Nemours
Children's Health System

Cymulate

Nemours Increases Visibility to Improve Detection and Response

Organization

Nemours Children's Health System, a nonprofit children's health organization, began more than 70 years ago with the vision of Alfred I. duPont to improve the lives of children and to do whatever it takes to prevent and treat even the most disabling childhood conditions. Today, through their children's hospitals and health system, they directly care for more than 483,320 children annually in Delaware Valley and Florida.

Nemours Information Security Department

Nemours security department is led by Chief Information Security Officer (CISO), Jim Loveless.
The department is comprised of two teams:
a risk and governance team, responsible for defining the organization's security program and policies, and an engineering and operations team tasked with the prevention, detection, and response to threats. Nemours faces financially motivated cyber threats that attempt to disrupt healthcare services, deploy ransomware, and steal electronic protected health information (e-PHI) for extortion, in addition to other types of threats.

Business Challenge

The security team is tasked with protecting their organization from evolving cyber threats, maintaining continuous healthcare services and, protecting the sensitive and personal information of the people they serve and treat, as well as their employees.
Their goal is to enable Nemours to provide better healthcare services by securing remote healthcare givers, providing a safe online customer experience, and protecting the IT environment and connected medical devices. With so much to accomplish and a fixed amount of resources, the team was challenged with false positive alert fatigue and a lack of visibility to prioritize team efforts, including patching vulnerabilities in the face of new threats. The team needed to deal with these challenges, while still improving their incident response capabilities and optimizing existing security controls.

Jim notes, **"we had to increase the team's productivity by reducing alert fatigue, we needed a better way to find where the real problems are and fix them."**

Challenge

Nemours needed a way to evaluate its defenses against the latest threats, prioritize remediation efforts better, and improve its team's productivity and incident response skills.

Solution

Cymulate's automated immediate threats intelligence assessments, purple team exercises and security control validation makes it simple for Nemours to know and control its security posture.

Benefits

Cymulate has helped Nemours improve its security posture and its security team's skills.
It has also increased its productivity by automating tasks, reducing false positives and prioritizing remediation activity.

Solution

The security team was able to deploy Cymulate quickly and saw immediate improvements by optimizing security controls in their existing multi-layer architecture. Jim noted that Cymulate has quickly become an integral part of Nemours' security architecture.
Eric Dixon, engineering and operations manager said that, **"Cymulate showed us how to prevent half of the known exploit techniques from succeeding by making one policy change in our endpoint protection tool. We implemented that change and it prevented 168 exploits from being able to run on Nemours' computers."**

Nemours also uses Cymulate to practice incident response exercises, such as emulating malware on a VPN connected endpoint. Once they saw Cymulate in action, Nemours extended the coverage of the continuous security validation platform to simultaneously cover multiple environments.

> *"Cymulate enables us to test Nemours' defenses against the latest cyber threats as they emerge, prioritize remediation efforts, and improve our security team's incident response skills."*
>
> Jim Loveless, CISO, Nemours

Benefits

Jim summarizes the benefits in his report,
"We purchased Cymulate to assess our security effectiveness. When a new threat emerges we are immediately asked if Nemours is protected against this threat. With Cymulate's capability we are now able to answer that question by simulating the attack and seeing how our tools detect or prevent it."
He goes on to say, "Following the assessment, we get a report back without the team having to get involved. This helps us immediately identify where our gaps are and fill them."

Another important benefit is Cymulate's contribution to the team's productivity. Just by using Cymulate, the team has enhanced their offensive skills, making them better defenders. It has also helped to reduce the amount of false positives through improvements in the security architecture and prioritizing patching efforts.

"Even if patches were not yet available, using Cymulate we know which counter measures are effective against the latest threats," says Jim.

About Cymulate

Cymulate was established with the vision of empowering security professionals to make better decisions faster, based on real-time data.
Founded and led by an elite team of cyber researchers with world-class experience in offensive cyber solutions, Cymulate is determined to become the golden standard for security professionals and leaders to know, control, and optimize their cybersecurity posture end to end. Trusted by hundreds of companies worldwide, Cymulate constantly enhances its methods to prepare organizations for any attack scenario or campaign.
With Cymulate, organizations continuously measure security performance in real-time, shore up defenses, and assure operational effectiveness.
Measuring your cybersecurity performance is fundamental towards creating a more secure organization!

Contact us for a live demo, or get started with a free trial

Start Your Free Trial

Headquarters: Maze St 3, Tel Aviv 6578931n, 7546302, Israel | +972 3 9030732 | info@cymulate.com