cymulate

CASE STUDY

Large Insurer goes Beyond Breach and Attack Simulation (BAS) with Cymulate

Challenge

For one of the largest financial services companies in Brazil, strong cybersecurity controls are a must to protect the business of life insurance, pension plans, capitalization and benefits management. With 38 branches, more than 3,000 employees, and over 5,000 digital assets, the security team recognized the need for a continuous and reliable method to validate the effectiveness of its security controls and verify its incident detection and response processes.

Even with an in-house red team and an experienced information security team, the manual validation process was expensive and time-consuming for the security analysts. The company looked for alternatives to accelerate and automate its security control validation process so it could keep up with the growing threat of malware, phishing and other attacks.

The cyber defense team purchased a BAS (breach and attack simulation) solution to solve this challenge but still faced high costs and manual work. Although the practice of executing attack simulations was very effective, the security team still faced the following obstacles:

- **The assessments and reporting were not comprehensive.**
  The BAS tool did not provide complete visibility because it lacked web application protection capabilities, full kill-chain assessments, and phishing assessments. Additionally, the team couldn't gain practical insights from the platform's reporting to confidently make data-based decisions.
- **There was no ability to integrate with other security tools.**
  Because there were no integrations, it was time consuming to analyze and measure the results of an assessment, making it difficult to improve security tool detection and response capabilities.
- **Scheduling automated assessments was complicated and time-consuming.**
  The team required automated assessments so they could effortlessly and continuously validate their security, but to do so on the BAS platform required advanced knowledge and assistance from the information security team.

The Cymulate Solution

After diligent research and evaluation, the company chose to implement Cymulate Breach and Attack Simulation to replace its current tool and take its security control validation to the next level.

Overview

Industry	Insurance
HQ	Brazil
Company Size	1K-5K employees

> Cymulate brings agility and confidence to the company's cybersecurity posture.
> — Cybersecurity Manager

Solution

- Breach and attack simulation
- Continuous automated red teaming

Results

- Comprehensive security validation
- Data-based analytics
- Improved operational efficiency

The organization's cybersecurity manager explained that Cymulate provides his team with:

Comprehensive assessments

"Cymulate evaluates each attack vector separately, including email gateway, web gateway, WAF and endpoint, as well as assesses against emergent threats. The security team can also run full kill-chain assessments to evaluate the overall effectiveness of its security control configuration. Additionally, the lateral movement capability enables the team to challenge its internal network configuration and segmentation policies."

Integrations with other security tools

"We can easily integrate our existing security tools with Cymulate via APIs. The integrations provide complete visibility of our SOC's detection and response to simulated attacks, without needing to access each tool separately to analyze the generated logs. This helps us prioritize gaps that are exploitable in the network. When threats are undetected, Cymulate provides detailed remediation steps and custom queries to include in the SIEM."

Easy-to-automate simulations

"Because Cymulate works in agentless mode, my team was able to immediately begin running simulations, without having to install any equipment. The platform's easy to use automated assessments ensure continuous validation, for all skill levels. Since using Cymulate, our red team has significantly reduced its manual labor."

Phishing assessments

"With the Cymulate phishing awareness capability we can carry out large phishing campaigns to increase cyber awareness among our employees."

Benefits

- **Increased efficiency** — Cymulate was simple to implement, and the security team began running assessments almost immediately. Overall, the team has decreased manual labor and increased operational effectiveness.
- **Enhanced communication** — The platform increased communication between all the cyber teams at the organization, including vulnerability management, SOC, incident response, and the red team. Each team works together to analyze the results of the attack simulations, so they can create countermeasures to detect and contain threats.
- **Improved visibility** — The technical and executive reports provide increased visibility of various security activities that are relevant to the audience who receives the report. As a result, executives don't need to muddle through the technical details, and the cyber defense analysts get all the granular data they need.