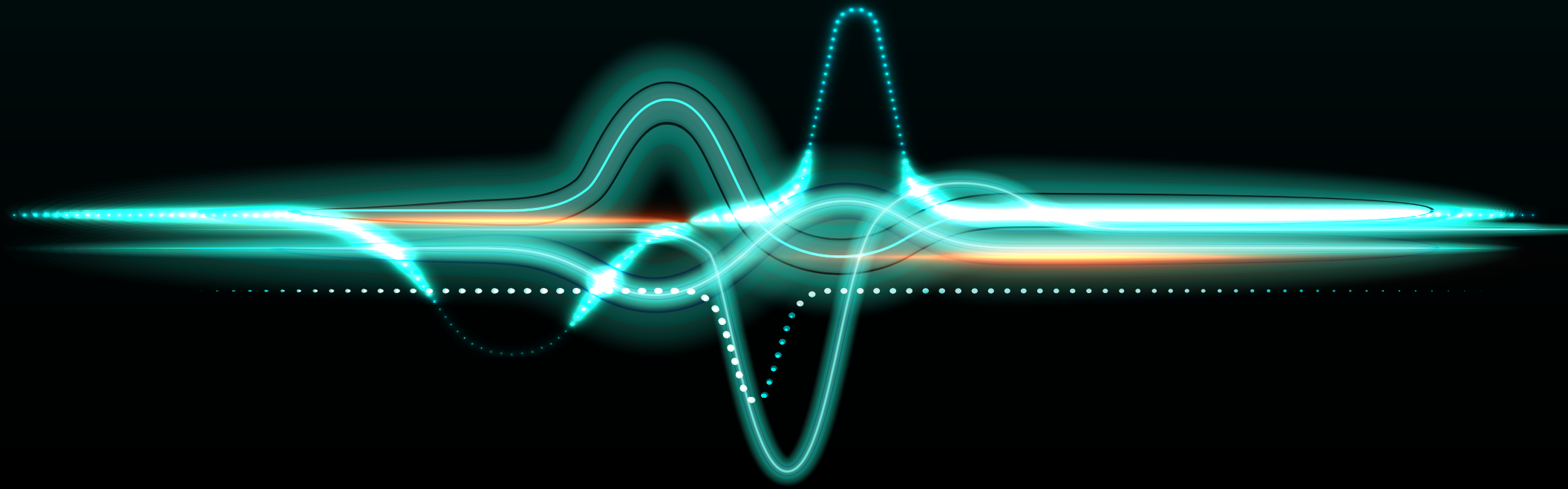
2025

SpyCloud

INSIDER THREAT
PULSE REPORT



Insider threats ***are a growing priority for security teams***, with over two-thirds of security leaders planning program enhancements.

But even teams with programs in place are struggling to close gaps and keep up with the scale of growing risks.

WHAT'S DRIVING THE INSIDER THREAT CONVERSATION TODAY

A letter from SpyCloud Co-Founder & CIO, Alen Puzic

Insider threats are commanding renewed attention in 2025, and for good reason. More than half of organizations experienced an insider-related security incident in the past year, putting these threats squarely in the spotlight for enterprise security teams.

While 64% of organizations now report having an established insider threat defense program, plenty of gaps remain as the threat landscape evolves. High-profile schemes, such as North Korea's fraudulent IT worker campaigns designed to infiltrate Western companies, have underscored the urgent need to revisit current strategies.

With insider risks becoming systemic and sophisticated – sometimes with ties to larger nation-state or financially motivated campaigns – now is a critical time for teams to reexamine defenses and reinforce approaches to addressing identity threats from within.

Alen Puzic

ABOUT THE DATA IN THIS REPORT

This report features insights from from a research survey conducted with 100 security leaders – 50 CISOs and 50 security managers/directors – across industries, at companies with at least 500 employees. The survey focused on how these professionals perceive, detect, and respond to insider threats.

Security professionals are unanimously concerned about both ***malicious*** and ***negligent*** insider threats.

HOW TEAMS ARE APPROACHING THE INSIDER THREAT PROBLEM

When we asked teams what they were more concerned about – malicious threats, meaning those who deliberately misuse data access, or negligent threats, meaning inadvertent threats like employees or contractors who fall victim to phishing or BEC attacks – they overwhelmingly said both.

97%
are concerned about negligent insider threats

93%
are concerned about malicious insider threats

TYPES OF INSIDERS

NEGLIGENT OR UNWITTING INSIDERS

These are individuals who put their organization at risk without meaning to – often by making everyday mistakes like clicking a link in a phishing email or ignoring a security policy. Their actions aren't malicious, but they can still open the door to account takeover, data theft, and other identity threats.

MALICIOUS INSIDERS

These actors deliberately misuse their access for personal gain or to cause harm. Think selling proprietary data, deleting critical files, or leaking credentials that enable follow-on attacks. Their motivations may vary – financial, personal, or ideological – but the outcomes can be severe.

Top 5 reported ***red flag indicators***

Here's a breakdown of the top 'red flag' indicators teams are using to identify potential insiders.

Security teams report taking a layered approach when it comes to insider threat indicators, monitoring for both technical and behavioral signals. While some organizations incorporate background check anomalies or personal stressors like financial hardship as early flags, these factors are typically seen as supporting details – not definitive indicators. Ultimately, detecting intent is much more an interpretive art than a precise science.

1

ANOMALOUS BEHAVIOR

Unusual access patterns, deviations from baseline activity, or data exfiltration attempts.

2

EXCESSIVE DATA ACCESS OR DOWNLOADS

An unusual number of downloads, large file transfers, or accessing sensitive data outside of job scope.

3

ATTEMPTS TO ACCESS RESTRICTED OR UNAUTHORIZED RESOURCES

Efforts to access or install things that are unauthorized or privilege escalation attempts.

4

SUSPICIOUS NETWORK ACTIVITY

Promiscuous internet usage or unusual network connections.

5

BEHAVIORAL CHANGES

Show of emotions during termination call or pattern displays of threats or anger.

The ***biggest challenge*** for security teams today lies in distinguishing insider threats from normal behavior amid alert overload.

The fact that more than half of organizations (**56%**) report experiencing an insider threat incident in the past year underscores that it's not just a theoretical problem – but rather a real and pressing concern for many enterprises.

64%
of teams have a defined insider threat defense program

Fortunately, more than half of teams (**64%**) also claim to have a defined insider threat program in place. Overwhelmingly, teams know where the risks lie but are struggling to react at speed and scale, universally reporting juggling a ***myriad of problems***. ⟶

ALERT FATIGUE AND FALSE POSITIVES
Teams are inundated with telemetry and overwhelmed by noisy DLP or UEBA alerts, making it difficult to piece together a coherent picture – resulting in missed signals, wasted effort on non-issues, investigator burnout, and delayed response.

LIMITED VISIBILITY
Data silos and shadow IT make it tough to correlate HR, identity, and security telemetry into a single risk picture.

TOOLING GAPS AND MANUAL PROCESSES
No SIEM in place, a lack of automation, and reliance on team members might all slow down investigations and create blind spots.

BUSINESS BUY-IN, POLICY, AND CULTURAL RESISTANCE
Educating executives, HR, and the broader workforce on insider threat realities often proves harder than the technical build-out, especially where privacy laws or works councils apply.

RESOURCE CONSTRAINTS
Small teams, limited tooling budgets, and expensive multi-stakeholder investigations stretch already thin security resources.

INSIDER THREAT SPOTLIGHT: The North Korean fraudulent IT worker problem

Some organizations are beginning to rewrite recruiter playbooks specifically to detect North Korean fake worker patterns, signaling that geopolitical threats are driving new HR/security partnerships.

We can't report on insider threats today without touching on the **North Korean (DPRK) fraudulent IT worker schemes**. Several of the respondents we surveyed noted it as a high priority on their list of concerns, particularly CISOs at companies with more than 1,000 employees.

Some survey respondents acknowledged beginning to shift internal processes in response to this threat, and a strong majority of respondents (**87%**) indicated that collaboration with their HR/recruiting department is part of their insider threat defense strategy already today. However, most noted that the collaboration is manual, ad-hoc, and/or behaviorally-focused.

The coordination between HR and security seems to run on a spectrum ranging from informal "call-me-when-there's-trouble" arrangements to more mature processes, with a minority having ticketing integrations or workflow automation that routes events to both teams in real time. About **60%** of respondents say coordination is done through informal chats, ad-hoc emails or manual ticket creation, with no automated workflows linking HR and security systems.

Background checks were the most universally noted touchpoint, yet even here depth and rigor vary widely, signaling an opportunity for deeper process and standardization.

about

60%

of security professionals say coordination between HR and security is a manual process

"Literally every Fortune 500 company has at least dozens, if not hundreds, of applications for North Korean IT workers. Nearly every CISO that I've spoken to about the North Korean IT worker problem has admitted they've hired at least one North Korean IT worker, if not a dozen or a few dozen."

CHARLES CARMAKAL | CTO, Mandiant Consulting
Source: Cyberscoop

What are security teams using to address insider threats today?

The teams actively working to address the insider threat problem are using SIEMs as the backbone of their efforts, commonly with a suite of other tools. Most organizations funnel logs into a SIEM, enrich them with DLP hits and UEBA risk scores, and then overlay endpoint telemetry for context. Most teams noted pain points with integration and automation gaps.

MOST USED TOOL

SIEM platforms

BIGGEST AREA FOR GROWTH

automation and integrations

COMMON TOOLSTACK FOR INSIDER THREAT PROGRAMS TODAY

SIEM PLATFORMS
to correlate events across endpoints, networks, and cloud services.

DATA LOSS PREVENTION (DLP) TOOLS
for high-fidelity signals on sensitive data handling.

USER AND ENTITY BEHAVIOR ANALYTICS (UEBA)
to surface user deviations that might indicate malicious intent.

ENDPOINT DETECTION & RESPONSE (EDR) TOOLS
for granular user device activity that feeds insider risk scoring models.

HR, IDENTITY & THREAT INTEL FEEDS
to create richer risk scoring that blends human context with technical data.

An opportunity to defend with earlier warning signals

SpyCloud's solutions provide visibility and action on both negligent/compromised and malicious insiders before behaviors even surface, bridging the gap between traditional detection and proactive mitigation.

Given the growing proliferation of insider threats, business-as-usual, behavioral analytics, and broad-purpose security tools alone can't detect every potential insider.

The good news is that insider threats, whether malicious or negligent, can often be tied back to some form of identity misuse.

Identity intelligence sourced from malware infections, third-party breaches, and phishing attacks fills a blindspot in existing tooling that helps teams uncover insider risk earlier in the threat timeline.

SPYCLOUD CUSTOMER

"I get bombarded all day long by vendors who want to show me DPRK stuff – but this is something I have not seen before. What you guys are able to do and show is amazing."

SECURITY LEADER | Global Online Marketplace

SpyCloud's identity intelligence identifies employees, vendors, and job candidates who are compromised, infected, or using stolen identities to:

PREVENT EMPLOYMENT FRAUD
Detect fraudulent candidates using stolen or fabricated identities, including fake North Korean IT worker fraud.

IDENTIFY MALICIOUS INSIDERS
Surface hidden connections between insiders and criminal infrastructure – revealing adversarial intent before access is abused.

DETECT COMPROMISED USERS
Spot legitimate employees and third parties who've had credentials and cookies exfiltrated by malware, introducing unseen risk to the business.

What's next?

Mitigating insider threats in 2025 and beyond

Insider threats – whether negligent or malicious – are now a systemic risk, amplified by remote work, identity sprawl, and even state-sponsored infiltration. Traditional detection methods often miss the mark because they rely too heavily on behavioral signals or manual processes.

This is no longer a problem to deprioritize or ignore. If you don't have a formal program or framework, now is a critical time to make one. And if you already have one, be sure to revisit, involve other teams, and augment it further together to account for the true scale of this threat.

67%

of security teams are making it a priority to augment their insider threat detection and mitigation program in the next 12 months

HERE'S HOW TO MODERNIZE YOUR APPROACH AND BEAT INSIDERS:

ELEVATE YOUR VISIBILITY WITH IDENTITY INTELLIGENCE

Behavioral analytics (like UEBA) are useful, but not enough, and may come into play too late. Insider threats often convey hidden indicators of risk via their digital exhaust. SpyCloud's recaptured darknet identity data **gives you those insights** – acting as an earlier warning system – to identify risk long before suspicious behavior is observable.

PRIORITIZE QUALITY OVER QUANTITY

Security teams are stretched thin. Instead of monitoring everything, focus your efforts on high-fidelity identity signals earlier in your process. These indicators reduce false positives and provide clarity on whether a user is negligent, compromised, or malicious.

STRENGTHEN PRE-ACCESS BACKGROUND CHECKS WITH DARKNET INTELLIGENCE

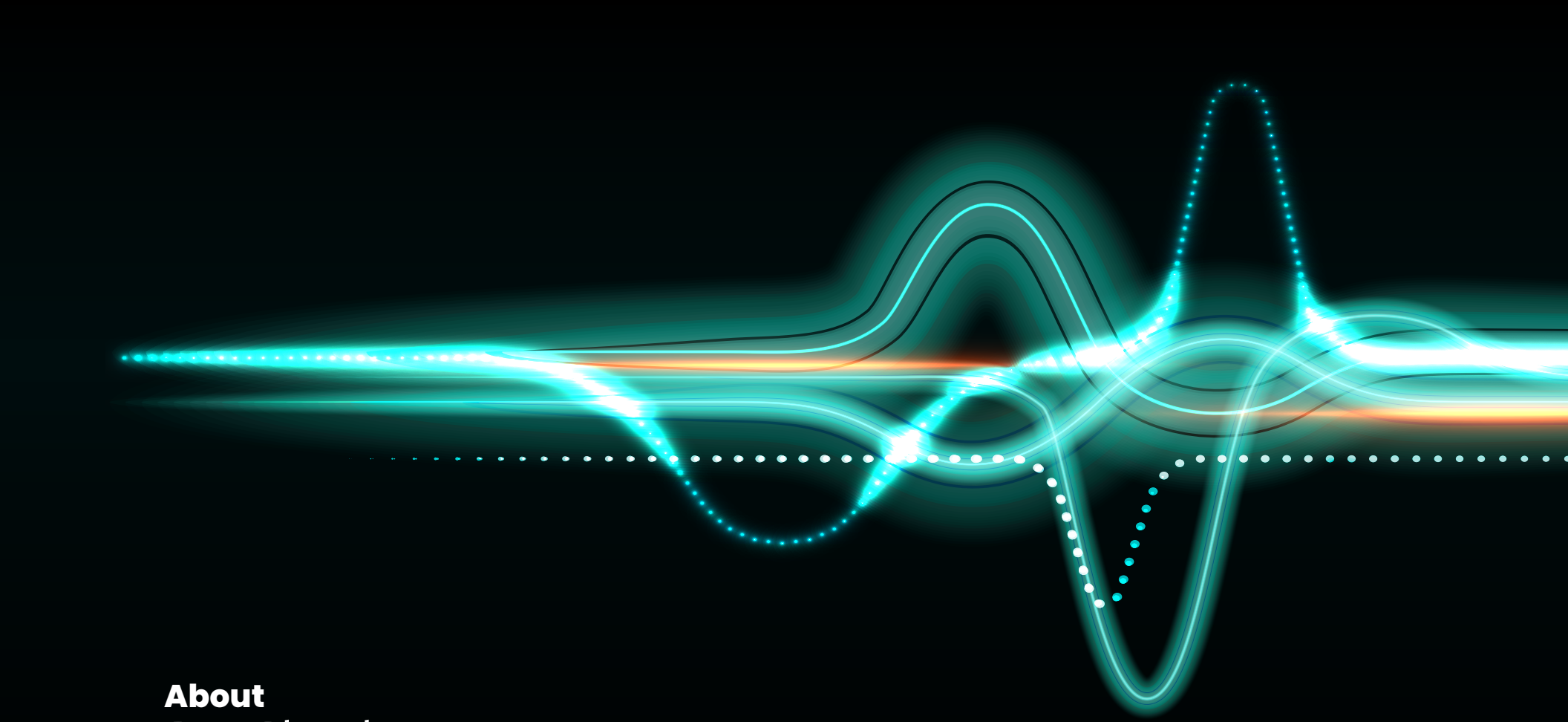
Malicious insiders, including North Korean IT operatives, are slipping through traditional background checks. SpyCloud helps organizations vet new hires and vendor identities, surfacing links to known adversarial infrastructure or fraudulent identities before access is granted.

CLOSE THE LOOP BETWEEN DETECTION AND ACTION

Manual processes and alert fatigue leave dangerous gaps, especially as adversaries speed up their efforts. SpyCloud integrates high-fidelity identity data directly into your workflows, surfacing only actionable signals and enabling automated risk remediation. This reduces noise while increasing your ability to catch and stop definitive threats.

UNITE SECURITY AND HR UNDER A SHARED PLAYBOOK

Insider threats cross organizational boundaries. Build workflows that tie identity risk to business processes – from onboarding to offboarding – and futureproof your insider risk program with shared accountability and continuous threat monitoring.



About SpyCloud

SpyCloud exposes fraudulent workers before HR onboards them, surfaces insider risk signals your SIEM or DLP miss, and shuts down threats in minutes.

GET A DEMO
to see how SpyCloud Investigations uncovers hidden risks from fraudulent job applicants ▸