Cymulate

SOLUTION BRIEF

Validate and Optimize SecOps Detection and Response

Challenges

SecOps teams are responsible for continuously monitoring security events, identifying and mitigating threats, and managing incident response to protect an organization's digital assets. While these tasks may seem straightforward, there are additional factors that leave SecOps teams feeling overworked and burned out:

- Security teams are often understaffed and struggle to keep up with the volume of alerts and incidents, especially when done manually.
- New threats that emerge daily can overwhelm security teams and make it difficult to determine which are the most dangerous threats to their organizations.
- Digital transformation projects and migrating applications to the cloud continuously expand an organization's attack surface.

Optimize Continuous Defense Validation

Whether you have an internal SOC (security operation center) or outsource to an MSSP (managed security service provider), Cymulate automates attack simulations to assess SOC tools and processes, validate and optimize detection and response, and benchmark performance over time.

Solution Results

91% **increase in malicious file detection**
Sport Media

25% **reduction in manual SecOps tasks**
Banking Company

168 **exploits prevented from 1 policy change**
Healthcare Organization

Solution Benefits

OPTIMIZE SECOPS & INCIDENT RESPONSE

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

- CISO, Healthcare Organization

BENCHMARK SECURITY RESILIENCE

"Cymulate gives us a benchmark to work towards improvement. I can effectively plan my security roadmap by outlining the steps I need to achieve optimized cybersecurity maturity."

- Assistant InfoSec Manager, Financial Services

TEST NEW THREATS

"Before Cymulate, it took us two to three 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."

- VP & Head of Cybersecurity, UAE Investment Firm

EXECUTE INCIDENT RESPONSE EXERCISES

"We are starting to use Cymulate for our incident response exercises, and we appreciate that we can customize the assessments directly to our needs."

- Markus Fletcher, Senior Security Manager, RBI

Use Cases

Security Control Optimization for SOC

SecOps teams can integrate their security information and event management (SIEM) systems and other security controls with Cymulate to run simulated attacks and validate whether they are accurately and fully detecting the relevant threats and properly alerting SOC analysts.

- **Test and assess**
  Cymulate attack simulations enable SecOps teams to assess whether their SIEM (security information and event management) is accurately detecting the relevant threats and properly alerting SOC analysts. API-based integrations help correlate attacks with SIEM findings, allowing analysts to quickly determine if the system is working as intended.
- **Fine-tune and optimize**
  Following each simulation, Cymulate provides indicators of compromise (IoC), indicators of behavior, sigma rules, and translation of the sigma rules to vendor-specific systems. This helps SecOps teams build new rules and fine-tune existing ones, enabling accurate detection and reducing false positives and negatives. Additionally, Cymulate automatically uploads critical IOC data directly to an organization's relevant security controls to ensure that potential threats are identified and addressed quickly.
- **Confirm and measure**
  Following remediation and fine-tuning, SecOps teams can easily retest and confirm that their activities improved detection and alerting. Additionally, Cymulate metrics and reporting enable security teams to benchmark and evolve their SecOps performance over time.

Security Control Validation for MSSP

Smaller security teams that outsource security operations or rely on managed service providers can run Cymulate attack simulations to assess whether their outsourced services perform as well as they guarantee.

- **Test and assess**
  Organizations can continuously assess MSSP detection and response capabilities by running Cymulate attack simulations against their security controls. Additionally, the Cymulate Threat Research Group creates simulations of new threats daily, making them immediately available for customers to independently validate whether they have full MSSP coverage against the newest emergent threats.
- **Fine-tune and optimize**
  With Cymulate, security teams can conduct live-data exercises alongside their outsourced service providers to practice cross-team coordination and run incident response drills. Following these exercises, Cymulate provides remediation guidance to the outsourced services for optimizing detection and response.
- **Confirm and measure**
  Cymulate enables security teams to quickly retest and confirm that their MSSPs have improved their detection and alerting. The platform's metrics and reporting also help security teams benchmark MSSP performance against Service Level Agreements (SLAs) to ensure contractual obligations.

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 of security weaknesses. Cymulate automates advanced offensive security testing to validate controls, threats, and attack paths. As an open platform, Cymulate integrates with existing security and IT infrastructure and drives the workflows of the exposure management process. For more information, visit www.cymulate.com.

Contact us for a private demo

Start Your Demo

info@cymulate.com | www.cymulate.com