cymulate

Bank Stays Ahead of Attackers with Cymulate Security Validation

CASE STUDY

Small security team seeks proactive validation

This small UK bank with about 1,500 employees specializes in savings accounts, mortgages and loans. With limited manpower, the team outsources its SOC and is always looking for new ways to implement cutting-edge technologies to support its mission of protecting critical systems and the personal data of its customers and employees.

The bank's Head of Cybersecurity continuously assesses compliance regulations in the field to stay on top of his team's security programming and standards. The Head of Cybersecurity had already implemented methods for security validation but believed that a more proactive and automated approach would help the bank's security program progress further. The security team faced the following challenges:

- **Lacking continuous validation**
  In addition to its annual required penetration tests, the team arranges a penetration test when a new technology is added or a new banking service is released. While these manual assessments are helpful, they provide only a point-in-time view, offering a partial picture of the bank's security posture without accounting for the evolving threat landscape.
- **Difficult to validate against emerging threats**
  The team tried to aggregate its threat intelligence from different platforms to validate against emerging threats, but the manual process was slow, unscalable and inefficient.
- **Unable to prioritize remediation**
  The team has strict lead times for remediation based on each vulnerability's criticality. However, without validating each vulnerability in the company's security infrastructure and assessing it against its defenses, the team found it challenging to understand the vulnerability's actual level of risk.

The Cymulate Solution

The Head of Cybersecurity wanted to optimize the company's existing security tools so that the team could anticipate future attacks and better protect the organization. After researching various automated security validation tools, the bank selected Cymulate. The Head of Cybersecurity recalled, "We loved that the platform's dashboard gave us immediate visibility into our security posture." Implementation was quick, and the bank's team received unmatched support.

In addition to continuously validating its security controls, the Head of Cybersecurity explained that his team uses Cymulate to assess emerging threats, streamline response, align with industry frameworks, and justify investments.

Overview

Industry	Financial Services
HQ	UK
Company Size	1,500 employees

> Cymulate ensures we get the most out of our security controls. It gives us accurate and timely assurance regarding the posture of our security program.
>
> – Head of Cybersecurity

Solution

- Breach and attack simulation

Results

- Continuously validate security
- Prioritize based on validated risk
- Map to cyber frameworks
- Fast, automated threat validation

Optimize security controls

“In the last few years, we have consolidated our security tools, and when we purchase a new tool, we use Cymulate to fine-tune it to ensure the best return on investment.”

Validate against emerging threats

“We have Cymulate set up to automatically validate any new emerging threat that the Cymulate Research Lab adds to the platform. No more manual processes, which saves us time and effort.”

Automate IoC mitigation

“The Cymulate IOC mitigation capability is invaluable for increasing the speed and accuracy of threat detection and response. It automatically uploads critical IOC data directly to our endpoint, so we can identify and address potential threats quickly.”

Prioritize based on risk

“Because we're a small team, we need to prioritize based on risk, and the Cymulate scoring allows us to do this. It provides us a full picture of our security posture and signals to us where we have potential exposures so that we can focus our efforts and resources.”

Justify investments

“Cymulate visualizes our gaps and helps rationalize our need to invest in new technologies to close those gaps. We are currently deploying a security service edge (SSE) because Cymulate showed a need for it, and we also used Cymulate to compare the different SSE vendors before we purchased the new tool. We've already seen the return on that investment.”

Map protection against cyber frameworks

“With Cymulate, we can measure and map our controls to frameworks like MITRE ATT&CK and NIST 800-53, ensuring we adhere to industry standards and best practices. The platform’s framework heatmaps allow us to visualize our strengths and weaknesses easily; we can see our gaps and track our progress to close them.”

Prove cyber resilience for audits

“When Ernest and Young were conducting an audit, they were impressed with our security program's maturity. We could easily answer their questions about our control environment with evidence from Cymulate. It showed them our investment in evaluating our organization’s threat environment and the measures we take to protect it.”

Benefits

- **Increased team efficiency** — The small security team relies on the platform's automation to boost team efficiency and maximize security activities.
- **Improved visibility** — Thanks to Cymulate risk scoring, mapping to cyber frameworks and reporting, the bank now has a clearer picture of the company’s security posture.
- **Accurate and timely assurance** — With Cymulate, the bank can independently and continuously validate its security without waiting for the next penetration test to obtain that assurance.