Cymulate

SIEM, SOC & IR Optimization

Solution Brief

Challenges

Security Operations Centers (SOCs) and Incident Response (IR) teams face growing challenges in detecting and responding to security events, even when managing their multiple security solutions with a Security Information and Event Management (SIEM). SIEM systems aggregate detection and response data, but their efficacy depends on ensuring that all event is detected, and that a comprehensive and contextual analysis of that data promotes prioritizing mitigation efforts for optimal impact.

Yet, configuring SIEM solutions without clear visibility into security gaps can consume significant resources, and the multiplication of misconfigured security controls result in increased false positives and subsequent alert fatigue. In addition, frequent reconfigurations are required to keep up with the constantly changing threat landscape and ongoing deployments and updates to IR playbooks.

Furthermore, optimizing Incident Response (IR) requires SOAR playbooks and IR routines to be agile and adaptable, capable of addressing new threats as they emerge and tailoring their approaches to specific environments. Conducting simulated tabletop exercises is vital for refining these playbooks and routines, making them an indispensable component of a proactive cybersecurity strategy.

SOC and IR teams face several challenges, such as insufficient data to verify the effectiveness of security tools in detecting and mitigating attacks. Additionally, the numerous security controls, some of which may be inadequately configured, result in increased false positives and subsequent alert fatigue.

The constantly changing threat landscape and ongoing deployments necessitate frequent reconfigurations and updates to IR playbooks. Furthermore, configuring SIEM solutions without clear visibility into security gaps can consume significant resources. To overcome these challenges, it is essential to adopt a unified, flowing approach for strengthening SOC, SIEM, and IR validation.

Overview

Cymulate security validation platform accelerates the optimization of SIEM, SOC, and IR capabilities. Its over 120 000 off-the-shelf production-safe attack simulations assess SIEM efficacy and identify security gaps.

One of the key benefits of using Cymulate is the ability to continuously tune incident response playbooks with minimal to no interference with daily operations. Security teams can run up-to-date tabletop exercises and fine-tune their playbooks based on the latest attack scenarios, ensuring optimal response readiness.

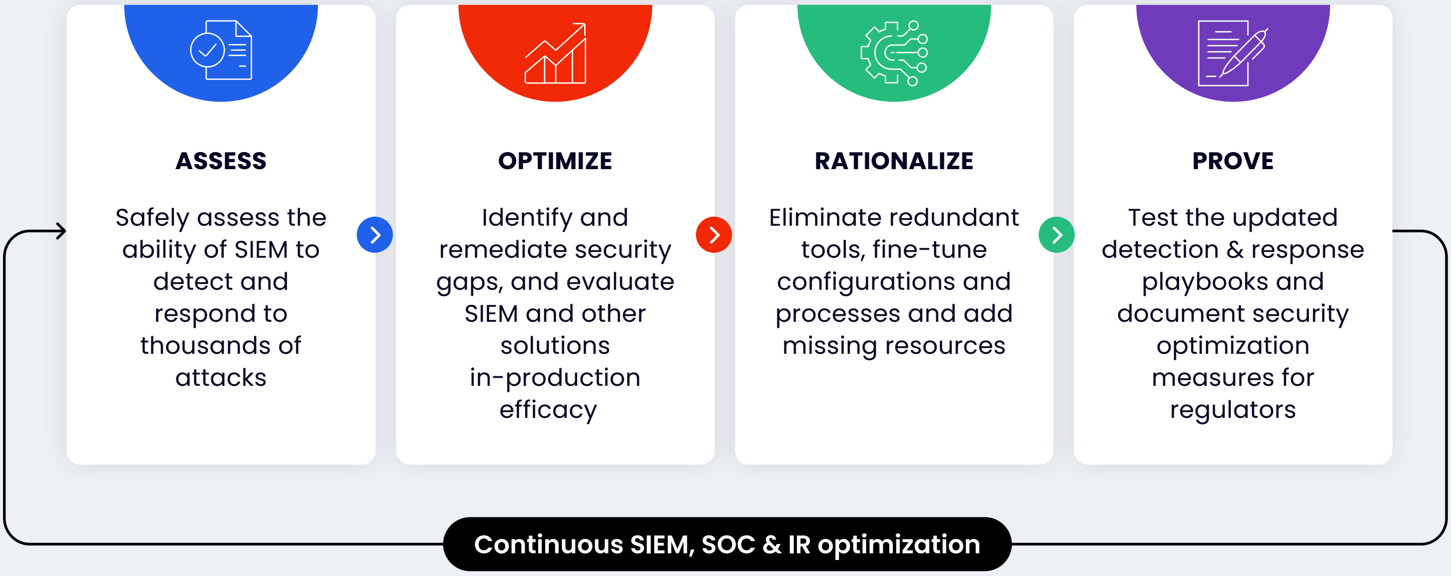
Thanks to its ability to integrate with multiple detection and response tools, the Cymulate platform also enables rationalizing the tool stack by identifying redundant and missing capabilities and providing granular information about inadequate configuration.

Actionable remediation guidance for uncovered security gaps accelerates the remediation process.

Benefits

- Simple to deploy
- 360º security posture visibility
- Continuous threat exposure monitoring
- Increases operational efficiency
- Improved security posture
- Security drift detection and prevention
- Reduced costs

Capabilities of SIEM, SOC, and IR Optimization



ASSESS

Safely assess the ability of SIEM to detect and respond to thousands of attacks

OPTIMIZE

Identify and remediate security gaps, and evaluate SIEM and other solutions in-production efficacy

RATIONALIZE

Eliminate redundant tools, fine-tune configurations and processes and add missing resources

PROVE

Test the updated detection & response playbooks and document security optimization measures for regulators

Continuous SIEM, SOC & IR optimization

Main Features

Real-time monitoring
Can monitor exposure to emerging threats continuously or check for specific threats individually or per type or APT group.

Integration with major detection and response tools and GRC, SIEM, and SOAR systems
Enables rationalizing the tool stack by optimizing their configuration based on hard data and identifying redundant capabilities.

Comprehensive set of automated attack simulations
120 000 out-of-the-box production-safe attack simulations, easily customizable with a drag-and-drop wizard as deemed appropriate.

Granular quantification of threat exposure
Provides a risk score for each category of security control - Email and Web gateway, Endpoint, Web Application Firewall (WAF) and data exfiltration (DLP).

Automatic report generation
Customizable template executive and technical reports facilitate communication across departments and with regulators and accelerate mitigation with actionable guidance and integrated ticketing for streamlined mitigation management.

Capabilities of SIEM, SOC, and IR Optimization

Nemours Children’s Health System

A nonprofit children’s health organization care for about 500 000 children annually in Delaware Valley and Florida.

Challenge
Nemours needed a way to evaluate its defenses against the latest threats, prioritize remediation efforts better, and improve its team’s productivity and incident response skills.

Solution
Cymulate's automated immediate threats intelligence assessments, purple team exercises and security control validation makes it simple for Nemours to know and control its security posture.

Benefit
Cymulate empowers the government agency with a holistic reflection of its security posture status, so it can optimize its investments and focus on risk prevention.

Read more

Quilter

A leading, international provider of advice, investments, and wealth management

Challenge
To build a world class cyber-security practice that supports organic and acquisition-based business growth while confronting the dynamic threat landscape.

Solution
Cymulate provides the security team rapid and effective security control validation, risk assessments and an open framework to exercise cyber “what-if” scenarios.

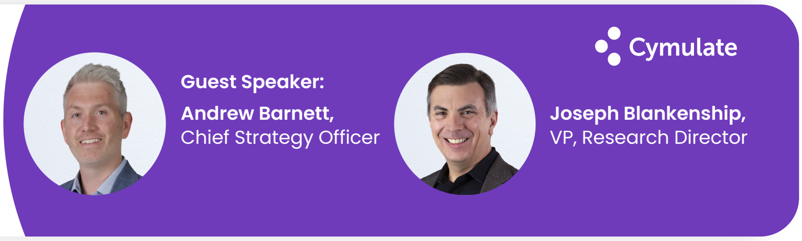
Benefits
With Cymulate, the security team is able to respond faster and more effectively to management queries, business initiatives and new threats.

Read more

Additional Resources

Making SecOps & Security Leaders More Successful

Read more



Cymulate

Guest Speaker:
Andrew Barnett,
Chief Strategy Officer

Joseph Blankenship,
VP, Research Director

Backed by the Industry

Awards and Accolades

About Cymulate

The Cymulate Security Posture Validation Platform provides security professionals with the ability to continuously challenge, validate, and optimize their on-premises and cloud cyber-security posture with end-to-end visualization across the MITRE ATT&CK® framework. The platform provides automated, expert, and threat intelligence-led risk assessments that are simple to deploy, and easy for organizations of all cybersecurity maturity levels to use. It also provides an open framework for creating and automating red and purple teaming by generating tailored penetration scenarios and advanced attack campaigns for their unique environments and security policies.

Contact us for a live demo, or get started with a free trial

Start Your Free Trial

info@cymulate.com | www.cymulate.com