CHEMOURS AND OPEN SYSTEMS HAVE THE RIGHT FORMULA FOR **CYBERSECURITY COLLABORATION**

About Chemours

The Chemours Company is a global chemistry company with a 200-year-old legacy and commitment to creating a better world through the power of its chemistry. Known for producing prominent brands such as Ti-Pure™, Opteon™, and Teflon™, Chemours has 6,400 employees serving approximately 3,200 customers in about 120 countries.

> Open Systems stepped up and became an integral part of the cybersecurity maturity model we aspired to – and achieved.

Reginald Williams, Chief Information Security Officer (CISO), Chemours

WHY CHANGE?

- Commitment at the corporate level to digital manufacturing
- Cybersecurity had to level up to support ambitious digital transformation goals

THE NEW REALITY

- 24x7 global coverage through Open Systems Mission Control SOC (security operations center)
- Integration into Microsoft tools for simpler coordination with IT
- Secure configuration of critical infrastructure
- Technology and human expertise leveraged to assess threats and speed up attack mitigation

WHY IT'S BETTER

- Reduces risk by accelerating security maturity, reducing complexity, and consolidating on a single security ecosystem
- Eliminates the silos between IT and security team by using common ecosystem
- Improves context on the attack surface
- Mitigates threats to stay operational

As a chemical manufacturer, Chemours operates its facilities with a strong focus on safety and securing the integrity of its data. To face this challenge and help ensure compliance, Chemours CISO Reginald Williams had a vision for transforming cybersecurity, a vision that maintains the integrity of the manufacturing process and its data – without slowing the business down.

With a global network of almost 6,400 users across approximately 60 locations, Chemours has a lot to protect. Historically, the chemical plants within Chemours have operated in siloes when it came to data and analytics, an approach that reduced the visibility in the manufacturing chain. Instead, Chemours needed to centralize these analytics – securely.

"We decided to go on a two-year journey to transform cybersecurity from where it was, to a much more mature state," says Reginald Williams, Chemours CISO. "Open Systems was an integral part of that journey with their managed detection and response capability."

COLLABORATION DRIVES CO-INNOVATION

Among the first decisions Williams made during this transformation was reducing the number of security tools in the company. Chemours is a Microsoft-first organization, with Microsoft Sentinel and Microsoft 365 E5 playing key parts in its cybersecurity strategy.

E5 provided the Chemours security team a mature security stack from a single vendor experienced in the manufacturing industry – and eliminated the need to manage and monitor 30 to 40 different cybersecurity products.

Chemours sought a partner and collaborator in managed detection and response (MDR). Since the company had consolidated around Microsoft, Chemours also wanted an MDR provider that was proficient in the Microsoft environment. After seeing a proof of concept from Open Systems, a Microsoft cybersecurity partner, Chemours added Open Systems MDR+ to their lineup.

Beyond an MDR service provider, Williams wanted a co-innovation partner, one that would listen to his company's needs and produce a solution tailored to them.

MISSION CONTROL: PROTECTING THE ENTERPRISE

Now, the Chemours ecosystem runs efficiently and securely, with help from the Mission Control 24x7 follow-the-sun SOC. Mission Control uses a combination of people, technology, and processes that follow repeatable security "missions," custom runbooks that prescribe how to protect the enterprise in real time today and level up its security posture for tomorrow.

Through its collaboration with Open Systems, Chemours also gained a strategic advantage by marrying the telemetry on the NOC with the SOC, bringing the logs into one operations center, where Open Systems engineers are doing the investigations and responding accordingly.

With MDR+, Chemours can manage cybersecurity with a smaller in-house team footprint, because Mission Control SOC analysts and engineers who have the expertise and knowledge of the Chemours environment to go beyond detection and response to mitigate the threats.

"The service that Open Systems provides for us is actually fulfilling the need of 10, maybe even 12 full-time individuals," says Williams. "With Open Systems, they're doing the engineering, they're doing the analysis, they're building capabilities that I don't have to shoulder myself."

Open Systems' Microsoft expertise, integrations, and machine learning models now provide Chemours with better context on the attack surface, integration into Microsoft tools for simpler coordination with IT, and secure configuration of critical Microsoft infrastructure. And to bring the analytics from the disparate plants together in a secure cloud environment, Chemours can use Azure Lighthouse to connect their Sentinel to Open Systems and maintain full data retention – so Chemours never loses visibility or control of their data.

Given that Chemours produces essential chemicals critical to much of modern-day living – data security and compliance will always be paramount.

"If there's a threat, I need a solution for that threat. Open Systems MDR+ not only solves my compliance needs, but it also extends beyond detection and response to mitigate threats," says Williams. With Open Systems' highly trained engineers working around the clock to partner with the Chemours security team, they can stop those threats in their tracks.