Cymulate

Indian Financial Services Company Validates MSSPs & Increases Security Program Efficacy with Cymulate

Overview

The company is a private finance institution based in Mumbai, India.

Challenge

The organization's security testing and validation processes with MSSPs were manual, labor-intensive, and time-consuming, putting the company at an unknown risk.

Solution

The company utilizes Cymulate to build an effective cyber defense improvement strategy by automating security validation with MSSPs, prioritizing patching, and continuous monitoring.

Benefits

Cymulate provides the company automation, prioritization, collaboration, improved communication, and increased productivity.

> *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

Challenge

The company's information security team consists of only three members, relying on nearly 30 consultants. Outsourced services include a managed SOC (security operations center) and penetration testing services. The in-house extended IT team helps manage the company's security controls. All teams work together to protect consumer-facing applications.

The main security challenge was that all security validation processes were manual and labor-intensive. The teams could not keep up and were unable to prioritize high-priority tasks, resulting in less productivity. Specific challenges included:

- **Assessing security controls –** To ensure its security controls were effective, the security team attempted to validate its controls manually. This took a lot of time and effort, mainly because the red team manually created and coded all the assessments. Additionally, because this process was manual and labor-intensive, it was difficult for it to be continuous.
- **Validating outsourced SOC detection and response –** Because the SOC services were outsourced, it was important for the organization to assess if the SOC could detect and prevent attacks. To do so, the red team manually executed attacks to see how the SOC would respond. Because this method was manual, it was prone to human error. The red team was limited in extensively testing all tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs). It also created a slow feedback loop because the SOC needed to wait for the red team to report on each assessment before they could remediate any gaps.

- **Ensuring protection against new threats –** 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 team from knowing if the organization was protected before an attack might occur.

To solve these challenges, the organization looked to purchase a security validation platform. It was vital that the tool would address everyone's needs. It should be easy to deploy and use to replace the team's manual, time-consuming methods. Another requirement was that the platform provide automation and prescriptive remediation guidance, features that would help reduce labor-intensive tasks.

The Cymulate Solution

After comparing different tools on the market, the company chose Cymulate because it fulfilled all its specifications. The organization utilizes Cymulate to build an effective cyber defense by prioritizing patching, improving monitoring, and modifying incident response playbooks. Cymulate provides:

- **Continuous security control validation –** The red team uses Cymulate Breach and Attack Simulation (BAS) and Cymulate Continuous Automated Red Teaming (CART) to run continuous automated attack assessments with zero coding, and Cymulate provides remediation guidance, facilitating quicker feedback and significantly increasing the security team's productivity. Following remediation efforts by the IT team, the red team automatically runs the same assessment to validate the changes. The team also prioritizes its mitigation efforts because the platform's real-time data indicates exactly where the team needs to bulk up its security.

  After performing the assessments, the security team uses the Cymulate MITRE ATT&CK dashboard to present to management how well they perform across the entire MITRE framework and its corresponding level of risk.

- **SOC validation and optimization –** With Cymulate, the 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. As a result, the team reduced its mean time to detect (MTTD) and mean time to prevent (MTTP).

*The organization's CISO estimates that his team is about **60%** more efficient now that it uses Cymulate.*

- **Immediate threat assessment –** The security team uses the Cymulate BAS immediate threat capability, updated daily with simulations of the latest attacks, to check if the organization is vulnerable to emerging threats. The red team has also started using BAS Advanced Scenarios to extensively test its full kill-chain against the latest threats with chained, customizable assessments.

  When the board asks the Assistant Information Security Manager if the organization is protected from the latest threat, he shows a Cymulate screenshot demonstrating that the team has already run the assessment. The Assistant Information Security Manager says, "With Cymulate, the board is more confident about the strength of our security posture and ability to protect against immediate threats."

- **Red team automation –** With Cymulate CART, the red team has increased its operational efficiency and optimized its adversarial activities. The Assistant Information Security Manager said,

> *"Cymulate allows us to extensively scale our red team activities with only one red teamer."*

  The small red team's testing is more extensive and efficient, with zero code assessments, automated reporting, and easy-to-digest mitigation guidance.

- **New product evaluation –** When evaluating vendors during a POC, the team uses Cymulate BAS and Cymulate CART to test the different products within its environment and help determine which tool works best.

Benefits

The Cymulate platform provides the company with many 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 get recorded on the Cymulate platform, so it's easy to tell if and where a gap exists. The platform's easy-to-digest remediation guidance also promotes collaboration between the teams.

Improved communication
The CISO uses the Cymulate executive reports in monthly meetings with management. He communicates to the board about the organization's cybersecurity posture and demonstrates how his team mitigates and reduces risk before an incident can occur.

Productivity
The CISO says, **"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."** Cymulate delivers a long-term strategy where the organization solves its immediate security challenges and grows along with the platform to use more capabilities as it advances its security maturity.

About Cymulate

Cymulate provides organizations with comprehensive security control validation and in-depth insights into breach feasibility. This modular solution addresses a wide variety of business and technical use cases and scales from out-of-the-box simulations to full customization for advanced attack simulations. With Cymulate, companies assess, optimize, rationalize, and prove their security program with minimal resource investment. Security professionals and business stakeholders leverage these insights to reduce cyber risk, justify investments, provide proof of security resilience to executive leadership, and to gain evidence for compliance and regulatory purposes.