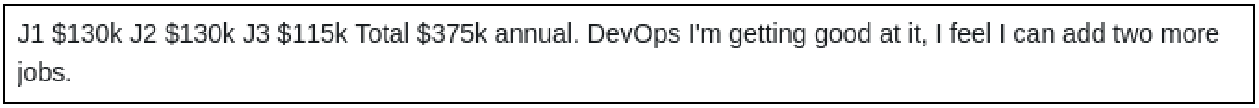
[redacted]

You don't want to know what [redacted] employees put me thru... Your so wrong they bragged about pushing college grads out of work at [redacted], because they were disgruntled with their service .. you [redacted]

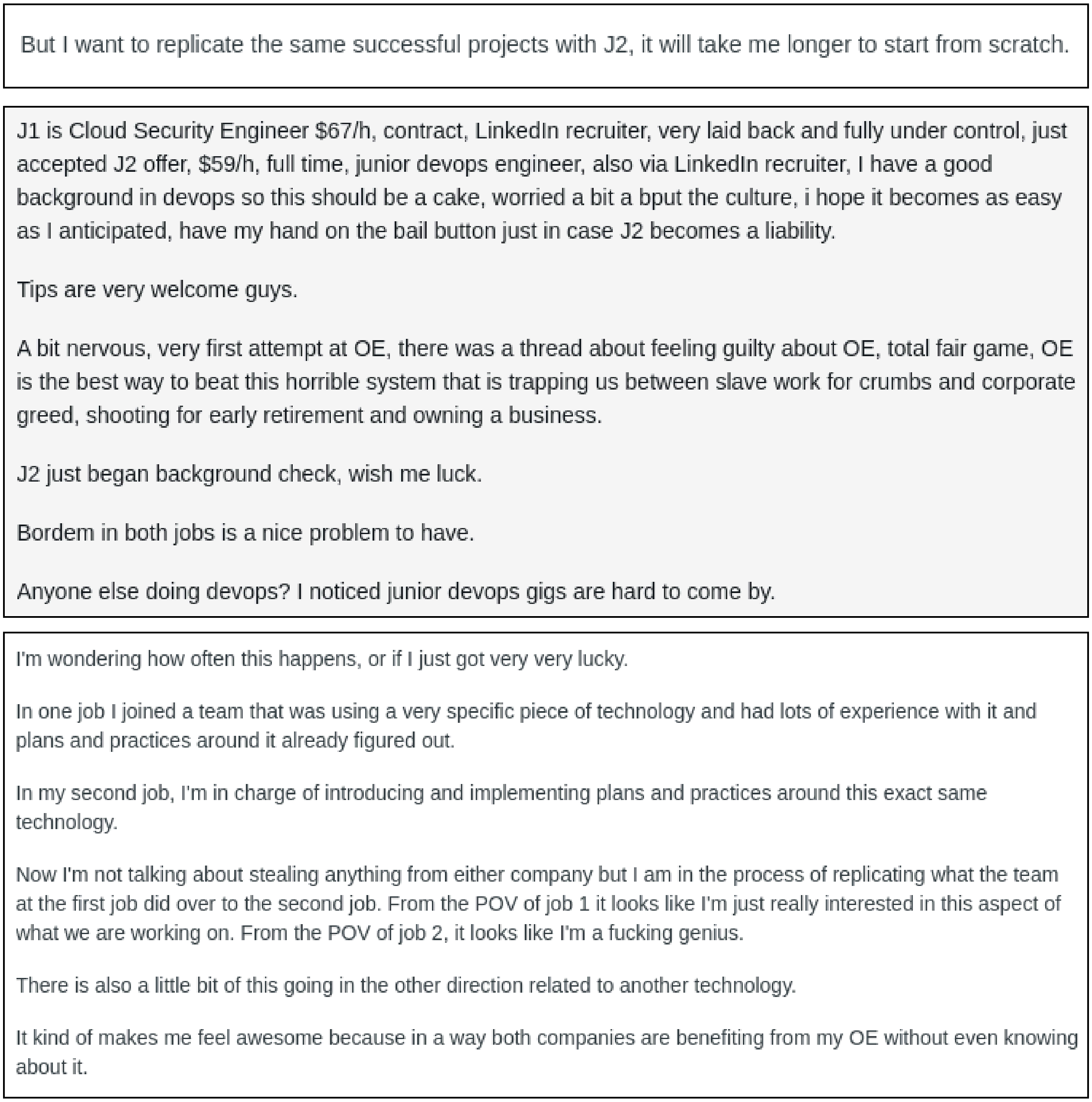
Graphics 1 and 2: Examples of social media posts about workplace conflicts.

Polywork

Individuals identified as insider threats often worked multiple full-time roles. When working multiple full-time jobs, individuals frequently shared sensitive company data or code between two companies to reduce their workload. Similarly, our investigations into the North Korean (DPRK) IT worker employment scheme showed that the same DPRK operator worked for multiple companies using the same or different fake personas. Due to their role in IT teams, DPRK IT workers were often given access to company code, intellectual property, and sensitive data, which they then attempted to exploit for financial gain once exposed. We can identify many of the risk indicators for polywork through open-source, pre-employment vetting.



J1 $130k J2 $130k J3 $115k Total $375k annual. DevOps I'm getting good at it, I feel I can add two more jobs.



But I want to replicate the same successful projects with J2, it will take me longer to start from scratch.

J1 is Cloud Security Engineer $67/h, contract, LinkedIn recruiter, very laid back and fully under control, just accepted J2 offer, $59/h, full time, junior devops engineer, also via LinkedIn recruiter, I have a good background in devops so this should be a cake, worried a bit a bput the culture, i hope it becomes as easy as I anticipated, have my hand on the bail button just in case J2 becomes a liability.

Tips are very welcome guys.

A bit nervous, very first attempt at OE, there was a thread about feeling guilty about OE, total fair game, OE is the best way to beat this horrible system that is trapping us between slave work for crumbs and corporate greed, shooting for early retirement and owning a business.

J2 just began background check, wish me luck.

Bordem in both jobs is a nice problem to have.

Anyone else doing devops? I noticed junior devops gigs are hard to come by.

I'm wondering how often this happens, or if I just got very very lucky.

In one job I joined a team that was using a very specific piece of technology and had lots of experience with it and plans and practices around it already figured out.

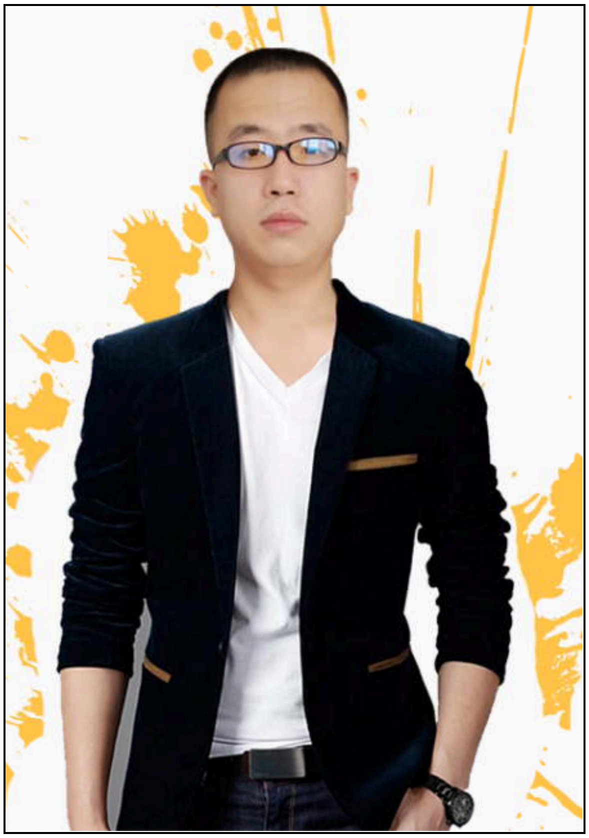
In my second job, I'm in charge of introducing and implementing plans and practices around this exact same technology.

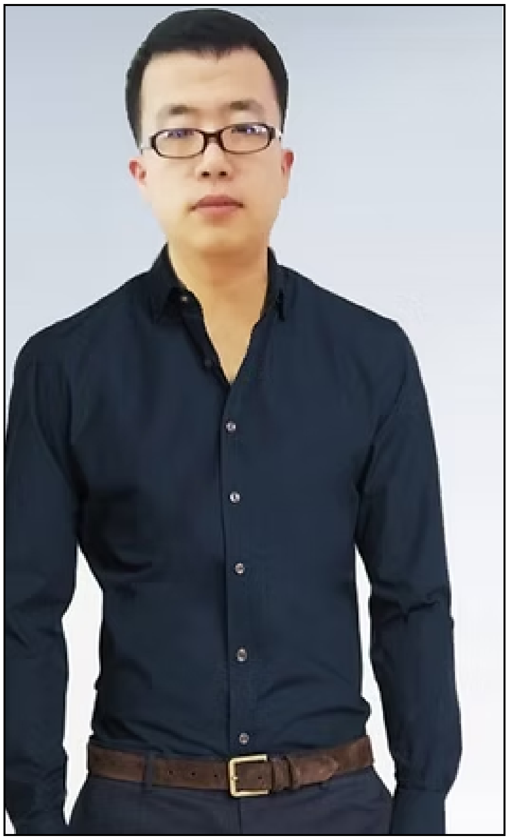
Now I'm not talking about stealing anything from either company but I am in the process of replicating what the team at the first job did over to the second job. From the POV of job 1 it looks like I'm just really interested in this aspect of what we are working on. From the POV of job 2, it looks like I'm a fucking genius.

There is also a little bit of this going in the other direction related to another technology.

It kind of makes me feel awesome because in a way both companies are benefiting from my OE without even knowing about it.

Graphics 3-6: Examples of social media posts about polywork.

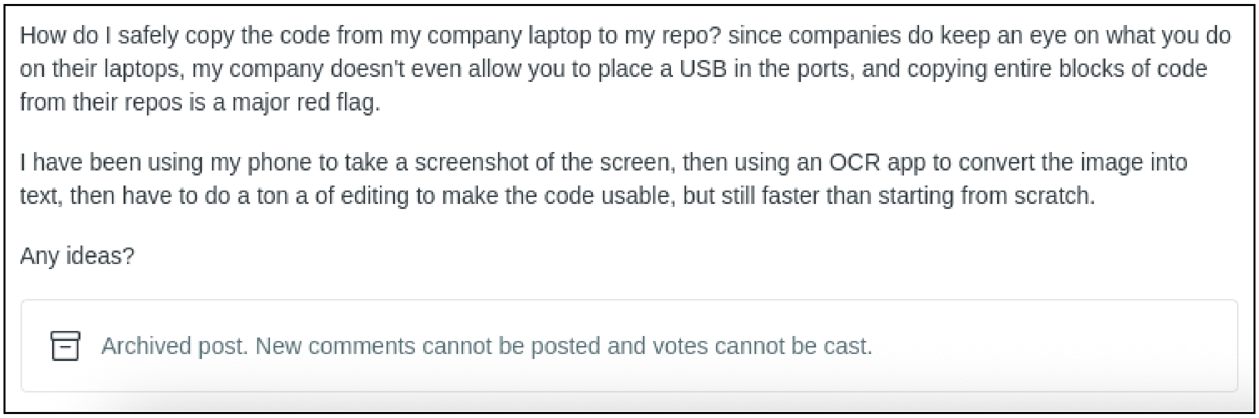




Graphics 7-8: Profile photos of the same suspected DPRK IT worker using different personas to gain employment.[2]

Data Collection

Individuals identified as insider threats frequently started collecting large amounts of company data or code into private repositories. In the following examples, individuals openly posted about their efforts to copy code from previous employers and attempts to circumvent security measures, including taking screenshots and using QR codes to transfer code.



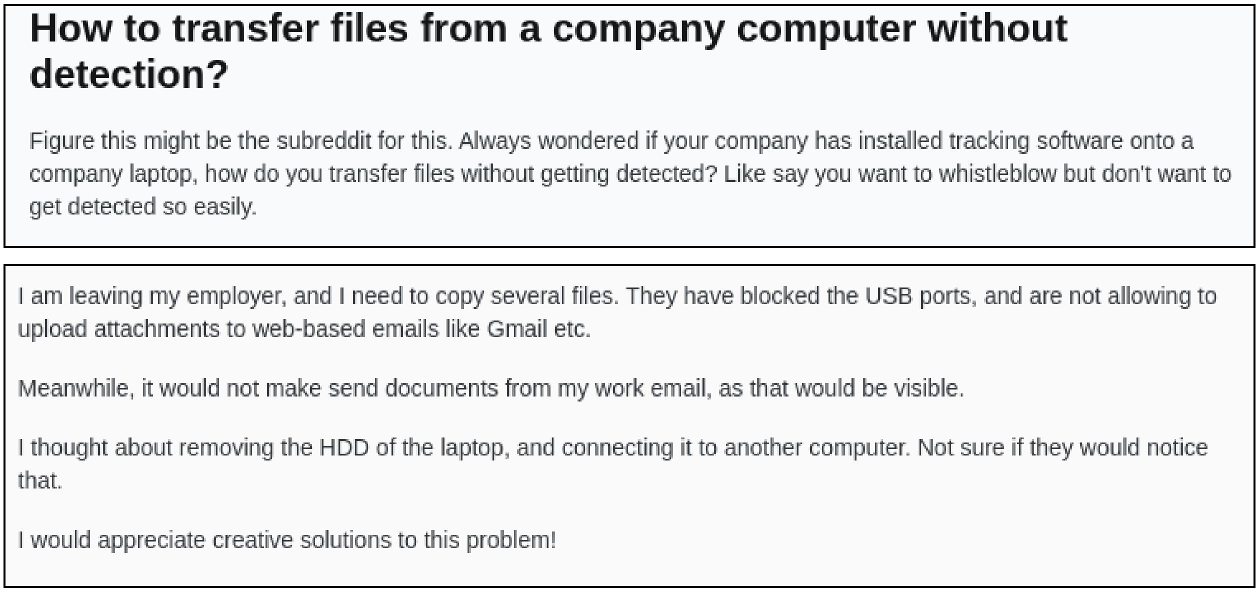
How do I safely copy the code from my company laptop to my repo? since companies do keep an eye on what you do on their laptops, my company doesn't even allow you to place a USB in the ports, and copying entire blocks of code from their repos is a major red flag.

I have been using my phone to take a screenshot of the screen, then using an OCR app to convert the image into text, then have to do a ton a of editing to make the code usable, but still faster than starting from scratch.

Any ideas?

Archived post. New comments cannot be posted and votes cannot be cast.

[2] https://nisos.com/research/dprk-it-threat-japan



How to transfer files from a company computer without detection?

Figure this might be the subreddit for this. Always wondered if your company has installed tracking software onto a company laptop, how do you transfer files without getting detected? Like say you want to whistleblow but don't want to get detected so easily.

I am leaving my employer, and I need to copy several files. They have blocked the USB ports, and are not allowing to upload attachments to web-based emails like Gmail etc.

Meanwhile, it would not make send documents from my work email, as that would be visible.

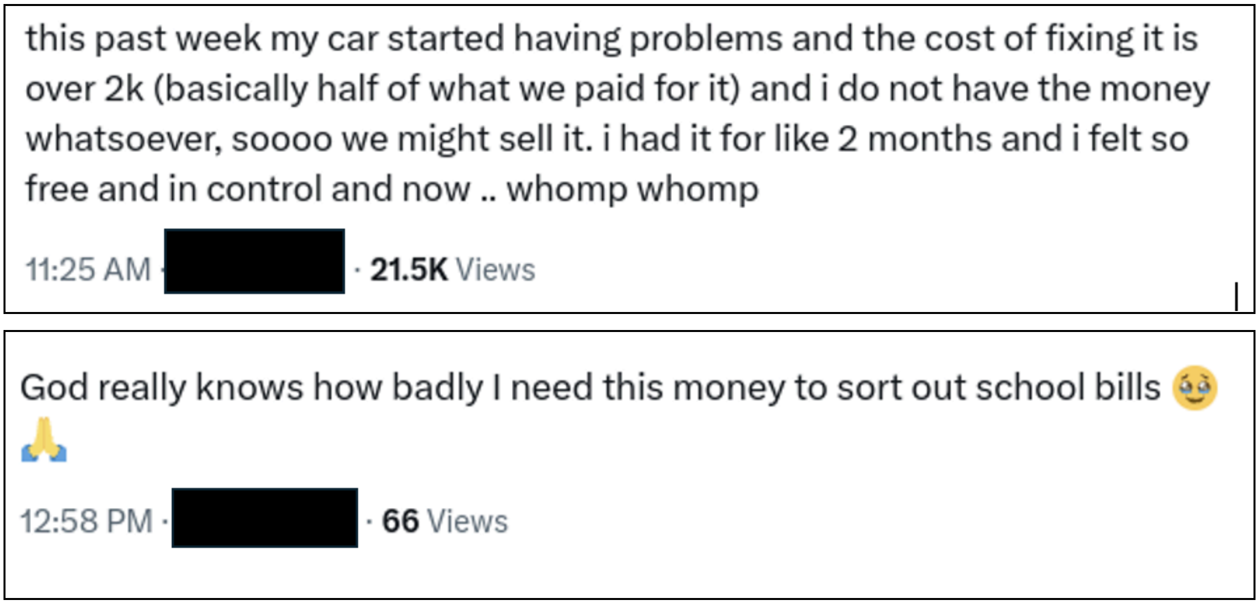
I thought about removing the HDD of the laptop, and connecting it to another computer. Not sure if they would notice that.

I would appreciate creative solutions to this problem!

Graphics 9-11: Examples of a social media post about data collection.

Financial Pressures

Individuals identified as insider threats posted about financial hardship, such as unusual financial stress or sudden changes in financial circumstance. In the following examples, individuals openly posted about their difficulties paying for car repairs and education fees.



this past week my car started having problems and the cost of fixing it is over 2k (basically half of what we paid for it) and i do not have the money whatsoever, soooo we might sell it. i had it for like 2 months and i felt so free and in control and now .. whomp whomp

11:25 AM · [redacted] · **21.5K** Views

God really knows how badly I need this money to sort out school bills 🥹 🙏

12:58 PM · [redacted] · **66** Views

Graphics 12 and 13: Examples of social media posts about financial pressures.

Insider Threat Platform Solution

Organizations often benefit from external resources to effectively identify and investigate human risks. Legal and regulatory restrictions can also limit an organization's ability to vet suspicious actors, uncover outside-the-firewall threats, and understand and remediate the damage caused. For nearly 10 years, Nisos has helped clients investigate insider threats with an analyst-led human risk management service designed to mitigate and prevent threats posed by partners, contractors, service providers, and other individuals conducting business with a client's organization. Based on our experience, Nisos has developed an insider threat module within our Ascend platform. Ascend's AI-powered capabilities provide our clients with intelligence-led risk assessments and monitoring at scale with sensitivity, scope, and urgency in mind. Nisos' insider threat intelligence solutions support clients by:

- Translating external risk signals into clear intent and investigation-ready insights.
- Identifying early risk signals by flagging polyemployment and policy-violating behavior before they escalate.
- Augmenting internal insider risk telemetry with outside-the-firewall intelligence. Social media posts, online activities, and sentiment shifts inform patterns and possible employee actions.

Conclusion

Insider threat mitigation requires insights from internal and external sources , especially in today's remote working environment. Enabling a trusted workforce and managing insider threats begins during the hiring process, to include risk assessments that identify online risk indicators. Our Ascend platform and deep insider threat investigation service provides clients with the resources to identify concerning indicators and threats early and mitigate risks at scale.