NEMOURS CHILDREN'S HEALTH

cymulate

Nemours Increases Visibility to Improve Detection and Response with Cymulate

CASE STUDY

Challenge

The Nemours security department is comprised of a risk and governance team and an engineering and operations team, both led by CISO Jim Loveless. The security team is tasked with protecting its organization from evolving cyber threats, maintaining continuous healthcare services, and protecting the sensitive and personal information of its patients and employees.

The team needed a solution that could:

- **Evaluate its defenses against the latest threats**
  As a healthcare organization, Nemours faces financially motivated cyber threats that attempt to disrupt its services, such as deploying ransomware or stealing electronically protected health information (e-PHI) for extortion.
- **Prioritize remediation efforts**
  The security team faced false-positive alert fatigue and lacked visibility to prioritize tasks, including patching vulnerabilities in the face of new threats.
- **Improve its incident response skills and optimize security controls**

Jim noted: **"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."**

The Cymulate Solution

Nemours deployed Cymulate Breach and Attack Simulation (BAS) and saw immediate improvements by optimizing security controls in its 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 **"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 the team saw Cymulate in action, Nemours extended the coverage of the platform to simultaneously cover multiple environments.

Overview

Industry	Hospitals & Healthcare
HQ	Florida, USA
Company Size	5-10K employees

> 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

Solution

- Breach and attack simulation

Results

- Improve security posture
- Reduce false positives
- Prioritize remediation activity

Benefits

Emergent threat assessments

"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."
– Jim Loveless, CISO

Automated reporting following each assessment

"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."
– Jim Loveless, CISO

Increased team 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 countermeasures are effective against the latest threats.**
> — Jim Loveless, CISO

About Cymulate

Cymulate, the leader in exposure management and security validation, provides the single source of truth for threat exposure and the actions required to close security gaps before attackers can exploit them. More than 500 customers worldwide rely on the Cymulate platform to baseline their security posture and strengthen cyber resilience with continuous discovery, validation, prioritization, and guided remediation of security weaknesses. Cymulate automates advanced offensive security testing to validate controls, threats, and attack paths. As an open platform, Cymulate integrates with existing security and IT infrastructure and drives the workflows of the exposure management process. For more information, visit www.cymulate.com.