cymulate

SOLUTION BRIEF

Continuous Threat Exposure Management

Proactive Security Demands Proof of Threat Resilience

Security leaders recognize the need for a more proactive approach to build threat resilience. Through deeper collaboration between security operations, red teams and vulnerability management, continuous threat exposure management (CTEM) aims to find and fix what matters most by taking an attacker's view of what can be exploited.

While vulnerability scanners and other assessment tools market themselves as exposure management, security teams continue to struggle with:

- A growing backlog of potential weaknesses
- Disparate systems for identifying and managing gaps across networks, clouds, applications, systems and more
- Proof and evidence of their true state of threat resilience

Security teams need a way to cut through the noise and focus exposures based on real-world exploitability to achieve their goal of threat resilience.

Elevate CTEM with Continuous Threat Validation

Cymulate puts the "T" in CTEM by delivering the key component other exposure management platforms lack: continuous threat validation.

By testing your defenses against real attack techniques using the latest threat intelligence, the Cymulate Exposure Management Platform empowers security teams to manage and reduce cyber exposure based on what attackers can actually exploit based on proof of threat resilience.

Cymulate delivers a continuous, risk-based and threat-validated approach to exposure management that integrates with vulnerability scanners and other exposure discovery tools. With correlation of exposures and evidence of threat prevention and detection, the Cymulate platform gives security teams the insights to focus on what matters most — their riskiest exposures.

> Cymulate shows us our security gaps so we know what to focus on, where to prioritize our patching, and discover where we should invest most of our efforts.
>
> – Vice President and Head of Cybersecurity, Investment Firm

Solution Benefits

30% ↑ in threat prevention

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

52% ↓ in critical exposures

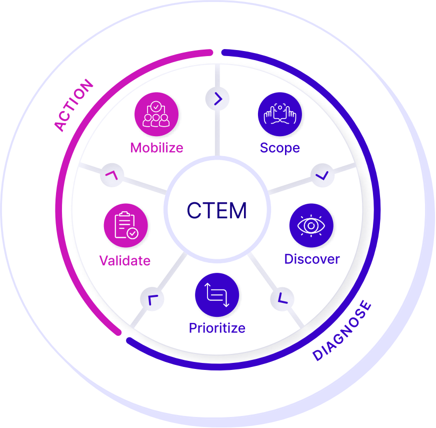
Aggregate and correlate all exposure and threat data to calculate new exposure score and identify true critical exposures.

3x↑ in threat detection

Build, test and tune new threat detections in hours, not weeks, with AI-powered features.

Prove threat resilience

Stay resilient by continuously monitoring and adapting to evolving exposures.



Cymulate Automates the CTEM Lifecycle with the Power of AI

The Cymulate Exposure Management Platform delivers value across the five CTEM phases with seamless integrations, powerful automations and innovative AI workflows that drive collaboration across SecOps, red teams and vulnerability management.

Scoping with business context to baseline security posture

To deliver measurable results, exposure management must start with an understanding of an organization's existing state of threat resilience. Cymulate baselines security posture for the attack surface across all environments and integrates with existing systems to add business context for every asset across endpoints, systems, applications, cloud, data and more.

Discovery of risk-profiled assets with seamless integrations

Cymulate provides a consolidated view of all exposure and affected assets by integrating with the IT and cloud infrastructure and technologies, such as vulnerability scanners, security technologies, EDR and configuration management solutions.

Prioritization based on proven threats and potential business impact

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

Validation with breach and attack simulation and continuous exposure validation

Cymulate automates and scales offensive security testing by running attack tests using the latest intelligence to validate security controls are successfully detecting threats and delivering resilience. Threat validation is tested across the entire attacker lifecycle, from initial access to privilege escalation to lateral movement and data exfiltration. Continuously validate all security controls to prove threat resilience.

Mobilization with automated remediation and streamlined detection engineering

Cymulate empowers security teams to optimize threat resilience with actionable remediation and automated mitigation, and creates new detection rules formatted for easy implementation across EDR, XDR and SIEM technologies. Some threats include the option to push threat updates directly to controls for immediate prevention.

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.

Seamless Easy integrations

Easy integration with out-of-the-box SIEM, EDR and XDR platforms to validate detections and improve threat resilience.

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 validate, 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.

Get a Demo