cymulate

DATA SHEET

Cymulate Detection Studio

Validate, Tune and Optimize SIEM Detection

Security teams rely heavily on SIEM detection rules to identify threats, but maintaining effective detection logic is complex, time-consuming and often reactive.

Cymulate Detection Studio transforms detection engineering by automating rule validation and mapping existing SIEM detections to real-world attack techniques to continuously optimize detection performance.

With the intelligence of Vero AI mapping SIEM rules to attack simulation, Cymulate Detection Studio enables security teams to validate whether SIEM rules actually trigger against real attack behaviors and provides clear, actionable guidance when they don't.

Cymulate eliminates manual rule analysis, testing and tuning workflows, enabling security teams to focus on improving detection coverage and reducing risk.

Automate the Detection Engineering Lifecycle

Cymulate Detection Studio provides a rule-led approach to detection engineering that integrates directly with SIEM to:

1. Import existing SIEM detection rules through native integrations.
2. Automatically map rules to attack techniques and scenarios using Vero AI.
3. Execute real-world attack simulations to validate rule effectiveness.
4. Collect logs and telemetry required to trigger detections.
5. Provide evidence of triggered and missed detections.
6. Recommend vendor-specific rule improvements for missed alerts.
7. Re-run scenarios to validate detection tuning.

This closed-loop workflow continuously tests, validates and improves detection logic.

Built-in dashboards provide detailed insights into detection engineering drift and ROI. Teams can visualize gaps, monitor validation results and prioritize improvements based on real attack scenarios. Detection coverage is mapped to MITRE ATT&CK techniques and correlated to SIEM rules, providing clear visibility into rule effectiveness across the attack lifecycle.

Benefits

Continuous rule validation

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

Improve detection accuracy

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

Visualize coverage gaps

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

Improve threat resilience

Reduce the likelihood of a cyber attack evading detection and leading to a material cyber breach.

Reduce Detection Engineering Time by 80%

Scale detection engineering to continuously expand coverage and automate the detection life cycle.

> Cymulate Detection Studio streamlines our detection engineering validation processes, saving us hundreds of hours at scale."
>
> – Markus Flatscher, Senior Security Manager, RBI Bank

Why Choose Cymulate?

Complete threat coverage

The most comprehensive threat library that enables validation across the full attack lifecycle – plus daily updates for the latest threats.

AI-powered environment and context mapping

Autonomous, AI-driven usability and workflows customize detection engineering for your environment.

Defense engineering control plane

Closed-loop system that turns validation into continuous improvement across controls and threat detection.

About Cymulate

Cymulate is the leader in proactive, AI-powered security that continuously proves, prioritizes and adapts against real attacker behavior – before incidents occur. More than 1,000 enterprise security teams rely on Cymulate for autonomous threat validation and cyber defense engineering. Founded and led by experienced red teamers who know that testing alone does not deliver better security, Cymulate goes beyond threat validation to build threat- and exposure-informed cyber defenses. For more information, visit www.cymulate.com.