

# 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 validate security control efficacy, adapt controls to changing environments and threats, and assist organizations in making informed decisions about their security stack.

## Benefits

Cymulate enables your business to:



### Generate Additional Recurring Revenue

Identify new services to offer your 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 your 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 your portfolio.

## 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.



### Vulnerability Prioritization

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



### Program Baseline & Monitoring

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



### SOC Optimization

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



### 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.



### 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
<b>Operation &amp; Management</b>	MSSP	MSSP and customer	Partner resells the Cymulate license to the client OR the license is procured by the customer through another fulfillment
<b>Support</b>	MSSP	MSSP and Cymulate	
<b>Customer Access to the Platform</b>	✗	✓	✓
<b>Pricing Model</b>	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 2021 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.



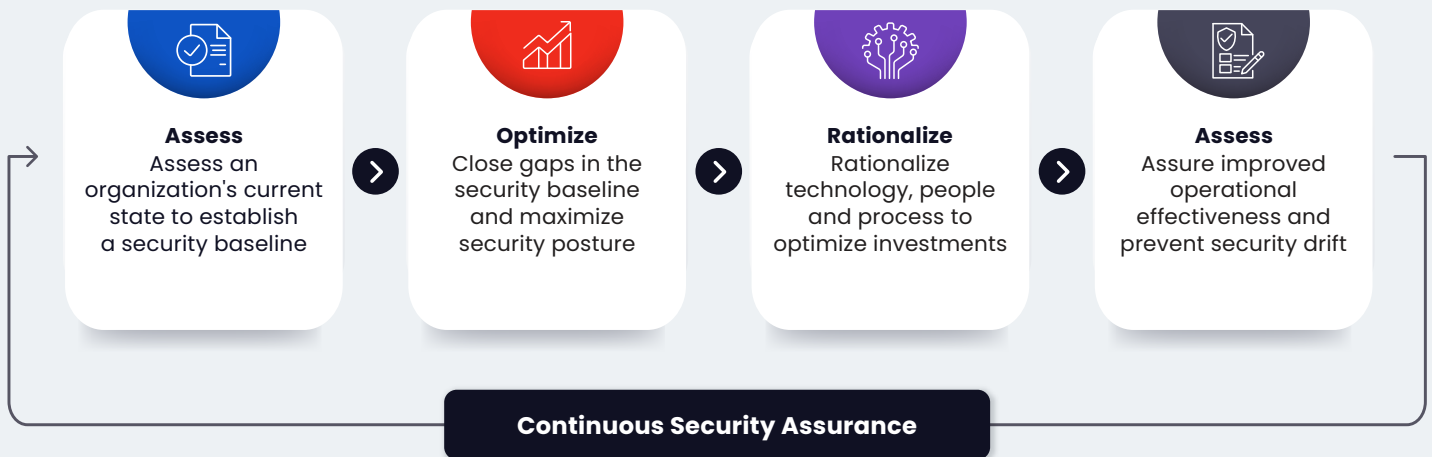
### Breach Feasibility

**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.

**Red Teaming Automation** – Cymulate's red teaming automation 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.

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

Cymulate Extended Security Posture Management (XSPM) enables MSSPs to deliver a continuous security assurance process to their clients



### 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

Cymulate was established with the vision of empowering security professionals to make better decisions faster, based on real-time data. Founded and led by an elite team of cyber researchers with world-class experience in offensive cyber solutions, Cymulate is determined to become the golden standard for security professionals and leaders to know, control, and optimize their cybersecurity posture end to end. Trusted by hundreds of companies worldwide, Cymulate constantly enhances its methods to prepare organizations for any attack scenario or campaign. With Cymulate, organizations continuously measure security performance in real-time, shore up defenses, and assure operational effectiveness. **Measuring your cybersecurity performance is fundamental towards creating a more secure organization!**

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

[Start Your Free Trial](#)