CASE STUDY

DUPONT DRIVES FASTER DECISIONS WITH AUTOMATED SECURITY INTELLIGENCE

OVERVIEW

DuPont is a global Fortune 500 company delivering technology-based materials, ingredients, and solutions that help transform industries and everyday life. More than 35,000 employees around the world apply diverse science and expertise to help customers advance their best ideas and provide essential innovations in key markets including electronics, transportation, construction, water, health and wellness, food, and worker safety.

Challenge

For more than 200 years, DuPont has been synonymous with life-changing discoveries and technological breakthroughs. Over the years, the enterprise has undergone numerous mergers and acquisitions. Most recently, they completed a sweeping restructuring to future-proof the business and continue delivering essential innovations that help people live safer, healthier lives.

Such periods of transition can introduce new cybersecurity risks to any organization. They generally bring team structure shifts, add new technologies to the mix, and introduce varied or inconsistent security practices that potentially create gaps for threat actors to try to exploit.

Understanding these risks, DuPont doubled down on building a global cyber threat team and sustainable program to effectively manage them across the enterprise. When global cyber threat leader Bob Stasio came on board in late 2019, he went straight to work. He began by standing up a new internal security operation center that would investigate incidents ranging from business email compromise, to fraud, to data loss, to advanced persistent threats targeting the organization's trade information and intellectual property.

Bob recalls, "There wasn't a strong focus on intelligence." He continues, "Things were contracted out and incidents were thrown over the wall without context. We needed to understand what was going on."

So, he started off doing a lot of the incident handling himself, while building out the team at the same time. He says, "During this initial stage we had a high mean time to respond — when an alert came in, it took us quite a bit of time to triage, mitigate, or remediate it."

But Bob had a vision and a plan for driving down this critical KPI with an "incident response 2.0" approach grounded in security intelligence.

Solution

A U.S. military veteran whose impressive career spans the NSA, U.S. Cyber Command, and private sector giants like Bloomberg and IBM, Bob draws strong parallels between intelligence activities and cyberspace operations.

He says, "In cybersecurity, as in the military, you often have to operate in an environment with very little information. You have to look for the early indicators and trends of something going on, then extrapolate and make a decision very quickly."

The ability to understand your adversaries — and the conditions under which you will have to disrupt them — is critical to speeding and amplifying these efforts. That's where security intelligence comes in. "I had known about Recorded Future for many years, and had worked with and trusted the company during my time in the private sector. It was one of the first calls I made after joining DuPont," says Bob.

Recorded Future's unique technology collects and analyzes vast amounts of data to deliver relevant insights in real time. This empowers security teams to quickly triage out false positives, automatically identify high-priority alerts, and easily drill into an unparalleled range of sources and evidence for deeper analysis. After bringing Recorded Future on board, DuPont's 24-member global cyber threat team quickly realized the power of actionable intelligence in enhancing their threat research and speeding cycles.

> We've structured our team so that much of the filtering and triage is done on the front end. With machine learning and automated security intelligence from Recorded Future, only the really important alerts bubble up to my team, and there are very few false positives.
>
> *-Bob Stasio*

Bob has many examples of the ways Recorded Future has empowered DuPont to disrupt adversaries. For instance, "A targeted phishing attack hit one of our plants in Asia using Formbook malware. With access to Recorded Future Intelligence Cards™ and great notes from their Insikt team, we were able to look at the malware in a sandbox and trace the attack back to a compromised third-party vendor — quickly narrowing down a list of 300 vendors to just two. We wouldn't have been able to do that without Recorded Future."

On another occasion, the team tapped Recorded Future to rapidly identify and shut down an advanced malware kit, then communicate their success back to leadership. "Having the ability to dive deeper and create professional reports that provide high-level, risk-based insights and are backed by a respected academic group is very powerful," he says.

The team also relies on security intelligence to streamline and justify vulnerability management efforts. Says Bob, "It's very difficult to get IT to take infrastructure down even for a minute for a patch. Recorded Future enables us to prioritize the vulnerabilities that present real risk, so we can say, 'Out of these 10,000 vulnerabilities, we really need to focus on these 10.'"

Results

Bob is confident in quantifying his team's success with Recorded Future. "By using security intelligence to understand threat severity and context, we've reduced our mean time to respond by a factor of 10."

He continues, "I view incident response in three steps. The first step is to confirm or deny there's an issue. The second step is to determine scope and scale. And the last is to remediate and get back to normal. To confirm or deny if it's a false positive, security intelligence is absolutely vital. You can't do anything else until you confirm that it's really an issue and wrap some context around it. Is this just a random drive-by malware or is this an advanced persistent threat trying to get into my network? And that will determine how you respond to it, how much time you spend on it, and how much effort you want to put against a particular alert. Security intelligence is really the linchpin across this entire process."

Looking Ahead

DuPont has offices and manufacturing facilities across Asia, Europe, and the United States, along with SCADA networks within its research centers and plants. With so many physical and digital assets around the world, automation is critical to defending against and responding to emerging threats at scale. As the team evolves their automation efforts, Bob plans to integrate elite, real-time intelligence from Recorded Future directly into the automation tools his team already uses to drive better, faster decision-making — without disrupting workflows.

Recorded Future®

www.recordedfuture.com

@RecordedFuture

About Recorded Future

Recorded Future delivers the world's most technically advanced security intelligence to disrupt adversaries, empower defenders, and protect organizations. Recorded Future's proactive and predictive platform provides elite, context-rich, actionable intelligence in real time that's intuitive and ready for integration across the security ecosystem.