cymulate

SOLUTION BRIEF

Threat Validation

AI accelerates exposure discovery, disclosure and weaponization. Security teams can no longer rely on periodic assessments or manual validation cycles to know whether their defenses are ready for the latest threat.

Cymulate continuously validates security against the latest threats, active campaigns and common attacks using real-world attack techniques. By safely testing prevention, detection and response in production, it helps security teams prove what works, identify gaps, prioritize remediation and strengthen defenses against the threats that matter most.

Prove the threat. Build exposure-informed defenses.

Cymulate automates production-safe attack simulations that validate defenses against the latest threats and TTPs. For identified gaps, Cymulate includes actionable and automated mitigations that update controls to prevent or detect the threat.

- Validate defenses against current threats, CVEs, campaigns and adversary techniques
- Measure prevention and detection effectiveness across essential security defenses
- Push control updates for new detection rules and IoCs to prevent or block the threat
- Retest after mitigation to confirm that risk has been reduced
- Provide leadership with proof of cyber resilience and security improvement

Validate against today's threats

Cymulate Research Labs provides daily updates for emerging threat intelligence into the Cymulate Platform to keep security validation aligned with real-world attacker activity. Security teams can safely validate protection against the latest threats in production without waiting for periodic assessments or manual analysis.

Threat intelligence-driven assessments help teams understand which threats are relevant, how controls respond and where coverage gaps exist. With Vero AI, Cymulate tailors validation scenarios to each organization's environment, assets, exposures and control context.

Key capabilities include:

- Daily threat feed from Cymulate Research Labs for validation and testing of emerging threats
- Integrations with third-party threat intelligence feeds that map organization-specific adversaries on the MITRE ATT&CK and enable quick validation of relevant techniques
- Threat intelligence notifications powered by Cymulate Vero AI that map new threats to the environment and tailored attack chains for validation
- Custom attack chains that reflect organization-specific threats with Cymulate Threat Studio

Solution Benefits

90% threat prevention

50% better threat detection

Test new threats in <1 hour

> I use many security solutions, but Cymulate is a must if you want to ensure your organization is safe from cyber threats. It's easy to use, intuitive, and the customer support is unparalleled.
>
> – Ariel Kashir, CISO, Hertz

Measure prevention, detection and resilience

Cymulate provides security teams with measurable evidence of how effectively their defenses perform against the latest threats. Cymulate helps teams baseline security posture, identify drift and demonstrate improvement over time.

Operational teams can use prevention and detection metrics to tune controls and close coverage gaps. Security leaders can use executive reporting to show resilience, risk reduction and progress against business objectives.

Key capabilities include:

- Prevention and detection metrics
- MITRE ATT&CK heatmaps
- CIS and NIST mapping
- Security drift monitoring
- Executive and operational resilience reporting

Prioritize exploitable gaps and strengthen security

The Cymulate Platform turns validated findings into measurable security improvements. By revealing exploitable security gaps and weaknesses proven through testing, Cymulate helps teams focus remediation on the issues that pose the greatest risk, not just the longest list of vulnerabilities.

Cymulate centralizes remediation workflows and tracks mitigation progress across teams, helping security operations, detection engineering and control owners move from validated exposure to coordinated action. After fixes are applied, automated retesting re-validates defenses to confirm risk reduction and measure improvement over time. With Cymulate Auto Mitigation, teams can also automate control updates and mitigation actions to accelerate remediation and reduce exposure windows.

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. More than 1,000 enterprise security teams rely on Cymulate for autonomous threat validation and cyber defense engineering. Founded and led by experienced red teamers who know that testing alone does not deliver better security, Cymulate goes beyond threat validation to build threat- and exposure-informed cyber defenses. For more information, visit www.cymulate.com.