cymulate

Proactive, AI-Powered SIEM Rule Validation and Detection Engineering

Save time and resources by automating the most critical tasks in modern SecOps

Security Operations Center (SOC) teams are overwhelmed. Between maintaining hundreds of detection rules, reacting to daily alerts and trying to stay ahead of evolving threats, there's little time left for proactive improvement. Detection engineering has become a tedious, manual grind of rule writing, trial-and-error validation and ongoing tuning.

There can be a better way. Detection engineering capabilities should automate the most critical and resource-intensive tasks. Using AI-powered analysis and a massive library of real-world attack simulations, you can continuously build, test and fine-tune threat detection—so you can see what works, fix what doesn't and continuously optimize your detections. Let's explore the top challenges of detection engineering, and how the Cymulate Exposure Validation Platform can help solve them.

The Top 4 Detection Engineering Challenges — Solved

Challenge #1: Rule Validation is Complex and Time-Consuming

The Problem: Security teams are flying blind when it comes to whether their detection rules actually work. Manually testing each rule requires staging attacks, triggering alerts and sifting through logs often without clear answers.

The Cymulate Solution: Cymulate pulls your SIEM detection rules and automatically maps them to its attack actions library. You select a SIEM, run an assessment and Cymulate simulates the mapped threats in your environment. It then validates:

- Whether your rule fires as expected
- Whether data is being collected correctly
- What's missing if no alert is triggered

If the rule succeeds, it's a trusted detection. If it fails, you get precise, SIEM-native recommendations to fix it—automatically formatted for your platform.

Challenge #2: Rule Creation is Manual and Error-Prone

The Problem: Creating new detection rules for emerging threats is a huge lift. Teams must manually define use cases, identify log sources and write detection logic from scratch often without full visibility into whether they're chasing the right threats.

The Cymulate Solution: Cymulate removes the guesswork by tying detection rule creation directly to real-world adversary tactics. With the AI Template Creator, simply upload a threat advisory 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. Using AI and real threat data, Cymulate generates detection content and helps you build effective rules faster. You don't need to start from a blank slate. You start from known threats and map to rules that work.

Challenge #3: Most MITRE Techniques are not Covered by the Average SIEM

The Problem: While many SIEMs claim MITRE ATT&CK alignment, in practice, most only detect a limited subset of techniques, often focused on well-known tactics like initial access or execution.

The Cymulate Solution: Cymulate offers a visual MITRE ATT&CK heatmap that maps detection coverage against real-world threats.

It highlights which behaviors are successfully detected, which are missed, and which need improvement, giving teams the clarity to prioritize rule development and tuning. This targeted visibility helps streamline detection engineering efforts and ensures stronger coverage across the entire attack kill chain.

Challenge #4: Continuous Rule Tuning is Reactive and Never-Ending

The Problem: Threat actors constantly evolve. What worked last month might not work today. But most teams only tune rules after a missed detection, or worse, after an incident.

The Cymulate Solution: Cymulate enables continuous rule validation and tuning. As threats evolve, so does the Cymulate attack simulation library. You can schedule regular assessments that:

- Automatically re-test detection logic against new or updated threats
- Identify stale or ineffective rules
- Deliver automated tuning suggestions in your SIEM's native syntax

This turns detection tuning from a reactive scramble into a proactive, automated process.

From Guessing to Knowing: Cymulate Makes Detection Measurable

With deep integrations into leading SIEM platforms and a continuously updated MITRE ATT&CK heatmap, Cymulate transforms detection engineering from a black-box guessing game into a measurable, repeatable science. You get:

- Automated validation of existing detection rules
- Fast creation of new, high-fidelity detection logic
- Ongoing optimization based on real threat behaviors

Ready to automate your validation and detection engineering?

Cymulate automates the build-test-tune lifecycle of detection logic so you can stop threats before they exploit blind spots. You can validate your defenses, close detection gaps and spend less time chasing false alarms. Turn exposure into insight. Turn rules into results. Turn your SecOps team into a detection powerhouse with Cymulate. **Sign up for a demo today.**

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.