Cymulate

CASE STUDY

Leading Finance Company Validates MSSP with Cymulate

Challenge

With a small three-person cybersecurity team, this banking and financial services company relies heavily on security consultants and managed services for security operations and offensive testing. However, the security leader is ultimately responsible for managing the organization's security controls.

While the company had a security strategy, it wanted to ensure that all its in-house and outsourced tools and processes would protect its consumer-facing applications in case of an attack. The security leader initially contracted with red team consultants to manually assess controls. Specific challenges included:

- **Manual control validation**
  The red team manually created and coded all the assessments, taking time and effort. Because this process was manual, it was difficult to be continuous.
- **Manual validation of MSSP detection and response**
  The organization utilized red team simulated attacks to assess whether its MSSP-managed SOC services could detect and prevent them. However, because the assessments were manual, they were prone to human error and limited to only select tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs). Additionally, if a gap was found, the SOC needed to wait for the red team to report on each assessment before they could remediate any gaps, increasing time to mitigation.
- **Manual threat validation**
  To validate protection against new threats in the wild, the red team would manually create assessments based on media sources and available IOCs. With an average of 30-40 new threats a month, this was a labor-intensive, time-consuming process that delayed the organization if it was protected before an attack might occur.

To solve these challenges, the organization looked to replace its manual, time-consuming methods with automated security control and threat validation.

The Cymulate Solution

After comparing different tools on the market, the company chose Cymulate for its ease of use, scheduling of automated assessments, and actionable reporting with remediation guidance. The organization utilizes Cymulate to build an effective cyber defense by prioritizing patching, improving monitoring, and modifying incident response playbooks.

Overview

Industry: Financial Services
HQ: Mumbai, India
Company Size: 177K employees
Security Team: 3 employees

"Cymulate gives us a benchmark to work towards improvement. I can effectively plan my security roadmap by outlining the steps I need to achieve optimized cybersecurity maturity."

- CISO

"With Cymulate, the board is more confident about the strength of our security posture and ability to protect against immediate threats."

- Assistant Information Security Manager

Solution

- Breach and Attack Simulation

Results

- 60% increase in team efficiency
- Validate managed services
- Effortlessly test against emergent threats

The team also uses Cymulate to:

Continuously validate security controls
"Cymulate allows us to run continuous automated attack assessments with zero coding. The remediation guidance significantly increases our productivity, and we automatically rerun assessments to validate the changes. We can also prioritize our mitigation efforts because the platform's real-time data indicates exactly where we need to bulk up security."
- CISO

Validate and optimize SOC services
"My team is about 60% more efficient with Cymulate. Before, the red team had to validate our outsourced SOC services with manually executed attacks, which is time-consuming and limited in scope. With Cymulate, our security team quickly runs assessments that extensively cover TTPs and IOCs with significantly less effort. The platform also generates SIEM-specific queries based on Sigma rules, making mitigation more streamlined and reducing the team's mean time to detect (MTTD) and mean time to prevent (MTTP)."
- CISO

Assess against emergent threats
"Cymulate Immediate Threats is updated daily with simulations of the latest attacks so that we can immediately check if the organization is vulnerable to emerging threats. We also use Cymulate BAS Advanced Scenarios to extensively test the full kill-chain against the latest threats with chained, customizable assessments."
- Assistant Information Security Manager

Automate red teaming
"Cymulate allows us to scale our red team activities extensively with only one teamer. Our testing is more extensive and efficient, with zero code assessments, automated reporting, and easy-to-digest mitigation guidance."
- Assistant Information Security Manager

Benefits

- **Automation –** By automating assessments and automatically generating remediation guidance, the security team can work faster and more efficiently—ensuring it mitigates risk before an attack can harm the organization.
- **Prioritization –** The Cymulate technical and executive reports generate insights into where the organization's security is strong, where there are redundant tools, and where more resources are needed because of gaps. The data-based analytics enable the team to prioritize its tasks and focus on the high-risk areas.
- **Collaboration –** Cymulate provides numerous integrations to help reduce miscommunication between the SOC and red and blue teams. All detections and alerts are recorded on the Cymulate platform, so it's easy to tell if and where a gap exists.
- **Improved communication –** The CISO uses the Cymulate executive reports to communicate to the board about the organization's cybersecurity posture and demonstrate how his team mitigates and reduces risk before an incident can occur.