CASE STUDY

Credit Union Adopts Proactive Security to Validate Exposure and Threats While Optimizing SecOps with Live-Data Exercises

SecOps lacks validation in their move to CTEM

In an era where cyber threats evolve faster than defenses, staying ahead is no longer optional—it's essential. This credit union's security operations (SecOps) team is responsible for managing the organization's security control configurations while supporting the shift to a proactive security posture through continuous threat exposure management (CTEM).

However, the team lacked the resources for ongoing validation of threats, exposures, and response processes. To implement a proactive security strategy, they needed both clear insight into how their defenses would perform against real-world attacks targeting known exposures and the automation required to build true threat resilience.

Annual pen tests were insufficient. Sporadic pen tests only provided the team with a point-in-time picture of its security and were ineffective in validating its security configurations in a continuous and timely manner.

No in-house red team. The organization lacks the resources to fund an in-house red team, and although the SecOps team wanted to validate its controls, it needed to focus on real-time threat detection and response and did not specialize in offensive tactics.

New threats are emerging daily. The SecOps team struggled to detect and prevent new threats as they emerged and continuously evolved.

Compliance audits demand proof of security effectiveness. As a highly regulated organization, the security program needed on-demand proof that security controls functioned as designed.

The SecOps team sought a proactive and continuous method for validating threats and exposures, as well as a platform for conducting tabletop exercises to assess the organization's incident response processes.

The Cymulate Solution

The VP of Cybersecurity had previous experience with Cymulate and decided that it was a good fit for his team due to its simple deployment, easy-to-use interface and library of over 100,000 attack actions.

Cymulate enables the credit union to conduct realistic live-data exercises, validate security controls, assess emerging threats, prioritize vulnerabilities and justify security investments – all in a repeatable, efficient and measurable way.

Overview

Industry: Banking

HQ: Arizona, USA

Company Size: 500 employees

"Cymulate is gold for proving continuous testing during regulatory audits."

– Manager of Cybersecurity Governance

"Cymulate is a red team in a box that I can reliably deploy without causing damage to the environment."

– Head of Cybersecurity Operations

Results

- Reduced incident response exercise setup time by at least 60%
- Independently validate control configuration
- Prioritize vulnerabilities based on control efficacy

> I love that Cymulate can replicate a real-world attack in a way that is safe and repeatable. I no longer need to engage with third-party sources because Cymulate is my reliable, vetted source.
>
> – Head of Cybersecurity Operations

Validate as part of CTEM to prioritize vulnerabilities

"We replaced our traditional vulnerability management with a continuous threat exposure management (CTEM) program. We used to prioritize our vulnerabilities based only on CVSS score and if the threat actor is targeting financial institutions, but Cymulate provides us with more context. We now test those high-priority threats against our controls so we can focus on patching the ones that can actually get through our defenses."

– Manager of Cybersecurity Governance

Automate live-data exercises

"In our most recent incident response exercise with Cymulate, we used three separate workstations across two geographic sites with agents to replicate ransomware data exfiltration and lateral movement inside the organization. If I needed to execute the same sort of traffic without Cymulate, it would probably have taken 25-30 hours to set up and configure. And I am not a programmer, so I don't know if I could have reliably executed the exercise. With Cymulate, the setup was easy, and I didn't have to worry about the execution. Overall, we cut the total time spent on the exercise by at least 60%."

– Head of Cybersecurity Operations

Validate security control configuration

"Cymulate allows us to quickly validate configurations and configuration changes that we make across the organization. Cymulate enables me to replicate and verify my tools without needing to maintain a functional red team skill set. Also, running Cymulate assessments is part of my vendor POC process. It's a great tool to evaluate what a vendor says they can do versus actual capabilities."

– Head of Cybersecurity Operations

Justify security investments

"We recently switched antivirus solutions, and within two Cymulate assessments, we immediately saw its positive impact on our security posture. Cymulate showed our executive board a clear ROI from this investment."

– Manager of Cybersecurity Governance

Benefits

- **Collaborate with vulnerability management** – SecOps provides the exposure validation insights for the CTEM program to prioritize vulnerabilities based on what's exploitable for their environment.
- **Independently run assessments** – Even without an in-house red team, the SecOps team has independence over its security and threat validation and can run assessments and live-data exercises whenever necessary.
- **Baseline and measure security efficacy** – By continuously validating its controls, the SecOps team creates a baseline and measures its security performance over time, easily detecting and managing security drift.
- **Improved visibility of security controls** – The SecOps team understands and can report on how well its controls are detecting, alerting to and preventing cyber threats.