Security Control Validation
Solution Brief

Investing in security controls is not a one and done operation. Out of the box configurations and a "trust the vendor" strategy to keep the controls optimized and current is bound to fail. Security controls need to be continuously validated. Traditional testing methods, such as pen testing, are limited in scope and out of date by the time the test results are reported. Additionally, security operation teams are unable to validate security controls because they are busy with other vital tasks and they usually don't have the necessary adversarial skills.

Gaps in security controls are caused by:

Undetected product deficiencies

Emerging threats

Policy misconfigurations

Vulnerabilities

Dynamic IT infrastructures

Business constraints

Comprehensive Security Control Validation

Cymulate automates security control validation with a continuous offensive approach to detect and remediate security gaps. Simulated attacks are organized by attack vector and mapped across the MITRE ATT&CK® framework, helping to identify systematic weaknesses and security drift.

Simple	Customizable	Comprehensive	Prescriptive
Out-of-the-box assessments make it easy to validate & optimize security controls	Customizable assessments are available for more advanced users	Dynamic reporting & analytics provide technical & executive teams data tailored to their specific needs	Easy-to-digest mitigation guidance following each assessment focuses remediation efforts

Assess These Security Controls

Email Gateway

The Email Gateway module enables organizations to test and optimize email security posture. The module challenges email security controls against a comprehensive set of attacks by sending emails with attachments containing ransomware, worms, trojans, or links to malicious websites. The simulation reveals which malicious emails, file types and embedded files that could potentially reach employees' inboxes.

Web Gateway

Organizations validate their web security controls with the Web Gateway module. This module challenges the controls that protect employees from both accessing and downloading malware from malicious and compromised websites. It tests inbound protection against thousands of different simulated malicious files and exploits, and outbound protection against a feed comprised of thousands of URLs, which are updated daily.

WAF Gateway

The Web Application Firewall (WAF) Gateway module empowers organizations to test and optimize their web security controls. The module first identifies all the forms of data import available on the target domain and then challenges the WAF against thousands of attacks (including OWASP top payloads, command injection and file inclusion attacks) to assess the integrity of the WAF configuration and its blocking capabilities.

Data Exfiltration

Organizations use the Data Exfiltration module to test the effectiveness of Data Loss Prevention (DLP) security controls. This module challenges DLP controls with a broad range of synthetic regulatory, company confidential, and custom data sets. The module packages the data into different file types, including images and office files, and attempts to exfiltrate them using multiple exfiltration methods.

Endpoint Security

The Endpoint Security Assessment module enables organizations to test and optimize the effectiveness of their endpoint security. The module challenges endpoint security controls against a comprehensive set of attacks that simulate malicious behavior of ransomware, worms, trojans and other types of malware. Security teams can create custom attack scenarios using hundreds of commands across the cyberattack kill-chain, mapped to the MITRE ATT&CK Framework.

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

Start Your Free Trial

+972 3 9030732 | info@cymulate.com