

Reducing Insider Risk and Incidents in Big Pharma

My number one question from the board is, where are my biggest risks and who are my riskiest users are – I now have the answer AND I can do something about it!

CISO

The Challenge

At the heart of the challenge this Fortune 100 pharmaceutical was facing was how do we protect our company IP from sophisticated attackers, but still enable the company's scientists and others to operate at maximum safe speeds in an environment where time to market is critical.

Balancing these two realities required a solution that truly understood the risks that every user in the organization presented, what those risks were and automation to enable the right level of protection that helped them stay ahead of incidents and breaches.

Project Goals

- Protect highly sensitive intellectual property balancing speed and safety
- Embed Elevate's threat intelligence into other systems and provide employee feedback
- Complement current SIEM/UEBA solution by identifying bad actions and orchestrating a response

Why Elevate

- Visibility into company, department and individual key risks that may lead to breaches
- Out of the box recommendations based on key insights from data
- NIST based playbook automation that allowed precision in proactive response and controls

The Organization

This Fortune 100 pharmaceutical company has a large workforce with a mix of full-time employees, contractors, and subcontractor roles. The company produces intellectual property that has high value to nation state attackers and needs to balance locking down security in the company with business velocity.

Note: *Elevate respects that some of our customers prefer not to publicly state which security vendors they use. As such, we have removed the client's name and anonymized specific details in this case study.*

The Solution

Going Beyond Insider Threat

The security team had already implemented SIEM, SOAR and insider threat tooling, but found that it was reactive by design. It helped in responding to incidents, but lacked insights to help them be proactive in their approach to defending their organization.

While insider threat was and still is a worry, moving towards a broader view of insider risk was a high priority given most of the challenges they needed to address were sophisticated attackers targeting their workforce with account takeover attacks and data loss threats.


This is where Elevate Security stepped in – by understanding every user's actions, access, how frequently they were being attacked, and the controls that were in place to protect them, the organization gained visibility into their true risks and was able to take immediate action on them through the Elevate Security platform.

Finding Value Quickly

– from a pilot program to coverage across the business in 6 months

The original deployment was to a small subset of the organization. Very quickly the security team realized the power of the platform and the user risk profiles available to other tools. This enabled the team to expand the deployment across a number of departments. After validating that they were seeing the same insights and value other customers had received from the Elevate platform, they decided to expand globally across the entire organization.

Some of the outcomes Elevate customers have seen are:

 82%
Reduction in malware/ransomware and account takeover incidents

 55%
Improvement in risky security decisions being made

 47%
Increase in the detection of attacks targeting employees

Productive Workforce, Secure Business

With the Elevate Security platform in place, the organization finally had a solution that went beyond their traditional program of one size fits all controls and relying on detection to catch threats fast enough. Elevate Security helped the security team to pinpoint where key business risks were and which users represented that risk, but gave them the tools to enable maximum safe speeds to the business. Users who were riskier were given tighter security controls and policies and those who were less risky were given more freedom.

In the end – a win-win for the security team and the business.