Cymulate for MSSPs and MDR/XDR Providers

Managing customers' security operations, infrastructure, and threat detection and response is challenging, even if technology is operating effectively and processes are efficiently executed. Managed Security Service Providers (MSSPs) and Managed/Extended Detection and Response (MDR/XDR) providers are expected to meet high security service demands, many times without having full control over the environments that they need to secure. In addition, it is difficult to demonstrate the value of a client's investment and monitor their security posture over time.

Cymulate offers MSSPs a way to provide more value to their customers by validating security control efficacy, adapting controls to changing environments and threats, and assisting organizations in making informed decisions about their security stack.

Benefits

Cymulate enables MSSPs and MDR/XDR providers to:

Generate Additional Recurring Revenue
Identify new services to offer customers and attract additional clients, create and implement security projects, and enhance technology solutions.

Meet SLAs
Adopt a continuous security validation strategy to discover and reduce mean time to detect (MTTD) and mean time to respond (MTTR), enhance processes, tune solutions, and do more with fewer resources.

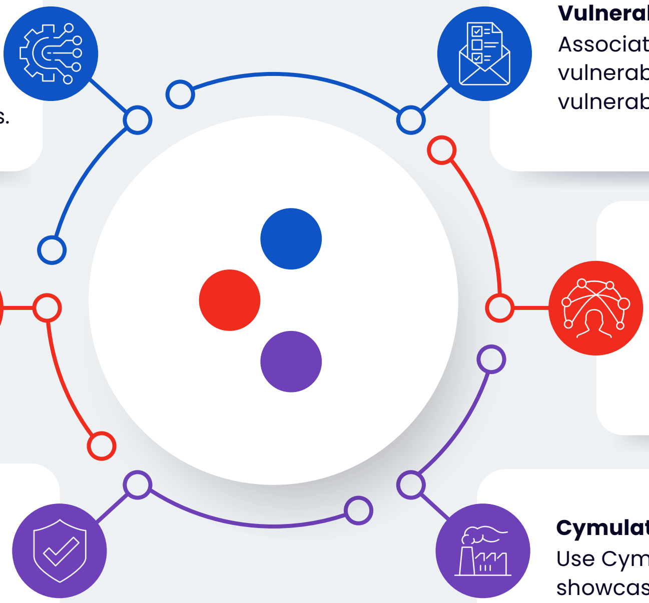
Minimize Operational Costs
Cymulate deploys in minutes and requires minimal pre-requisites to be effective. Launch an attack from one dashboard for multiple clients, simultaneously, and easily conduct regularly scheduled assessments with out-of-the-box templates.

Make Quick Data-Based Decisions
Dynamic dashboards, technical and executive reporting, and a rich UI generate easy to digest analytics. Use this data to baseline and track security posture, enhance controls, and deliver management ready reports across the portfolio.

Create Customizable Dashboards and Reports
Select relevant data per client or group of clients, filter it, and present it in graphs, charts, or metrics in a few clicks. The reports can be emailed or exported as a PDF for clients who don't have direct access to the platform.

High-Level MSSP Use Cases

Examples of existing MSSP offerings augmented by Cymulate's capabilities



Embed within MDR/XDR
Ingest Cymulate generated data or embed Cymulate within an MDR/XDR service package to supercharge generation of use cases and detections.

Program Baseline & Monitoring
Measure and track data related to an organization's maturity to demonstrate improvement or regression over time.

Proactive Security Validation
Simulate attacks against an organization to validate the efficacy of existing security controls. Use the results to improve the organization's security posture.

Vulnerability Prioritization
Associate attack data with vulnerability scans to identify the most vulnerable assets.

SOC Optimization
Improve a SOC team's ability to detect, alert, and respond to actual security threats and behaviors.

Cymulate Powered Projects
Use Cymulate assessments to showcase the need for a special project related to security technologies and controls.

Partner Delivery Approaches

Partners can deliver and operate Cymulate in three ways:

	Cymulate-as a-Service	Co-managed	Reseller
Operation & Management	MSSP	MSSP and customer	Partner resells the Cymulate license to the client OR the license is procured by the customer through another fulfillment
Support	MSSP	MSSP and Cymulate	
Customer Access to the Platform	✗	✓	✓
Pricing Model	Annual subscription or utilization-based	Annual subscription	Annual subscription

The Most Comprehensive Security Validation Technology

Cymulate's Extended Security Posture Management platform provides an end-to-end overview of an organization's security posture. This framework presents a comprehensive understanding of current levels of risk, exposure, drift, and even potential savings.

Security Controls Validation

Breach and Attack Simulation - Cymulate's Breach and Attack Simulation (BAS) technology was ranked #1 in innovation by Frost & Sullivan in the 2022 BAS Radar. Cymulate's BAS combines red (offense) and blue (defense) activities. It simulates thousands of attack scenarios and correlates them to security control findings through API integrations, as well as provides actionable detection and mitigation guidance.

- **Immediate Threat Intelligence** – Save time on threat research with prepackaged threat intelligence-led assessments that are updated daily, including samples, IoC's CVE's, detections, and mitigations.

Advanced Purple Teaming - Advanced Purple Teaming expands BAS into the creation and automation of custom advanced attack scenarios. Customized scenarios can be used to exercise incident response playbooks, pro-active threat hunting and automate security assurance procedures and health checks. Advanced Purple Teaming is primarily used by security practitioners with adversarial skills, including red teamers and pen-testers.

Attack-Based Vulnerability Management

Cymulate's Attack–Based Vulnerability Management (ABVM) integrates with leading third-party vulnerability management solutions and cross-references information on vulnerabilities provided by these vendors, along with the analysis from Cymulate's ABVM, and offers a practical view of compensatory security controls over unpatched vulnerabilities in the network. Cymulate's ABVM enables organizations to accurately prioritize remediation and patching or reconfiguration of compensating security controls.

Breach Feasibility

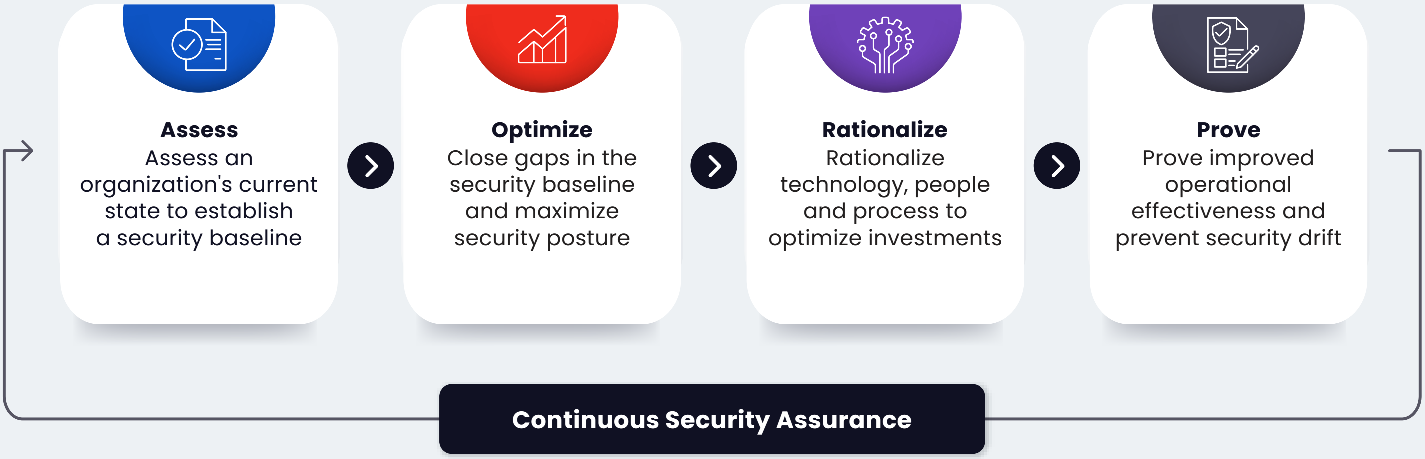
External Attack Surface Management - Cymulate's External Attack Surface Management (ASM) technology emulates real attackers to identify digital assets (such as domains, IP addresses, and more) and assesses their exploitability against the organization's security policies and solutions. With findings mapped to the MITRE ATT&CK® framework's TTPs (Tactics, Techniques, and Procedures), business enterprises can take the necessary mitigation steps.

Automated Red Teaming - Cymulate's automated red teaming capability amplifies attempts to penetrate the organization by deploying attack techniques that evade detection controls and gain an initial foothold within the network. It can also trigger the attack with a well-crafted phishing email. After gaining the initial foothold, the attack subsequently tests network segmentation policies by lateral movement within the network in search of a pre-defined objective.
Blue teams leverage Cymulate's adversarial capabilities to assess their cybersecurity resilience, and companies that have in-house red teamers benefit from customization and automation to increase their operational efficiency.

Cymulate

Know, Control, and Optimize an Organization's Cybersecurity Posture

Cymulate enables MSSPs to deliver a continuous security assurance program to their clients



Assess
Assess an organization's current state to establish a security baseline

Optimize
Close gaps in the security baseline and maximize security posture

Rationalize
Rationalize technology, people and process to optimize investments

Prove
Prove improved operational effectiveness and prevent security drift

Continuous Security Assurance

Why Cymulate

- Deploys in Minutes
- Comprehensive In-Depth Validation
- End-to-End Visibility
- Vulnerability Prioritization Technology
- Red & Purple Teaming Framework
- Immediate Threat Intelligence

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