STRIDER

CLIENT STORY

Countering PRC IP Theft at a Fortune 100 Chemical Company

Background

Our client is one of the world's largest chemical manufacturers, producing essential components—using a patented process—for life-saving products relied on by millions.

When the company became the target of an intellectual property theft attempt by state-sponsored actors, its global security team turned to Strider for support. Leveraging insights from Strider's strategic intelligence platform, the team successfully protected their proprietary manufacturing process.

This case highlights how Strider not only helped prevent a significant theft attempt, but also enabled the client to establish a proactive, intelligence-driven approach to securing its most valuable assets.

Uncovering an Attempted IP Theft

In 2021, our client received an alert from the U.S. government that the People's Republic of China (PRC) was actively working to replicate one of the company's flagship products. A successful duplication of the patented manufacturing process would have severely impacted the client's competitive edge and long-term profitability.

To respond effectively, the company needed critical answers: Which PRC entity was behind the effort? Which employees had access to the proprietary process? And were there any connections—direct or indirect—between those individuals and the PRC government? They also needed visibility into any active attempts to approach, engage, or recruit current employees with access to sensitive knowledge.

Leveraging Strider's Insights for Actionable Intelligence

To address these concerns, the company turned to Strider's Insights. With this intelligence, they identified the specific technology at risk and determined which current and former employees had been involved in its development.

Insights flagged a former employee with deep expertise in the manufacturing process and concerning ties to the PRC. During their tenure, the individual had significant visibility into the patented process. The investigation uncovered that the employee had participated in a PRC government talent program, delivered lectures at PRC-affiliated events, and was now teaching at a Chinese university conducting research closely aligned with the client's proprietary technology.

Deepening the Investigation

The company submitted a Request for Information (RFI) to Strider's Global Intelligence Unit for more detailed insights. The RFI report provided in-depth information on the former employee's publications and work history, establishing the employee's deep understanding of the client's proprietary technology.

The investigation also revealed that the former employee's current role at the Chinese university involved leading efforts to replicate the company's manufacturing process on behalf of the PRC.

RESULTS AND IMPACT

After understanding the scope and scale of the IP theft attempt, the company took several strategic actions to secure its flagship product and manufacturing process:

1. Internal Investigation

The company's Office of General Counsel initiated a formal investigation into the former employee. Through continued collaboration with Strider, they determined that up to 70% of the manufacturing process had been exposed to the former employee. This allowed the company to focus on securing the remaining 30% that had not been compromised.

2. Employee Training and Security Enhancements

Leveraging Strider's Insights, the company identified current employees with expertise in the remaining 30% of the manufacturing process. These employees received additional training on data handling and were briefed on enhanced security protocols.

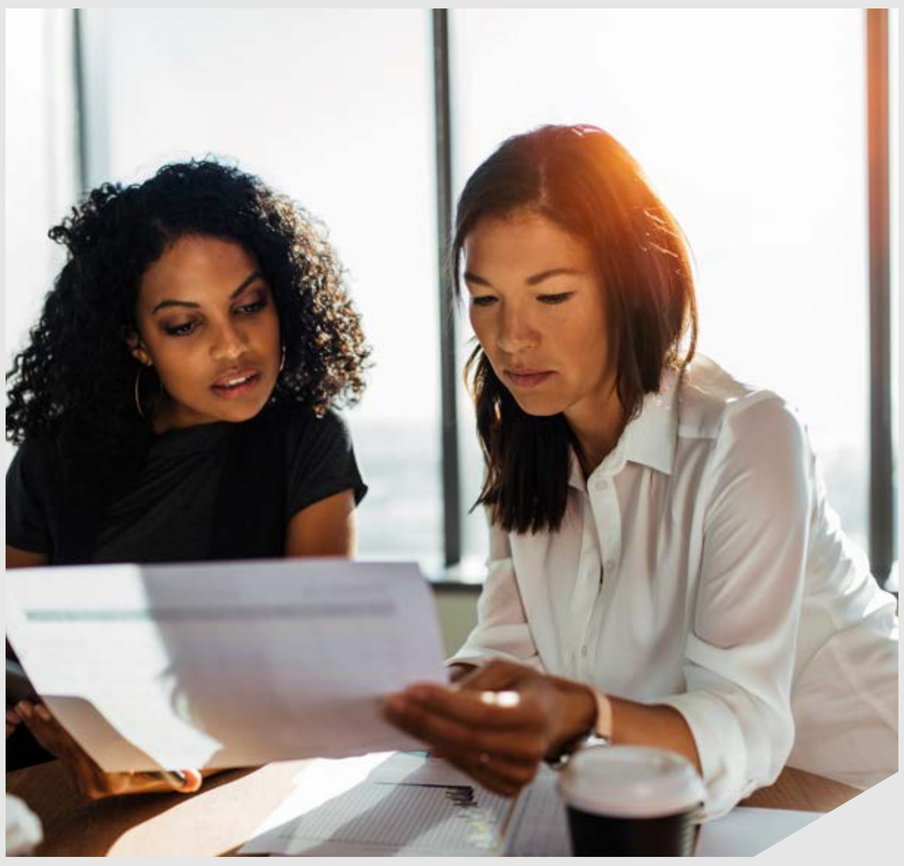
3. Deploying Shield for Email Security

To strengthen their defenses, the company implemented Shield to monitor and block communications linked to known PRC-affiliated actors—including the former employee, their associates, and connected institutions. Shield delivered real-time alerts for any suspicious outreach, enabling the security team to act immediately and prevent further exposure.

PROACTIVE SECURITY STRATEGY

This incident underscored the need for the client to implement broader changes across its security strategy to proactively secure additional key technologies and processes. They used Strider products to:

- Identify other critical technologies that could be targeted by state-sponsored actors.
- Determine which employees were involved with these sensitive technologies.
- Strengthen data access management for these technologies.
- Communicate the risks of state-sponsored theft through regular security briefings and training sessions.
- Monitor external communications from known state-sponsored actors.



About Strider

Strider transforms open-source data into strategic intelligence that empowers organizations to protect and advance innovation. By combining advanced AI technologies with proprietary methodologies, Strider helps clients proactively identify and respond to state-sponsored risks—including intellectual property theft, talent targeting, and supply chain vulnerabilities.

See what insights Strider can reveal for your organization.

striderintel.com/request-demo