DATA SHEET

Cymulate Exposure Management Platform

Prove the Threat, Improve Resilience

Exposure management without the context of validation is just old-school vulnerability management. To build true threat resilience, cybersecurity teams must build exposure management programs that integrates discovery and validation.

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

- Prove and optimize resilience to the most advanced cyber attacks
- Accelerate detection engineering
- Drive continuous threat exposure management
- Measure and baseline security posture

Validation Made Easy with Automation & AI

Cymulate combines the best of adversarial exposure validation with breach and attack simulation (BAS) and continuous automated red teaming (CART) to prove threat resilience with empirical evidence that can only come from live, offensive testing.

The Cymulate platform includes automation to scale offensive testing and artificial intelligence-powered workflows that make advanced customized testing easy for every security team.

With a library of the most advanced attack actions, Cymulate provides templates for best practices and includes daily updates for new active threats and complex attack campaigns. To validate the threats that impact your organization, Cymulate applies AI to scope your testing based on critical factors such as industry threat actors, critical assets and team resources.

For more advanced custom testing, red teams rely on the attack scenario work bench to build and run complex, chained attacks. To build new custom testing in minutes, the Cymulate platform includes an AI-powered template creator that converts threat advisories, plain language commands and SIEM rules into custom testing that scales across systems and cloud deployments.

Measure and Benchmark Threat Resilience

While automation makes validation a daily and weekly process, Cymulate provides the insights, heatmaps and dashboards for security leaders to measure their true state of threat resilience and teams to track their progress with metrics such as:

- Threat prevention and detection
- Coverage of MITRE ATT&CK tactics and techniques
- Exposures mitigated with security controls

Benefits

30%↑ in Threat Prevention

Optimize threat prevention by finding your weaknesses and updating 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.

52% ↓ in Critical & High Exposures

Prioritize exposures based on exploitability with proof of threat resilience and effective mitigation.

Escalate High-Risk, Low-Severity

Elevate low and medium exposures that are exploitable and impact critical assets.

Backed by the Industry

FROST & SULLIVAN
FROST RADAR LEADER
cymulate
Frost Radar™ :Automated Security Validation, 2024

Gartner
Peer Insights
Customers' Choice 2024

Exposure Prioritization: Focus on the Exploitable

Cymulate applies the proof of your threat resilience to prioritize the exposures that are actually exploitable. By integrating with vulnerability scanners and other exposure discovery tools, Cymulate aggregates exposures and then stack ranks them based on validated exposure scoring that considers:

- Proof and evidence of threat prevention and/or threat detection
- Threat intelligence for known exploits, threat actors and active campaigns targeting your industry
- Business context and asset criticality

Optimize Threat Resilience with Actionable and Automated Mitigation

Because threat resilience requires continuous evolution to stay ahead of the next threat, Cymulate provides actionable and automated threat mitigation. Cymulate findings include remediation guidance and mitigation that includes:

- Automated security control updates to update prevention for new threats
- Custom detection rules directly applied to endpoint security, SIEM and XDR
- Recommended configuration changes

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.

About Cymulate

Cymulate is the leader in exposure management that proves the threat and improves resilience. More than 1,000 customers worldwide rely on the Cymulate platform to prove, prioritize and optimize their threat resilience as they make threat validation a continuous process in their exposure management programs. For more information, visit www.cymulate.com.