Cymulate

Bank Increases In-House Security Testing without a Red Team

CASE STUDY

Annual Penetration Tests Provided Only Limited Scope

Without the resources to staff an in-house red team, this Singapore bank still recognized the need to think like an attacker. The obvious first option was to outsource penetration testing.

However, the team understood that this once-a-year assessment provided limited scope and only a point-in-time snapshot of the organization's defenses. The team wanted to increase the visibility of its security posture with continuous assessments, so the SecOps team began exploring ways to automate their penetration testing without building an in-house red team.

The Cymulate Solution

After evaluating various automated penetration testing vendors, the bank's senior security manager discovered Cymulate. He recalled, **"We were hooked when we saw that Cymulate also individually validates security controls — all from the same platform. We understood that automated control validation would give us a better picture of our security efficacy than just automated red teaming. It's not only about assessing the potential attack paths; it's also important to validate our control efficacy overall."**

The senior security manager explained that while initially his organization was looking for an automated penetration testing tool, his team also uses Cymulate to automate security validation beyond black-box testing.

Continuously validate security controls

"With Cymulate, we can regularly simulate real-world attacks against our security without an in-house red team."

Automatically validate against emergent threats

"Before Cymulate, our SoC would notify us about certain threats, but these were subject to the threat intelligence solutions it was using. Even after we were alerted about a threat, creating an assessment and evaluating if we were safe would take about three days. The Cymulate Threat Research Group creates assessments of the latest threats, which we have automated to run as soon as they are released. Now can evaluate if we are safe within 24 hours."

Overview

Industry: Financial Services
HQ: Malaysia
Area Served: Singapore
Size: 10K+ employees

"Cymulate is a great solution for organizations interested in both security control validation and automated pen testing."
- Senior Security Manager

Solution

- Breach and attack simulation
- Continuous automated red teaming

Results

- **3 times faster** at assessing emerging threats
- **98% reduction** in network security risk score
- **Increased visibility** of security posture

Automate IOC mitigation

"Cymulate integrates with our XDR to improve our threat detection and response. The Cymulate IOC (indicators of compromise) mitigation capability automatically uploads critical IOC data directly to our XDR to ensure that potential threats are identified and addressed quickly, without manual intervention."

Network penetration testing

"We were unaware that there were open ports in our network, which would have been the easiest way for an attacker to breach our systems. Cymulate alerted us to these gaps and provided remediation guidance, so that we could improve our network segmentation and reduce risk by 98%."

Evaluate and fine-tune new controls

"When we wanted to change web gateways, we used Cymulate during the POC to see how the new control would work in our environment. We also used the Cymulate assessments to ensure the control was configured correctly once we purchased it."

Benefits

- **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 whenever necessary.
- **Better align security policies —** The team can evaluate each security policy, especially the ones configured by predecessors, and understand whether it is properly configured or necessary for the business.
- **Increased visibility —** With both continuous control validation and automated penetration testing, the SeCops team can validate its controls as well as assess its security across the full kill-chain.