SOLUTION BRIEF

Cymulate

Security Control & Threat Validation

Challenges

Security leaders understand the importance of investing in security controls; however, the required continuous configuration of these controls is often overlooked. Designed to minimize security risks, security controls can still be misconfigured, preventing them from functioning as intended and resulting in a false sense of security or an overload of false-negative alerts. Organizations that validate their controls with infrequent manual third-party penetration tests receive expensive, narrowly focused assessments that do not provide immediate feedback.

Additionally, today's evolving threat landscape introduces new threats daily, and organizations need to act fast to ensure that their security controls can protect them against the latest emergent threat. Manually researching each threat, developing production-safe assessments to test controls, and taking steps toward remediation when necessary do not provide an organization with immediate protection.

Continuously Validate Your Defenses

The Cymulate Platform safely and continuously assesses the efficacy of security controls against threat activity across on-premises, cloud, and hybrid environments. New assessments are added daily to test against the latest emergent threats, so organizations can immediately evaluate their defenses. This leads to targeted and effective tuning of operations, true risk visibility, and fewer false-negative alerts.

The Role of Control and Threat Validation in Exposure Management

Cymulate determines the true impact of exposures and emergent threats by testing controls, understanding the effectiveness of compensating controls, and measuring response capabilities. By correlating this analysis with vulnerabilities and other potential exposure risks, organizations can prioritize patching and remediation based on risk as part of a larger continuous threat exposure management (CTEM) program.

"Integrate BAS in a cybersecurity validation roadmap, as part of a continuous threat exposure management (CTEM) program. Don't run BAS in isolation."

- Gartner: Hype Cycle for Security Operations, 2023

Solution Benefits

MAXIMIZE EXISTING RESOURCES

"Cymulate provides us with the insights to close gaps and optimize the controls we already have in our security stack—we don't need to waste time or money looking for new tools to improve our security."

- Liad Pichon, Director of Cybersecurity, BlueSnap

OPTIMIZE SECOPS & INCIDENT RESPONSE

"Cymulate enables us to test Nemours' defenses against the latest cyber threats as they emerge, prioritize remediation efforts, and improve our security team's incident response skills."

- Jim Loveless, CISO, Nemours

RATIONALIZE INVESTMENTS

"With Cymulate, we can present quantifiable data to the board and show a direct correlation between investments and the reduction in risk."

- Avinash Dharmadhikari, CISO, Persistent Systems

BENCHMARK SECURITY RESILIENCE

"Cymulate improved our risk management process and decision-making."

- Yoav Gefen, CISO, Maman Group

Use Cases

Detect and Control Drift

Cymulate provides automated testing and reporting for continuous monitoring of security drift. With the platform's automation, organizations continuously assess environments and systems to track overall resilience and catch gaps, vulnerabilities, and misconfigurations as quickly as possible. Cymulate scores based on test results and security frameworks help detect changes to overall risk, and easy-to-digest remediation guidance allows for quick mitigation.

> **"We chose Cymulate because we saw right away that it would require much less effort and time on our part to get immediate and effective insight."**
> - Itzik Menashe, VP Global IT & Information Security, Telit

Validate and Optimize SIEM/SOC

Cymulate attack simulations validate SIEM visibility and assess SOC processes to reduce both false positives and negatives. Applied to both internal and external SOCs (MSSPs), Cymulate provides indicators of compromise, indicators of behavior, Sigma rules, and translation of the Sigma rules to vendor-specific systems to help build new rules and fine-tune existing rules to render accurate detection. The reporting enables teams to benchmark and evolve SecOps performance over time.

> **"Under the workload our team experiences, Cymulate sheds light on what to focus on to constantly improve our cybersecurity posture."**
> - Ramon Clota Palacio, Director, IT and Security, Prevision Mallorquina

Test Against Emergent Threats

The Cymulate Threat Research Group updates simulations of new threats daily, making them immediately available for customers to test safely. Remediation guidance enables organizations to quickly reduce exposure to emergent threats in less time and with less effort.

> **"Before Cymulate, it took us 2 to 3 days to evaluate a threat—now it takes us one to two hours because all we need to do is run the assessment that Cymulate prepares for us."**
> - Vice President and Head of Cybersecurity, UAE Investment Firm

About Cymulate

Cymulate, the leader in exposure management and security validation, provides the single source of truth for threat exposure and the actions required to close security gaps before attackers can exploit them. More than 500 customers worldwide rely on the Cymulate platform to baseline their security posture and strengthen cyber resilience with continuous discovery, validation, prioritization, and guided remediation. For more information, visit www.cymulate.com.

Contact us for a private demo

Start Your Demo

info@cymulate.com | www.cymulate.com