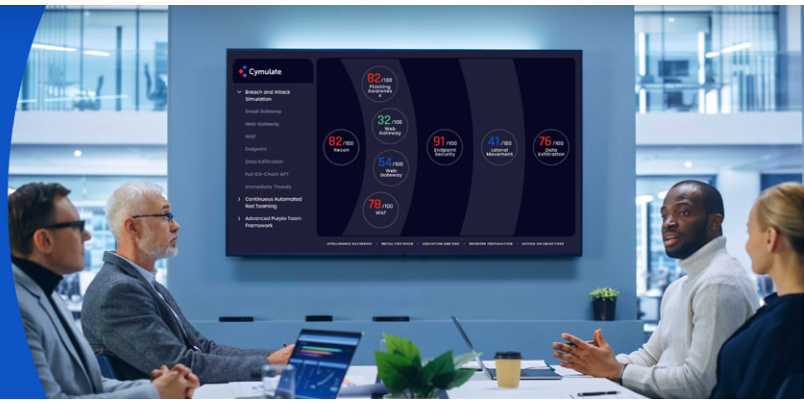
Cymulate

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



Organization

This organization is one of the largest insurance companies in Brazil and specializes in life insurance, pension plans, capitalization, and benefits management. The company has 38 branches and has more than BRL 6.5 million in customers.

Security Challenges

The insurance company has more than 3,000 employees with over 5,000 digital assets on its network. Because of the sensitive data that the company handles, it needed a continuous and reliable method to validate the effectiveness of its security controls, as well as verify its incident detection and response processes. Even with an in-house red team and 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 faced the following obstacles:

- **The assessments and reporting were not comprehensive.**
  The BAS tool did not provide the team complete visibility because it lacked web application protection capabilities, as well as the ability to run assessments across the full kill-chain. Additionally, the tool was unable to assess phishing awareness. The platform's reporting did not provide sufficient insights for the team to confidently make data-based decisions.
- **There was no ability to integrate with other security tools.**
  Because there was no integration, 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 attention from the information security team.

Challenge

The security team wanted to implement a continuous security validation strategy, but their BAS tool was not comprehensive or easy to automate.

Solution

The insurance organization implemented Cymulate for end-to-end security validation which provided automated comprehensive assessments, integrations, and advanced reporting.

Benefits

Increased communication and visibility between teams has led to better countermeasures to detect and contain threats, improving operational effectiveness.

Cymulate

Solution

After diligent research and evaluation, the company chose to implement Cymulate's Extended Security Posture Management platform to replace its BAS tool and take its security control validation to the next level. Cymulate provides:

- **Comprehensive assessments**
  The platform evaluates each attack vector separately, including email gateway, web gateway, WAF, endpoint, and immediate threats. The assessments are based on the MITRE ATT&CK framework, so the security team knows exactly where they need to focus their efforts to reduce risk.

  The Phishing Awareness module enables the security team to carry out large phishing campaigns to increase cyber awareness within the company. The security team can also run Full Kill-Chain Campaigns to evaluate the overall effectiveness of their security control configuration from the perspective of an attacker. Additionally, the Lateral Movement module enables the team to challenge their internal network configuration and segmentation policies.

- **Integrations with security tools**
  The insurance organization easily integrates its existing security tools with Cymulate via API. The integrations provide complete visibility of the SOC's detection and response to simulated attacks, without needing to access each tool separately to analyze the generated logs. This allows the security team to prioritize remediation of gaps that are exploitable in the network. When threats are undetected, the platform gives detailed remediation steps and queries to include in the SIEM.

- **Easy-to-automate simulations**
  Because Cymulate works in agentless mode, the security team was able to immediately begin running simulations, without having to install any equipment. Additionally, the platform provides easy to use automated assessments to ensure continuous validation, for all skill levels. Following each assessment, the platform also automatically provides both technical and executive reports. Since using Cymulate, the red team has significantly reduced its manual labor.

Benefits

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.

The platform increased communication between all the cyber teams at the organization, including vulnerability management, SOC, computer security 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.

Additionally, 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.

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

Contact us for a live demo, or get started with a free trial

Start Your Free Triel

Headquarters: Maze St 3, Tel Aviv 6578931, Israel | +972 3 9030732 | info@cymulate.com | US Office: +1 212 6522632