cymulate

Lead Your Exposure Management Strategy with SecOps

Security Operations (SecOps) lives in constant motion. Threats evolve daily. New vulnerabilities and exposures surface hourly. Attackers don't wait for patch cycles or annual pen tests. They exploit the weakest link anytime, anywhere.

For this reason, security teams are overwhelmed. There's a recognition for proactive security, but teams struggle to understand what demands attention and how to quickly build threat resilience. Treating exposure management as an extension of vulnerability management is dangerous. A strategy of scan, patch and repeat no longer works. It doesn't reflect how attackers operate. This leaves SecOps teams forever reacting instead of getting ahead. To truly get proactive, SecOps must lead exposure management. That means continuous visibility, real-time validation and adaptive response. It's the blueprint for **Continuous Threat Exposure Management (CTEM)**.

The Exposure Management Mandate for SecOps

Traditional vulnerability management revolves around a list of weaknesses, but SecOps needs far more. You need to know:

What's new today?

Which exposures and external threats are emerging right now?

What's real?

Which weaknesses are exploitable by attackers in your environment, bypassing your defenses?

What's the best option?

Should you patch, reconfigure or apply a "virtual patch" by tuning security controls?

SecOps Should Drive CTEM

SecOps already has the visibility and mandate to see risk in motion: detection coverage, defensive gaps and day-to-day operational threats. By taking ownership of exposure management, SecOps can:

- **Validate threats continuously** against live infrastructure and evolving TTPs.
- **Optimize security controls** so prevention and detection align with current threats.
- **Translate findings into action** with remediation and detection rules ready for SIEM, EDR and XDR deployment.

This shift transforms exposure management from a static, scanner-driven checklist into a dynamic, intelligence-driven discipline reflecting how attackers truly operate.

Organizations using Cymulate for SecOps-driven CTEM achieve:

52%	**reduction** in critical exposures
3x	**lower** breach likelihood with a 30% boost in threat prevention
60%	**increase** in team efficiency through streamlined workflows

How Cymulate Empowers SecOps

Cymulate equips SecOps with **production-safe, automated exposure validation** that integrates directly into daily workflows.

01 Validate Resilience to Today's Threats

- Test new TTPs and exploits against your environment as soon as they emerge.
- Confirm whether security controls detect and prevent the latest threats.

02 Baseline Security Posture and Identify Drift

- Create a baseline of security posture and unexpected decreases in threat coverage with security control dashboards.
- Provide proof of the current state of cyber resilience with MITRE ATT&CK heatmaps and technical and executive level reports.

03 Optimize Threat Prevention and Detection

- Integrate with security controls to push updates for immediate threat prevention.
- Build and fine-tune EDR, XDR and SIEM detection rules to block real attacks.

04 Prioritize Exposures Based on Business Context

- Correlate validated exposures with threat intelligence and asset criticality.
- Focus on the exposures that present the highest risk to operations and business outcomes.

05 Drive a Proactive Security Culture

- Lead the organizational shift from chasing alerts to preventing incidents with continuous, production-safe testing.
- Collaborate seamlessly across blue teams, red teams and vulnerability management to embed exposure management into daily workflows.

SecOps Benefits

Proactive Exposure Management

Evolve SecOps from reactive threat response to proactively build threat resilience.

Measurably stronger cybersecurity

Security controls optimized for threats with proof and evidence of validated threat coverage.

Faster validation and tuning for new threats

Test new threats in under one hour, deploy IOCs in seconds and build new detection rules in minutes.

Identify security drift

Maintain threat resilience by identifying weaknesses that were previously strengths.

Next Steps

Move beyond static checklists. Make exposure management a SecOps discipline. Cymulate helps SecOps evolve into proactive defenders continuously validating threats, optimizing controls and accelerating resilience.

Start Your Live Demo

About Cymulate

Cymulate is the leader in exposure management that proves the threat and improves resilience. More than 1,000 customers worldwide rely on the Cymulate platform to prove, prioritize and optimize their threat resilience as they make threat validation a continuous process in their exposure management programs. Cymulate integrates with assessment tools and continuously tests defenses against the full kill chain of attack techniques providing cybersecurity teams with the automation and insights to prove and optimize threat resilience; accelerate detection engineering; drive continuous threat exposure management; and measure and baseline security posture. Prove the threat. Improve resilience. For more information, visit www.cymulate.com.