cymulate

SOLUTION BRIEF

Detection Engineering

Early Detection is Critical to Stopping Cyber Attacks

Threat actors often move across IT networks and cloud environments, evolving tactics to gain access and avoid detection. Without intelligent detection, these threats can escalate into significant cyber breaches.

To mitigate this risk, SecOps teams 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 can accurately detect malicious activity while minimizing false positives. Building precise detection rules is already a lengthy process, while manually validating those rules is time-consuming and too slow to keep up with evolving threats.

SecOps are turning to automated testing to create, validate and fine-tune detection rules, detecting attacks before they cause disruption.

Automate Detection Engineering to Reduce Exposure Risk

The Cymulate Exposure Validation Platform accelerates detection engineering by automating the most critical and resource-heavy tasks in modern SecOps. Cymulate provides the most robust attack simulation with AI-powered analysis, so SecOps teams can build, test and fine-tune threat detection using live-data attack simulations and custom rules that streamline detection workflows.

By simplifying and accelerating detection engineering with Cymulate, SecOps teams can:

- Shorten the cycle from rule creation to validated threat coverage
- Get actionable insights when detection rules fail to trigger
- Maximize visibility and coverage across the MITRE ATT&CK® framework

> **When we create a new detection rule in our SIEM that we can’t validate with historical logs, we use Cymulate assessments to generate the appropriate events and see if the rule was successful in its detection. The immediate feedback is useful when fine-tuning our SIEM and practicing detection engineering.**
>
> – Markus Flatscher, Senior Security Manager, RBI Bank

Solution Benefits

Accelerate rule creation & validation

Streamline detection workflows to reduce mean time to detect (MTTD) and speed up validation of threat detection rules.

Improve detection accuracy

Minimize false positives and negatives to increase alert fidelity, reduce analyst fatigue and improve confidence in detections.

Visualize detection coverage

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

Minimize exposure risk

Continuously validate detection coverage to reduce the chance of undetected threats leading to a material cyber breach.

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.

Validate, tune and maintain SIEM detection rules

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?

Streamlined rule creation

Create or improve detection with targeted guidance, indicators of behavior, and detection rules mapped to specific SIEM and EDR platforms.

Effortless validation

Automatically map SIEM rules to attack scenarios for custom testing that continuously validates and optimizes detection logic.

Control integrations

Out-of-the-box integrations with leading SIEM, EDR and XDR platforms to validate detection, log collection and visibility to threats.

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