Empowering Proactive Defense Against Insider Threats

→ PRODUCTS FEATURED: INSIGHTS, PEOPLE SEARCH, SHIELD

Client Background

A Fortune 500 financial institution operated with mature cyber, supply chain, physical security, and Global Security Operations Center (GSoC) teams to address external threats. However, insider risks—particularly those involving nation-state actors—lacked ownership and visibility. With no dedicated Insider Threat team and no purpose-built tools for early detection, the organization was exposed to covert but high-stakes threats that could compromise personnel and proprietary innovation.

To fill this gap, the institution established a centralized Insider Threat team. Strider was brought in to equip the team with a suite of strategic intelligence tools—**Insights**, **People Search**, and **Shield**—to proactively identify, assess, and respond to insider risk signals.

The Challenge

An employee received an unexpected email from a prestigious U.S.-based academic institution. While the message appeared harmless, the client's security team had recently flagged the same sender in Strider's Insights tool during a "targeted technology" review—a workflow designed to identify suspicious outreach tied to foreign influence activity.

Without clear context, Legal and HR were hesitant to escalate, and the employee was unsure whether the outreach represented a threat or an anomaly. The Insider Threat team needed a way to validate this activity without triggering unnecessary alarm.

How Strider Helped

The Insider Threat team leveraged Strider's platform to investigate and respond:

Shield's real-time threat feed was integrated into the institution's SIEM through the Shield API, enabling continuous monitoring of high-risk selectors.

Within days, **Insights** surfaced historical context showing that the same sender had previously contacted other flagged employees—suggesting a coordinated pattern.

Using **People Search**, the team conducted a profile analysis of the sender, uncovering multiple verified risk signals—among them, foreign government affiliations, research collaborations with strategic competitors, and foreign funding connections.

By combining Shield's curated signals, the relationship context from Insights, and People Search's entity-level risk intelligence, the team confirmed the activity as part of a broader targeting campaign—all in under one week.

Outcomes

While specific metrics are still being evaluated, the client has reported meaningful changes:

A Two-Tiered Data Verification Process: Accelerates decision-making and reduces ambiguity.

Faster Cross-Functional Collaboration: Legal and HR now approve escalations within hours, not days.

A Cultural Shift: Employees are proactively reporting unusual outreach, seeing security as a partner—not just an enforcer.

Executive Alignment: Leadership now champions Strider's intelligence-led approach, driving broader adoption across departments.

What's Next

Following the success of this deployment, the Insider Threat team is:

- Expanding **Shield**-powered email filtering to more business units.
- Launching training programs using real examples surfaced through **Insights**.
- Exploring **Organizations Search** to vet third-party collaborators and strategic partnerships.

About Strider

Strider empowers industry, government, and academia with strategic intelligence to protect their people, technology, and relationships from nation-state threats. In a world of escalating geopolitical competition, we enable organizations to safeguard innovation and maintain their long-term strategic advantage.

Interested in how Strider can help your team identify and respond to insider threats?

Schedule a personalized demo to explore the platform.

REQUEST A DEMO →