Cymulate Extended Security Posture Management Modules

Does managing your cybersecurity seem over-complex?

Every day brings change to your security posture. Changes in the IT architecture modify the attack surface, configuration changes to security controls introduce unforeseen security gaps , and new threats to avoid are introduced every day.
It seems impossible to know how effective your security controls are right now, which digital assets are exposed, how the network can be penetrated, what requires fixing, and what to prioritize.

Penetration testing is not enough as by the time you get the reports they are outdated and irrelevant. Other alternatives may give you a current picture, but it is usually just partial. Maintaining a robust security posture and keeping risk low requires you to continuously monitor your security program's performance, end-to-end.

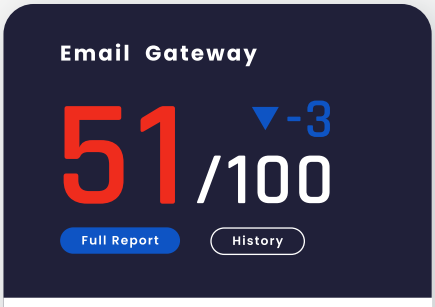
Manage your security posture with Extended Security Posture Management

Cymulate SaaS-based Extended Security Posture Management (XSPM) platform deploys within minutes, enabling security professionals to continuously challenge, validate and manage the optimization of their cybersecurity posture end-to-end, across the MITRE ATT&CK® framework. The platform includes Breach and Attack Simulation (BAS) technology ranked #1 in innovation by Frost & Sullivan in the 2021 BAS Radar™, Continuous Automated Red Teaming (CART), and Advanced Purple Teaming Framework. With Cymulate, you can run out-of-the-box or customized assessments, as well as test your security against the latest emerging threats. These assessments are simple to deploy and use for all maturity levels and they are constantly updated. It also provides an open framework to create and automate purple and red teaming by generating penetration scenarios and advanced attack campaigns tailored to unique environments and security policies.

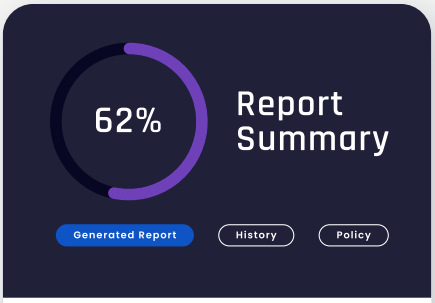
How it works

Cymulate empowers you to manage your security posture based on real-time data, 24 hours a day, 7 days a week, 365 days a year in just three simple steps:

1 Simulate
Simulate attacks across any vector.



2 Evaluate
Know where your company is exposed.



3 Remediate
Fix your security gaps.

Security Posture Management Modules

Testing with Intelligence

The Cymulate **Attack Surface Management module** discovers what a hacker can find out about your company during the initial information gathering phase of an attack. The module identifies and fingerprints your domains and sub-domains to discover internet facing weaknesses and vulnerabilities. It also looks for Open Source Intelligence (OSINT) to uncover leaked credentials and organizational information that can be used in an attack.

Testing Your WAF Security

The **Web Application Firewall (WAF) module** enables you to test and optimize your web security controls. This vector first identifies all the forms and other means 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.

Testing Your Email Security

The **Email Gateway module** enables you to test and optimize your email security posture.
This module challenges your 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 your employees' inbox.

Securing Your Web Gateway

The **Web Gateway module** validates your organization's web security controls. This module challenges the controls that protect employees from both accessing and downloading malware from malicious and compromised websites. The module 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.

Challenging Your DLP Controls

The **Data Exfiltration module** enables you to test the effectiveness of your Data Loss Prevention (DLP) security controls and optimize them.
This module challenges your 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. The attack simulation results are presented in a comprehensive and easy-to-use format, allowing organizations to understand their DLP-related security gaps and take the appropriate measures to remediate.

Safeguarding Your Internal Network

The **Lateral Movement (Hopper) module** challenges your internal network configuration and segmentation policies against different techniques and methods used by attackers to propagate within the network and control additional systems.
The module simulates an adversary that has control over a single workstation and attempts to move laterally within the organization. The result of the assessment is a visualization of all the endpoints that the assessment was able to reach with a detailed description of the methods used for every hop.
The assessment identifies infrastructure weaknesses, network misconfigurations and weak passwords, and provides guidance to remediate them.

Cymulate

Improving Security Awareness

The **Phishing Awareness module** enables you to evaluate employee security awareness. It provides all the resources required to create, customize, launch and measure phishing campaigns.
Each campaign is tracked for 5 different actions (opening, clicking, entering credentials, reporting and completing a quiz) providing the full picture of employee security awareness levels, enabling the organization to focus on those that require more education and monitoring than others.

Simulating Full Kill-Chain APT

Full Kill-Chain APT module enables you to test, measure and improve the effectiveness of your security controls against real-world Advanced Persistent Threats (APT). The module provides pre-defined templates for testing against well-known APT groups and enables red teams to create their own APT attacks from tens of thousands of attack simulations across the entire kill chain, including Email, Web, Phishing, Endpoint, Lateral Movement and Data Exfiltration.

Automating Purple Teaming

Advanced Scenarios operationalizes the MITRE ATT&CK® framework to create, launch and automate custom attack scenarios. In addition to the extensive library provided out-of-the-box, security staff can craft or modify executions to create both simple and complex scenarios of atomic, combined, and chained executions. The module enables APT simulation, purple team exercises, incident response playbook exercises, pro-active threat hunting and automates assurance procedures and health checks.

Testing Your Endpoint Security

The **Endpoint Security Assessment module** enables you to test and optimize the effectiveness of your endpoint security. The module challenges your endpoint security controls against a comprehensive set of attacks that simulates malicious behavior of ransomware, worms, trojans and other types of malware. Red team testing enables the creation of custom attack scenarios using hundreds of commands across the cyberattack kill chain, mapped to the MITRE ATT&CK Framework.

Defending Against the Latest Attacks

The **Immediate Threat Intelligence module** enables you to safely test and optimize your organization's security posture against specific, real and emerging cyber threats. The module is updated daily by Cymulate security analysts that monitor the web for new threats. The Immediate Threat Intelligence module tests email, web gateway, and endpoint security controls.

Prioritizing Your Vulnerabilities

The Attack–Based Vulnerability Management (ABVM) dashboard is an add-on to Cymulate's security control validation process. ABVM integrates with common vulnerability scanners to combine the data on found vulnerabilities with the results of Cymulate's simulated attacks. The dashboard correlates the criticality of vulnerabilities with the value of assets so you can optimize patching prioritization and reduce the patching workload.

About Cymulate

The Cymulate SaaS-based Security Posture Validation Platform provides security professionals with the ability to continuously challenge, validate and optimize their on-premises and cloud cyber-security posture with end-to-end visualization across the MITRE ATT&CK® framework. The platform provides automated, expert, and threat intelligence-led risk assessments that are simple to deploy, and easy for organizations of all cybersecurity maturity levels to use. It also provides an open framework for creating and automating red and purple teaming by generating tailored penetration scenarios and advanced attack campaigns for their unique environments and security policies.

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

Start Your Free Trial

info@cymulate.com | www.cymulate.com