Cymulate was founded in 2016 to reduce the risk of breaches through attack surface assessment, continuous validation of security, and testing for breach feasibility.

Gartner Peer Insights:
Cymulate Exposure Management & Security Validation by Cymulate in Breach and Attack Simulation (BAS) Tools
4.8 ★★★★★ 125 Ratings

Gain an Attackers View of Attack Surfaces, Vulnerabilities, and Security Efficacy to Support Continuous Threat Exposure Management Programs and Performance Verification

Cymulate Exposure Management & Security Validation Platform

- **Attack Surface Management**
  - Vulnerability Assessment

- **Breach and Attack Simulation**
  - Control Validation

- **Automated Red Teaming**
  - Attack Path Validation

**Exposure Analytics**
- Remediation Prioritization and Business Risk Contextualization

**Take an Attacker's View to Exposure Management**
- Continuously measure and baseline cyber effectiveness and risks to leadership
- Validate controls, discover security drift, and understand emergent threat risks
- Prioritize vulnerabilities and understand exposures mapped to security frameworks
- Rationalize cyber security spend and manage costs
Fuse Technical Data with Business Context

Cymulate for Continuous Threat Exposure Management (CTEM) Programs

**Mobilization:** Mobilize teams to action with remediation guidance and insights to business impact

**Validation:** Automated control testing validates effectiveness, determines likely attack success, & measures response capabilities

**Scoping:** Insights to security posture, biggest gaps, and best opportunities for improvement

**Discovery:** Map attack surface and identify vulnerabilities with aggregated data from Cymulate, IT, and cloud infrastructure

**Prioritization:** Contextualized prioritization with context of business impact and control effectiveness

*CTEM program framework as defined by Gartner

About Cymulate

Cymulate, the leader in exposure management and security validation, provides a modular platform for continuously assessing, testing, and improving cybersecurity resilience against emergent threats, evolving environments, and digital transformations. The solution has a quantifiable impact across all five continuous threat exposure management (CTEM) program pillars and on a business’s ability to reduce risk by understanding, tracking, and improving its security posture. Customers can choose from its Attack Surface Management (ASM) product for risk-based asset profiling and attack path validation, Breach and Attack Simulation (BAS) for simulated threat testing and security control validation, Continuous Automate Red Teaming (CART) for vulnerability assessment, scenario-based and custom testing, and Exposure Analytics for ingesting Cymulate and 3rd-party data to understand and prioritize exposures in the context of business initiatives and cyber resilience communications to executives, boards, and stakeholders. For more information, visit www.cymulate.com.

Contact us for a live demo

Start Your Live Demo

info@cymulate.com | www.cymulate.com