cymulate

SOLUTION BRIEF

Exposure Management

Growing Backlogs and Little Proof of Cyber Resilience

Security leaders recognize that legacy approaches to security operations cannot answer the critical question, "How exposed is our organization?" To this end, exposure management, or continuous threat exposure management (CTEM), takes a proactive approach 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, etc.
- Proof and evidence of their true state of cyber resilience

Validation Provides the Filter to Focus on True Exposure

Cymulate brings security validation to the heart of exposure analysis in a unified and open platform. This gives security teams agility and full context to determine true threat exploitability based on the effectiveness of their own defensive controls.

Recognized for its best-in-class security validation, the Cymulate Exposure Management platform also includes the integrations and analysis to support every stage in the CTEM process – from scoping through mobilization – to help security teams to:

- Aggregate visibility and analysis of exposure assessments
- Focus on what's truly exploitable
- Prove resilience to new threats
- Measure the true state of their security posture and baseline improvements as the program matures

> 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

Focus on true exposure

Correlate control effectiveness, threat intel and business context to prioritize validated threat exposure.

Accelerate mitigation

Mobilize teams to action with a clearer understanding of a vulnerability's operational and business impact.

Prove cyber resilience

Baseline security posture based on the evidence of security validation and proof of MITRE ATT&CK coverage.

Scoping with business context to baseline security posture

To deliver measurable results, exposure management must start with an understanding of where you are today and the state of resilience for essential processes, business units, critical assets and more. Cymulate baselines security posture for the entire attack surface across environments with the required business context to every asset across endpoints, systems, applications, clouds and more.

Discovery with native assessments and integrations for risk-profiled asset inventory

Cymulate provides native discovery of the external attack surface and an open platform that integrates the security stack and infrastructure. By aggregating the findings from vulnerability scanners, security controls, configuration management and more, Cymulate provides a consolidated view of all potential exposures and effected assets.

Prioritization based on validated threats and potential business impact

To highlight the biggest weaknesses, Cymulate correlates all assets with their exposure risk and business context. This prioritization also considers the results from validated attack paths, the effectiveness of compensating controls to mitigate the threat and the various options for remediation or mitigation.

Validation with breach and attack simulation and continuous automated red teaming

Cymulate automates offensive security testing to validate controls, threats and attack paths. Offering the most trusted security validation, Cymulate combines breach and attack simulation with automated red teaming to safely test how controls respond to threats and assess the potential for threats to move laterally to reach the crown jewels.

Mobilization with comprehensive remediation guidance

To effectively address exposure risk and strengthen security posture, Cymulate provides detailed remediation plans backed by the proof and evidence provided through validation. Cymulate delivers actionable remediation guidance that includes all options for remediation (patching and configuration updates), mitigation through security controls and potential business impact of the risk.

Cymulate helps us prioritize exploitable vulnerabilities in our environment. By integrating with our vulnerability management products and running Cymulate assessments, we can easily discover which vulnerabilities are an actual threat to our organization.

- Kevin Roberts, Information Security Analyst, Nedbank

About Cymulate

Cymulate is the leader in exposure management and security validation. More than 500 customers worldwide rely on the Cymulate platform for continuous discovery, validation, prioritization, and guided remediation of security gaps before attackers can exploit them. For more information, visit www.cymulate.com.

Get a Demo