cymulate

SOLUTION BRIEF

Accelerate Detection Engineering

The Sooner You Detect, the Faster You Defend

Threat actors continuously evolve their tactics to move across IT networks and cloud environments undetected, leaving you at risk of suffering a significant cyber breach.

To mitigate this risk and build resilience, SecOps must continuously create, fine-tune and validate that their SIEM (security information and event management), EDR (endpoint detection and response) and XDR (extended detection and response) systems to accurately detect malicious activity while minimizing false positives. However, this process is both resource-intensive and slow, leaving gaps as threats evolve.

SecOps are turning to AI and automation to rapidly create, validate and fine-tune detection rules, accelerating the path to threat resilience by detecting attacks before they cause disruption.

Stronger Threat Resilience for SecOps

Cymulate Exposure Validation accelerates detection engineering by automating the most critical and resource-heavy tasks in modern SecOps. By combining robust attack simulations with AI-driven analysis, Cymulate empowers teams to build, test and fine-tune threat detection using live-data attack simulations and custom rules that streamline detection workflows.

With Cymulate, SecOps can:

- **Reduce detection gaps** faster by shortening the time from rule creation to validated coverage
- **Pinpoint gaps** with actionable insights when detection rules fail to trigger on expected behavior
- **Expand detection visibility** by aligning rules to real attack techniques mapped across the MITRE ATT&CK framework

> **“Cymulate’s AI SIEM Rule Validation streamlines our detection engineering validation processes with automated rule matching, saving us hundreds of hours at scale.”**
>
> – Markus Flatscher, Senior Security Manager, RBI Bank

Solution Benefits

30% increase in threat detection accuracy

Build, test and tune new threat detections in hours, not weeks, with rules specific to your SIEM, EDR and XDR.

60% increase in team efficiency

Automate and streamline the most critical tasks in modern SecOps to reduce the likelihood of a breach.

Visualize detection coverage

Map detection rules to threat frameworks like MITRE ATT&CK to identify gaps and prioritize areas for improvement.

Cymulate Offering

- **Exposure Validation**
- **Custom Attacks Add-on (optional)**

Detection Engineering Solution Features

Cymulate is an open platform that integrates with top SIEM, EDR and XDR vendors to build, validate and optimize high-fidelity detections and minimize false positives. Operationalize detection engineering with AI-powered offensive testing that validates detection and essential log collection to support advanced correlation.

Build and validate new detections for emergent threats

Upload a threat advisory or news article into the Cymulate AI template creator to instantly generate a custom assessment and validate controls against new real-world threat behaviors. If detection gaps are found, Cymulate provides recommended SIEM, EDR or XDR rules formatted to the specific control for easy implementation. SecOps teams can then re-run the assessment to validate that new rules trigger the correct alerts, ensuring fast, effective protection against evolving threats.

Map and validate existing SIEM detection rules with AI

Cymulate integrates with the SIEM to validate existing detection rules by applying AI to match relevant attack scenarios for each detection rule. With the push of a button, SecOps teams can validate whether rules trigger as intended, uncover detection gaps and receive targeted recommendations to improve rule logic. Once updates are made, teams can instantly re-run assessments to confirm rule performance and visualize coverage using the MITRE ATT&CK heatmap. With built-in automation, Cymulate makes it easy to continuously test and tune rules, ensuring lasting protection against evolving threats across the full kill-chain.

Baseline and optimize MITRE ATT&CK coverage

Cymulate provides a visual MITRE ATT&CK heatmap that highlights detection gaps based on real-world threats and current rule coverage. With clear visibility into which behaviors are detected, missing, or underperforming, teams can prioritize where to build new rules or improve existing ones, streamlining efforts to strengthen detection across the kill-chain.

Test SecOps processes, policies and playbooks

Cymulate simulates real-world attack scenarios to help SecOps teams rehearse detection and response workflows in a safe, controlled environment. These exercises surface gaps in visibility, tooling or process execution, allowing teams to fine-tune detections, improve collaboration across stakeholders and validate that playbooks and alerts function as intended. By proactively identifying weaknesses before an actual incident, Cymulate helps reduce mean time to detect and respond while strengthening overall operational readiness.

> **Using the Cymulate integrations, we launch assessments to see if our tools detect them. If they don’t, Cymulate provides mitigation guidance and Sigma rules, and we easily rerun the assessments to validate remediation.**
>
> – Karl Ward, Head of Cybersecurity, LV=

Why choose Cymulate?

Build new detections in minutes

Create or improve rules with targeted guidance, indicators of behavior, pre-built Sigma and EDR rules.

Optimize threat coverage

Visualize threat detection gaps and create detection logic for full MITRE ATT&CK coverage.

Collaborate to mitigate exposure

Partner with your SOC or MDR provider to adapt and enhance detection to new threats.

Contact us for a live demo Start Your Live Demo info@cymulate.com www.cymulate.com