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 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 teams 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 helps SecOps teams build, test and optimize SIEM, EDR and XDR detection rules by automating security control validation. With the best of breach and attack simulation and automated red teaming, SecOps can confidently validate existing detections, identify blind spots, fine-tune detection logic and reduce false positives. Cymulate enables a streamlined, prioritized approach to detection engineering, accelerating rule development and maximizing 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

> **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=

Solution Benefits

Accelerate rule creation

Automate and streamline the detection engineering workflow to reduce your controls' mean time to detect (MTTD).

Improve detection accuracy

Reduce false positives and false negatives, giving analysts higher confidence in alerts and decreasing alert fatigue.

Visualize coverage gaps

To prioritize improvements, visualize how well your detections align with threat frameworks like MITRE ATT&CK™.

Minimize exposure risk

Reduce the likelihood of a cyber attack evading detection and 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 high-fidelity detections while minimizing false positives. Operationalize detection engineering with offensive testing that validates detection and essential log collection to support advanced correlation.

Find detection gaps with actionable threat modeling

Cymulate simplifies the detection engineering workflow by minimizing the initial stages of traditional SIEM, EDR and XDR rule creation. Instead of manually defining use cases, identifying log sources and writing detection logic from scratch, SecOps can filter the Cymulate MITRE ATT&CK™ heatmap based on relevant threats and detection status. This instantly reveals which techniques are already covered by detection rules and highlights those that are missing or underperforming, guiding SecOps directly to where new rules are needed or existing ones that require improvement.

To further focus efforts, Cymulate assessments can also be filtered by the most relevant threats to an organization based on indicators of compromise (IOCs), known advanced persistent threat (APT) activity, or a specific environment. This allows SecOps to narrow in on high-priority scenarios and optimize rule development where it matters most.

Create and fine-tune detection rules

Most detection failures stem from missing or misconfigured telemetry. When Cymulate flags an undetected technique or threat, it provides targeted guidance on creating or refining a detection rule, removing ambiguity from the detection engineering process. Instead of sifting through broad threat intel or relying solely on internal knowledge, SecOps gain actionable, technique- and threat-specific insights. Cymulate further accelerates tuning with relevant IoCs, indicators of behavior, pre-built Sigma rules and EDR rules. Cymulate even offers translations of Sigma rules to vendor-specific systems to increase tuning efficiency and accuracy.

Validate detection rules with build-in feedback loops

SecOps teams can easily re-run the relevant Cymulate assessment to validate if the new or fine-tuned rules trigger the correct alerts. With automation built in, Cymulate enables continuous cross-vector validation and tuning, ensuring that detection rules remain effective against evolving, real-world attack techniques and threats across the full kill-chain.

Test SecOps processes, policies and playbooks

By simulating real-world attack scenarios, Cymulate allows SecOps to rehearse detection and response workflows in a controlled environment. These exercises surface gaps in visibility, tooling and processes, enabling SecOps teams to fine-tune detections, improve collaboration across stakeholders and validate that playbooks and alerts function as intended. Instead of waiting for a real incident to expose weaknesses, Cymulate empowers teams to proactively strengthen their response capabilities and reduce mean time to detect and respond.

Why choose Cymulate?

Visibility of detection gaps

Automatically visualize MITRE ATT&CK™ and threat coverage to pinpoint weak or missing detection rules.

Streamlined rule creation

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

Validate processes, policies and playbooks

Surface gaps in visibility, tooling, and processes so SecOps teams can proactively strengthen their response capabilities.

About Cymulate

Cymulate, the leader in security and exposure 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 1,000 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.