cymulate

SOLUTION BRIEF

Optimize Threat Resilience

Proactive Security Builds Threat Resilience

Cyber risk is business risk. With more than **80% of boards** treating cybersecurity as a strategic business concern, security leaders recognize that their mission is to build the resilience to withstand the next attack.

Evolving beyond assumed-breach and over-reliance on detection and response, security leaders recognize both the need and opportunity for a more proactive approach to security that continuously adapts defenses for the next threat.

This is the essence of threat resilience.

Prove the Threat, Improve Resilience

By continuously testing your defenses against the latest advanced threats and the full kill chain of attack techniques, the Cymulate Exposure Management Platform provides the continuous validation, automation and insights to:

- Prove your resilience to the most advanced cyber attacks
- Optimize security controls to improve threat resilience
- Accelerate detection engineering
- Measure and baseline security posture

The Cymulate Exposure Management Platform automates production-safe breach and attack simulations for offensive testing that continuously validates security controls using the latest threat tactics and real-world attack techniques.

Threat Validation for Essential Security Controls

- Endpoint security
- Email gateway
- SIEM detection
- Cloud workload protection
- Cloud detection and response
- Web application firewall
- Web gateway
- Firewall / IPS
- Data loss prevention

The results of these assessments highlight the gaps and weaknesses in your security defenses and provide you with remediation guidance to tune and optimize your controls. As a SaaS solution designed for simple and fast deployments, Cymulate enables organizations to fortify their cyber defenses, reduce their exposure to cyber threats and prove their state of cyber resilience.

Validate Resilience to Today’s Threats

With a daily feed of new active threats, the Cymulate Exposure Management Platform automates breach and attack simulations of the latest immediate threats to prove your state of resilience. The Cymulate Research Labs monitors the threat intelligence community daily to update the Cymulate platform. New threat alerts are typically loaded as immediate threat simulations within 24 hours of the alert being published.

Benefits

30% ↑ in threat prevention

Improve threat prevention by mitigating proven exposures and optimizing security controls.

3x ↑ in threat detection

Build, test and tune new threat detections in hours, not weeks.

Test new threats in <1 hour

Automate continuous validation of threats with daily updates of new attacks and campaigns.

> Cymulate integrates with our XDR to improve our threat detection and response. Cymulate automatically uploads critical threat data directly to our XDR to ensure that potential threats are identified and addressed quickly, without manual intervention.
>
> – Senior Security Manager, Singapore Bank

Baseline Security Posture and Identify Drift

With ongoing automated testing, Cymulate creates a baseline of security posture, unexpected decreases in threat coverage and provides proof of the current state of cyber resilience. Key features include:

- Security control dashboards and MITRE ATT&CK heatmaps highlighting strengths, weaknesses and exposure levels
- Technical and executive-level reports provide proof and evidence of security posture with performance trending
- Drift analysis that identifies changes in security control configurations and the environment that impact security posture
- Industry benchmarking to compare security effectiveness to peers

Optimize Threat Prevention and Detection

Cymulate provides actionable and automated remediation and mitigation. Cymulate integrates with security controls to mobilize action with recommended detection and automated mitigation to block active threats.

Go from exposure to mitigation with immediate prevention

When Cymulate identifies a threat that was not prevented, the platform includes the option to push updates for that specific threat directly to the security control for immediate threat prevention. By combining validation and mitigation, the Cymulate platform gives security teams the technology and integrations to automate manual tasks to optimize threat resilience.

Build custom detection rules

Based on testing results and gaps in threat coverage, Cymulate provides custom detection rules. Depending on the threat and security control, these Cymulate detection rules follow industry standards like Sigma or include query translators to map recommended rules to the vendor-specific format for SIEM, EDR and XDR.

Map SIEM rules to attack library with AI

Cymulate integrates with SIEMs to validate existing detection rules by applying AI to match relevant attack scenarios for each detection rule. Cymulate validates whether rules trigger as intended, uncover detection gaps and receive targeted recommendations to improve rule logic. With built-in automation, Cymulate makes it easy to continuously test and tune rules, ensuring lasting protection against evolving threats across the full kill chain.

> **Using the Cymulate integrations, we launch assessments to see if our tools detect them. If they don’t, Cymulate provides mitigation guidance and Sigma rules, and we easily rerun the assessments to validate remediation.**
>
> – Karl Ward, Head of Cybersecurity, LV=

Why choose Cymulate?

Continuous Threat Validation

Best-in-class exposure validation with a single platform to optimize controls, scale offensive testing and provide essential exposure insights.

Simple Automation

Advanced testing for any blue or red teamer to run and customize with templates, best practices and AI assistant to scale offensive testing.

Put the “T” in CTEM

Make threat validation a continuous process with collaboration across security operations, threat intel and vulnerability management teams.

Contact us for a live demo **Start Your Live Demo** info@cymulate.com www.cymulate.com