SOLUTION BRIEF

Continuous Security Control Validation

Challenges

Despite years of investment, security leaders struggle to answer the basic questions of "Are we exposed?" and "What are my biggest gaps?" The answers become more uncertain when faced with the daily evolution of threats and digital transformation projects that adopt new technologies, migrate applications to the cloud, and integrate internal systems with supply chain partners.

Testing and proving cyber resilience are especially challenging for smaller teams that outsource security operations or rely on managed service providers. With or without a managed service, security leaders struggle to:

- Test controls against the latest emerging threats
- Know the current state of their cyber program – both strengths and weaknesses
- Prioritize investments and projects to optimize existing controls or implement new technologies

Continuously Validate Controls & Optimize Defenses

Cymulate Breach and Attack Simulation (BAS) automates advanced production-safe offensive testing to continuously validate controls against the latest threats and provide remediation guidance to tune and optimize defenses. As a SaaS solution designed for simple and fast deployments, Cymulate BAS enables organizations to identify the biggest gaps to address and prove their state of resilience.

Continuously validate controls
Test for prevention, detection, and proper alerting on real threat scenarios to confirm that your security controls are functioning correctly or if threats can evade them.

Test against emergent threats
Automatically test your security controls against new and emerging threats observed in the wild with daily updates of new assessments based on real-world active threats.

Optimize defenses
Detailed remediation guidance and heatmaps of security gaps provide insights into tuning and optimizing your security controls and policies.

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

Cymulate

Use Cases

Optimize Controls and Manage Drift

Cymulate provides automated testing to validate security controls, identify drift, and optimize prevention and detection. 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, and Managed Services

Cymulate attack simulations validate SIEM visibility and assess SOC processes to reduce false positives and negatives. Applied to internal SOCs and 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.

> "Before Cymulate, our red team had to validate our outsourced SOC services with manually executed attacks, which is both time-consuming and limited in scope. With Cymulate, our security team quickly runs assessments that extensively cover TTPs and IOCs with significantly less effort. The platform also generates SIEM-specific queries based on Sigma rules, making mitigation more streamlined and reducing the team's mean time to detect (MTTD) and mean time to prevent (MTTP)."
> - Assistant Information Security Manager, Financial Services Company

Assess Immediate and Custom Threats

The Cymulate Threat Research Group creates simulations of new threats daily, making them immediately available for customers to test safely on the platform. Security teams can also utilize Cymulate's open framework to build custom test cases based on a library of attack techniques, executions, and more. 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 1 to 2 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 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.

Contact us for a private demo

Start Your Demo

info@cymulate.com | www.cymulate.com