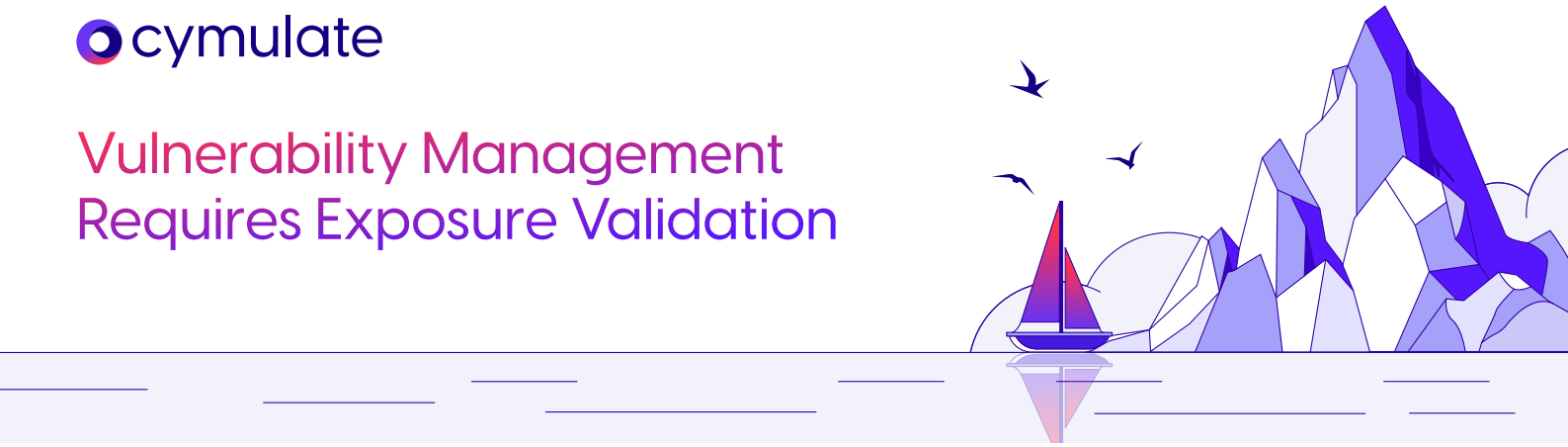
cymulate

Vulnerability Management Requires Exposure Validation



Vulnerability managers are drowning in a flood of CVEs, endless "critical" flags and pressure from leadership to "fix it all." But in truth, most of that noise is not real risk and patching everything is unrealistic. Prioritizing based on threat intelligence is not enough. Without validation to prove the theoretical and confirm exploitability, vulnerability management is a guessing game. When attackers move faster than patch cycles, guessing isn't good enough.

Vulnerability Management Realities

Vulnerability scanners are excellent at one thing: listing out potential weaknesses. They're less helpful when it comes to answering the question that matters most: **"Which of these vulnerabilities can actually be exploited in my environment right now?"**

The result?

- **Overwhelming backlogs** of "critical" weaknesses that may never be touched by an attacker.
- **Wasted time and resources** chasing theoretical risks instead of real threats that have been proven to have mitigation gaps and likely impact business operations.
- **Siloed data** from scans, asset inventories and patching systems that never paints a full picture.

Attackers don't care how many vulnerabilities your scanner found. They care about the ones they can exploit today, in your environment, with your existing controls in place.

Why Traditional Vulnerability Management Isn't Enough

Legacy vulnerability management programs often stop at detection. You scan, you report, you patch. But modern cyber resilience demands a shift away from counting vulnerabilities and patches and reporting on "high severity" issues without context. Some programs may have some level of prioritization based on threat intelligence and theoretical attack path mapping, but this is not enough. It does not test your existing security controls. Instead, it's time to focus on:

- **Validating** against live infrastructure and evolving TTPs.
- **Optimizing** so prevention and detection align with current threats.
- **Translating** with remediation and detection rules ready for SIEM, EDR and XDR deployment.

The key to this shift: **Continuous Threat Exposure Management (CTEM)**.

CTEM: Closing the Gap Between Theory and Reality

CTEM doesn't just list exposures. It proves which exposures matter by continuously testing your defenses against real-world threats. With CTEM, you can:

- **Integrate exposure discovery** across your endpoint, network, cloud, applications and data.
- **Automate threat validation** to simulate real attacks, validate existing prevention and detection and confirm exploitability.
- **Prioritize with context,** combining technical severity, business impact and proof of exploitability.
- **Mobilize with evidence-based remediation** that teams can act on immediately.

How Cymulate Elevates Vulnerability Management to CTEM

Cymulate puts the "T" in CTEM by delivering the key component traditional vulnerability management programs lack: continuous threat validation. **Here's how it works:**

01 Integrate Exposure Discovery

- Ingest and aggregate data from vulnerability scans and asset discovery.
- Enrich automated threat validation with full context for an accurate picture of your attack surface.

02 Automate Exposure Validation

- Integrate with existing security technologies across the architecture.
- Test and prove threat resilience for attacks and exploits that target vulnerabilities and exposures.
- Run automated attack scenarios to identify existing threat prevention and detection exposures.

03 Prioritize with Context

- Calculate actual risk scores by aggregating data across validated prevention and detection controls, threat intelligence, asset criticality and business context.
- Stack-rank exposures with full context of threat resilience and validated exposure scoring – filter on proven most critical risks.

04 Mobilize w/ Automated Remediation + Streamlined Detection Engineering

- Create actionable plans backed by hard evidence from threat validation.
- Push new detection rules formatted for easy implementation into EDR, XDR and SIEM technologies.
- Streamline patching and detection engineering so teams fix what matters first.

Are You Managing Risk, or Just Managing Lists?

If your vulnerability management program is still operating without threat validation, you're working harder than you need to and taking on more risk than you think. It's time to modernize and move beyond patch counts and vulnerability reports to a risk-proven approach. With Cymulate, vulnerability managers gain the power to:

Prove which vulnerabilities matter most

Prioritize with confidence

Show measurable improvement in resilience

Prove the threat. Improve resilience. Discover how Cymulate can transform your vulnerability management into a fully validated CTEM program so you can focus on the threats that matter, cut risk faster and sleep better at night.

Measurable Impact

Organizations modernizing vulnerability management with Cymulate have achieved:

52% **reduction** in critical exposures

3x **lower** breach likelihood with a 30% boost in threat prevention

60% **increase** in team efficiency through streamlined workflows

Benefits

- **Focus on the Exploitable**
  Zero in on vulnerabilities attackers can actually use in your environment.
- **Streamline Workflows and Integrate Security Teams**
  Break down silos by integrating vulnerability management data with threat validation findings in one integrated process.
- **Prioritize Actionable Remediation**
  Create evidence-backed, context-driven remediation plans that accelerate time to risk reduction.
- **Measure & Improve Threat Resilience**
  Benchmark performance and threat resilience with dynamic reporting and dashboards and monitor for security drift so you can prove ROI to leadership.

Contact us for a live demo **Start Your Live Demo** info@cymulate.com www.cymulate.com