cymulate

SOLUTION BRIEF

Continuous Threat Exposure Management

Managing Exposures at Attacker Speed

In a post-Mythos era, attackers are weaponizing vulnerabilities at an unprecedented speed. They are shrinking the window between disclosure and active exploitation from weeks to days, and in some cases, hours. Organizations can no longer rely on periodic assessments or traditional vulnerability management alone. They need to continuously validate which exposures are truly exploitable and prioritize remediation based on real-world risk.

Cymulate enables Continuous Threat Exposure Management (CTEM) by unifying security operations, vulnerability management, red and purple teams to continuously identify, validate, prioritize and mobilize the exposures that matter most. By combining real-world attack simulation with exploitability intelligence and business context, organizations focus resources where they will have the greatest impact on cyber resilience.

Accelerate CTEM with Agentic Cyber Defense Engineering

Cymulate Agentic Cyber Defense Engineering transforms an organization's CTEM program by accelerating each phase of the CTEM lifecycle. By combining real-world threat intelligence, attack simulation and intelligent automation for exposure validation, Cymulate enables organizations to:

- Identify threats most relevant to their environment
- Automatically configure security assessments and validate exploitability
- Prioritizes exposures with risk-based contextual scores
- Mobilize fixes for exposures with automated remediation
- Verify successful remediation with exposure validation

With Cymulate, security teams have data-driven continuous confidence that their security controls are preventing and detecting the attacks that matter most to them. Organizations reduce exposures faster and continuously prove their threat resilience with validation.

> Dealing with vulnerabilities used to be a lot more time-consuming. With Cymulate, I can quickly see which vulnerabilities will impact the organization and prioritize patching and mitigation.
>
> – CISO, Retail

Solution Benefits

> 90% threat prevention

Improve threat prevention by mitigating exploitable vulnerabilities

60% more efficient prioritization

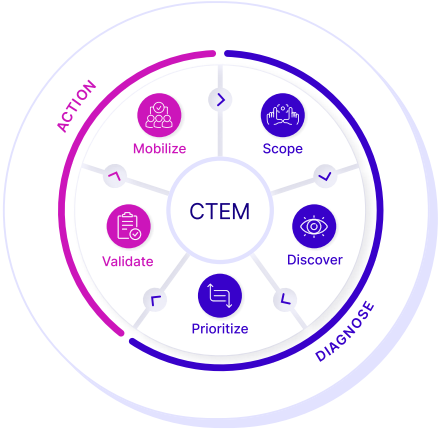
Focus remediation on validated exposures that pose real risk

95% reduction in critical exposures

Reduce critical exposures by validating exploitability and prioritizing real-world risk

> 50% threat detection

Continuously validate, build and deploy new rules to improve threat detection.



Cymulate Automates the CTEM Lifecycle with Agentic AI

The Cymulate Platform delivers value across all five phases of the CTEM lifecycle through seamless integrations, intelligent automation and innovative agentic AI workflows powered by Vero AI. By connecting traditionally siloed offensive and defensive security teams, Cymulate enables continuous collaboration, automated validation and accelerated mobilization.

Scoping with business context to baseline security posture

Cymulate uses environment-aware AI agents to establish and maintain a dynamic baseline of your organization's security posture by understanding your industry, APTs, attack surface, integrated security ecosystem, business-critical assets and current threat landscape.

Discovery and correlation of exposures to threats

Cymulate integrates with scanners, asset management and more to centralize and aggregate the discovery and inventory of exposures, assets and detection coverage, using environment-aware AI agents. Emerging threats are automatically mapped to your unique environment for automated exposure validation.

Prioritization based on proven threats and potential business impact

Cymulate stack ranks exposure with the full context of threat resilience and validated exposure scoring that considers validated prevention and detection controls, threat intelligence and business context.

Validation of exposures with tailored attack simulation

Cymulate combines agentic AI with automated breach and attack simulation to continuously validate exposures by proving the effectiveness of security controls to preventand detect attacks and exploits. Vero AI tailors assessments to the exposures by mapping the tactics, techniques and behaviors that attackers would use to exploit the vulnerability.

Mobilization with automated mitigation, detection engineering and focused action

Cymulate includes the Mitigation Hub for focused mobilization that recommends next best action. In addition to recommended patching and policy updates, Cymulate-guided mobilization includes vendor-specific detection rules and IOCs that can be automatically pushed to integrated security controls.

Why choose Cymulate?

Complete threat coverage

The most comprehensive threat library that enables validation across the full attack lifecycle – plus daily updates for the latest threats.

AI-powered environment and context mapping

Autonomous, AI-driven usability and workflows customize detection engineering for your environment.

Cyber defense engineering control plane

Closed-loop system that turns validation into continuous improvement across controls and threat detection.

About Cymulate

Cymulate is the leader in proactive, AI-powered security that continuously proves, prioritizes and adapts against real attacker behavior – before incidents occur. Cymulate goes beyond threat validation to build threat- and exposure-informed cyber defenses. For more information, visit www.cymulate.com.

Get a Demo