cymulate

SOLUTION BRIEF

SOC Optimization

Security operations teams are under pressure to prove that their detections, controls and response workflows work against the threats that matter most. But many security operations centers (SOCs) are still stuck in reactive alert handling, disconnected tooling and static playbooks, making it hard to demonstrate measurable risk reduction.

By combining exposure context, threat intelligence, production-safe validation and closed-loop testing, Cymulate helps SOC teams evolve to more proactive security. Prove what works, identify gaps and build new detections faster.

Prove Your SOC. Reduce Real Risk.

Cymulate validates whether SOC detections, playbooks and response workflows perform as intended against realistic threat scenarios. These results provide SecOps teams with evidence of detection coverage, response effectiveness and validated remediation, so they can focus on the gaps that pose the greatest risk.

With Cymulate, organizations can:

- **Validate detections.** Confirm that SIEM, EDR and XDR detections fire as expected against realistic attacker behaviors.
- **Improve detection engineering.** Build, test, tune and continuously revalidate detections to reduce noise and prevent rule drift.
- **Validate SOAR playbooks.** Test SOC playbooks and automated response workflows against realistic threat scenarios.
- **Prioritize threat hunting.** Turn threat intelligence, exposure context and validation results into focused hunt hypotheses and priorities.
- **Measure SOC improvement over time.** Track detection coverage, time-to-validate, validated remediation and response workflow effectiveness with defensible metrics.

Solution Benefits

Prove detection coverage

Validate SIEM, EDR and XDR detections against the threats that matter most.

Prioritize real risk

Use validation, threat and exposure context to focus on the highest-risk gaps.

Improve detection engineering

Safely and continuously test, tune and revalidate detection rules.

Validate response workflows

Test SOC playbooks, prove effectiveness and confirm fixes worked.

> In our most recent incident response exercise with Cymulate, we used three workstations across two geographic sites to replicate ransomware data exfiltration and lateral movement. Without Cymulate, it likely would have taken about 30 hours to set up. As a non-programmer, I'm not sure I could have executed it reliably. With Cymulate, the setup was easy and execution was worry-free. Overall, we cut the total prep time by at least 60%."
>
> – Head of Cybersecurity Operations, Credit Union

Validate Detection Coverage Continuously

Cymulate helps SOC and detection engineering teams prove whether detections work before a real incident occurs. Production-safe validation exercises test SIEM, EDR and XDR detections against real-world attacker behaviors, so teams can confirm what fires, what misses and where coverage needs to improve.

Instead of relying on assumed coverage or vendor claims, teams can map attacker techniques to detection logic, telemetry sources and control responses. Continuous retesting helps prevent detection drift and verify that rule changes improve coverage without introducing new noise or regressions.

Key capabilities include:

- Detection validation for SIEM, EDR and XDR controls
- Mapping of attack techniques to detection logic and coverage gaps
- MITRE ATT&CK-aligned coverage visibility
- Continuous retesting after rule changes, control updates and environmental drift
- AI-powered, environment-tailored validation with Cymulate Vero AI

Validate SOC Playbooks and Response Workflows

SOC playbooks are only valuable if they work against the threats most likely to impact the organization. Cymulate validates triage, investigation, enrichment and response actions against realistic threat scenarios, helping teams prove whether response workflows are relevant, effective and reduce risk.

By bringing validated threat and exposure context into response workflows, Cymulate helps SOC teams move from static playbooks to evidence-based response improvement. Teams can confirm that automated actions execute as intended, that analysts receive the right context and that remediation steps reduce validated exposure.

Key capabilities include:

- SOAR validation for triage, investigation, enrichment and response workflows
- Evidence that playbook actions are relevant and effective
- Exposure and threat context to improve response prioritization
- Closed-loop retesting to confirm that updates and remediation worked

Focus Threat Hunting on Validated Exposure Context

Threat hunting is most effective when hunters know which threats matter to the environment. Cymulate turns threat intelligence, exposure context and validation evidence into focused hunt hypotheses, helping teams prioritize the adversaries, campaigns, techniques and exposures most likely to impact the business.

SOC and threat hunting teams can use simulation evidence to validate assumptions, guide investigations and convert findings into improvements to detection or response. This helps reduce manual effort and ensures hunting activity is connected to measurable risk reduction.

Measure SOC Improvement Over Time

Cymulate helps SOC leaders demonstrate progress through evidence-based metrics rather than activity-based reporting. Teams can measure detection coverage, exposure window reduction, time-to-validate, validated remediation and response workflow effectiveness over time.

By connecting validation evidence to prioritized remediation and retesting, Cymulate gives security leaders a defensible way to show that SOC activity is reducing risk, not just creating more alerts.