SOLUTION BRIEF

Detection Engineering

cymulate

Continuous Validation for Better Threat Detection

Threat actors move across IT and cloud environments and continuously evolve tactics to evade detection. SecOps teams must create, tune and validate detections across SIEM (security information and event management), EDR (endpoint detection and response) and XDR (extended detection and response) to identify malicious activity while minimizing false positives.

Security teams are turning to exposure validation to accelerate detection engineering and maintain effective threat detections across their security controls.

Automate and Scale Detection Engineering

Cymulate transforms detection engineering from a manual, resource-intensive process into a continuous, automated lifecycle. By combining attack simulation with AI-driven analysis from Vero AI, Cymulate enables SOC and Detection Engineering teams to continuously validate, tune and expand detection coverage at scale.

Through multiple detection engineering approaches, Cymulate enables teams to:

- Build and test new detections for emerging threats with *threat-led detection engineering* for SIEM, EDR, XDR, cloud, WAF and more
- Validate and optimize existing SIEM detections with *rule-led detection engineering*
- Baseline and systematically improve coverage across adversary techniques with *MITRE ATT&CK–aligned detection engineering*

Cymulate maps attack scenarios to detection logic, pinpoints gaps, and provides actionable, vendor-specific recommendations so teams can prove coverage, reduce noise and accelerate workflows.

Cymulate Platform	Detection Engineering Features
Exposure Validation	• Daily threat feed for attack simulation • Attack library with full coverage of MITRE ATT&CK techniques • Vero AI maps threat intel to attack library for custom testing • Integration with security controls to validate alerting and telemetry • Recommended detection rules for SIEM, EDR, cloud, WAF, YARA, Sigma and more
Detection Studio	• Sync SIEM rules with validation • Map SIEM rules to attack techniques • Identify drift for SIEM rules
Auto Mitigation	• Push vendor-specific rules directly to EDR

Solution Benefits

Fast rule creation and continuous 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.

Optimize SIEM and EDR

Continuous testing and tuning to get the best threat detection from security logs and security controls.

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

Cymulate Detection Engineering Workflows

Threat-led detection engineering

Cymulate Exposure Validation enables organizations to rapidly create and validate detections for emerging threats. By uploading a threat advisory or article, Vero AI generates a custom assessment that simulates real-world attacker behavior and tests existing controls.

Cymulate monitors detection rules during execution to determine whether alerts trigger as expected. If detections fail, Cymulate provides ready-to-use, vendor-specific rules for SIEM, Cloud, Sigma, WAF and YARA, formatted for direct implementation within the relevant security control. Cymulate also delivers EDR/XDR behavioral detection rules and IoCs, enabling teams to detect malicious activity across endpoints and networks.

With **Cymulate Auto Mitigation**, behavioral detection rules and IoCs can be automatically deployed to integrated security controls, accelerating response and reducing manual effort. Teams can then apply updates and re-run scenarios to confirm improved detection performance.

Rule-led detection engineering

Validate, tune and maintain SIEM *Validate, tune and maintain SIEM detection rules*. detection rules. **Cymulate Detection Studio** enables continuous validation and optimization of existing SIEM rules at scale. Rules are ingested from supported integrations and automatically mapped by Vero AI to relevant attack scenarios from its extensive library.

Cymulate assessments validate whether alerts trigger as expected, identify gaps and receive vendor-specific rule recommendations. When a group of relevant events lacks detection, Vero AI can also suggest new rules to implement based on the customer's environment. Updated rules can be tested instantly, while mappings are continuously maintained to ensure detection logic remains accurate as environments evolve.

MITRE ATT&CK-aligned detection engineering

Baseline and optimize MITRE coverage. Cymulate *Baseline and optimize MITRE coverage*. Exposure Validation enables organizations to baseline and optimize detection coverage across MITRE ATT&CK techniques using a visual heatmap to identify gaps by threat relevance and detection status. Users select techniques to validate, while Vero AI maps them to relevant attack scenarios, helping prioritize high-risk areas and focus efforts where coverage is weakest.

With **Cymulate Detection Studio**, the MITRE heatmap can also be mapped directly to SIEM rules (in addition to assessments), providing a rule-level view of coverage. The heatmap is continuously updated to reflect evolving threats and environments.

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.

Cyber 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.