cymulate

CASE STUDY

Fintech Organization Automates Security Testing for PCI-DSS with Cymulate

Challenge

This fintech organization specializes in processing payments and has about 2,000 employees spread across three regions. Like other organizations in the financial sector that are susceptible to cyberattacks, this company needs to ensure the protection of its corporate network and the infrastructure that runs its customers' payments.

The organization's cybersecurity function includes a SecOps team, an internal penetration testing team and a security tools and infrastructure team. The latter oversees more than 18 security tools and ensures their effectiveness by analyzing them to find gaps and applying updates.

As a PCI-DSS compliant organization, the security team is required to continuously assess its tools. The team would run vulnerability assessments and penetration tests to assess its security posture, but these did not continuously test the organization's security controls in depth.

The organization did not have the resources to validate its tools manually, so the security tools and infrastructure team began to evaluate the different automated security validation platforms in the market.

The Cymulate Solution

The security team chose to implement Cymulate because it not only offered security control validation with its breach and attack simulation, but it also included assessing lateral movement with its continuous automated red teaming.

While the organization originally purchased Cymulate to prove PCI-DSS compliance, the security team quickly understood the additional value the platform could bring. The manager of cybersecurity explained, **"We knew we needed Cymulate for proof of compliance, but we now see how continuous security control validation has changed the way we assess our security posture as a whole and work towards improvement."**

The manager of cybersecurity elaborated on the different uses that his team has for the Cymulate platform:

Automate security testing for PCI-DSS compliance

"We use the Cymulate reporting to show both internal and external auditors that we are continuously assessing our security tools and improving our security posture as a result."

Overview

Industry	Financial Services
HQ	UAE
Company Size	2,000 employees

Solution

- Breach and attack simulation
- Continuous automated red teaming

Results

- Meet compliance demands for security testing
- Automatically test against emergent threats
- Continuously validate security controls
- Detect and prevent security drift

Continuously validate security

"Cymulate helped us automate our security control validation across three locations, multiple network segments (vLANS) within each location and diverse environments (Windows and Linux). Following our automated assessments, the Cymulate report indicates if any IOCs got past our security controls. If there are areas where our controls are vulnerable, my team knows which IOCs to push into the respective controls and how to focus its efforts to optimize our defenses."

Validate immediate threats

"When the Cymulate Threat Research Group adds a new emergent threat assessment, we have Cymulate set up to automatically run that assessment and identify whether the latest threat can be exploited in our environment."

Apply threat intelligence

"When my SOC team receives intel about critical or 'famous' vulnerabilities, they inform me so that we can run Cymulate assessments and ensure we are not vulnerable."

Prioritize vulnerabilities

"Instead of dealing with a long list of vulnerabilities, my team can focus and prioritize vulnerabilities that our controls can't mitigate – all based on our Cymulate assessments."

Benefits

- **Increased team efficiency —** Cymulate's automation enables the security team to scale its testing and focus its remediation efforts.
- **Real-time visibility —** The security team no longer needs to wait for penetration tests to understand how its security is performing and where it needs to invest its resources to reduce risk.
- **Security drift management —** The security tools and infrastructure team can easily track its security controls' performance with Cymulate. The platform automatically informs the team of security drift so it can take action immediately if its controls are not performing as expected.

> Cymulate allows us to mitigate emergent threats and continuously assess our security controls, strengthening our security posture and making our fintech organization more secure.
> - Manager of Cybersecurity

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. For more information, visit www.cymulate.com.