STRIDER

CLIENT STORY

COUNTERING PRC IP THEFT AT A FORTUNE 100 CHEMICAL COMPANY

Background

Our client is one of the largest chemical manufacturers in the world. Using a patented manufacturing process, this company creates essential components for life-saving products used by millions.

Recently, the company faced an IP theft attempt orchestrated by state-sponsored actors. With insights provided by Strider intelligence, the company's global security team successfully safeguarded its proprietary information. This case study illustrates how Strider's products not only prevented the theft of a critical manufacturing process but also helped the organization establish a proactive security strategy.

Uncovering an Attempted IP Theft

In 2021, our client received a warning from the U.S. government that the People's Republic of China (PRC) was attempting to develop a product identical to one of the company's flagship offerings. If the PRC had successfully replicated the manufacturing process, it would have significantly undermined our client's market position and profitability.

The company needed to know which PRC entity was attempting to replicate their product, which of their employees had access to the patented manufacturing process, and if there was any connection between those employees and the PRC government. Additionally, they wanted to identify any ongoing attempts to engage or recruit current employees.

Leveraging Ranger for Actionable Insights

To address these concerns, the company turned to Strider's Ranger platform. They identified the specific technology at risk and pinpointed which current and former employees were involved in its development.

Ranger flagged a former employee with expertise in the technology and suspicious ties to the PRC. During this employee's tenure, they had significant visibility into the patented manufacturing process. It was discovered that the employee had participated in a PRC government talent program, lectured at events hosted by the PRC, and was now teaching at a Chinese university known for research closely related to the client's manufacturing process.

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 data, 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

The company implemented Shield, Strider's email security tool, to monitor or block any communications with known PRC actors. This included the former employee, their collaborators, and institutions associated with the employee. The tool provided real-time alerts for any suspicious communication attempts.

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 publicly available data into strategic intelligence to secure and advance innovation. Leveraging cutting-edge AI technology alongside proprietary methodologies, Strider intelligence helps organizations proactively address and respond to risks associated with state-sponsored intellectual property theft, targeted talent acquisition, and supply chain vulnerabilities.

See what insights Strider can reveal for your organization.

striderintel.com/request-demo