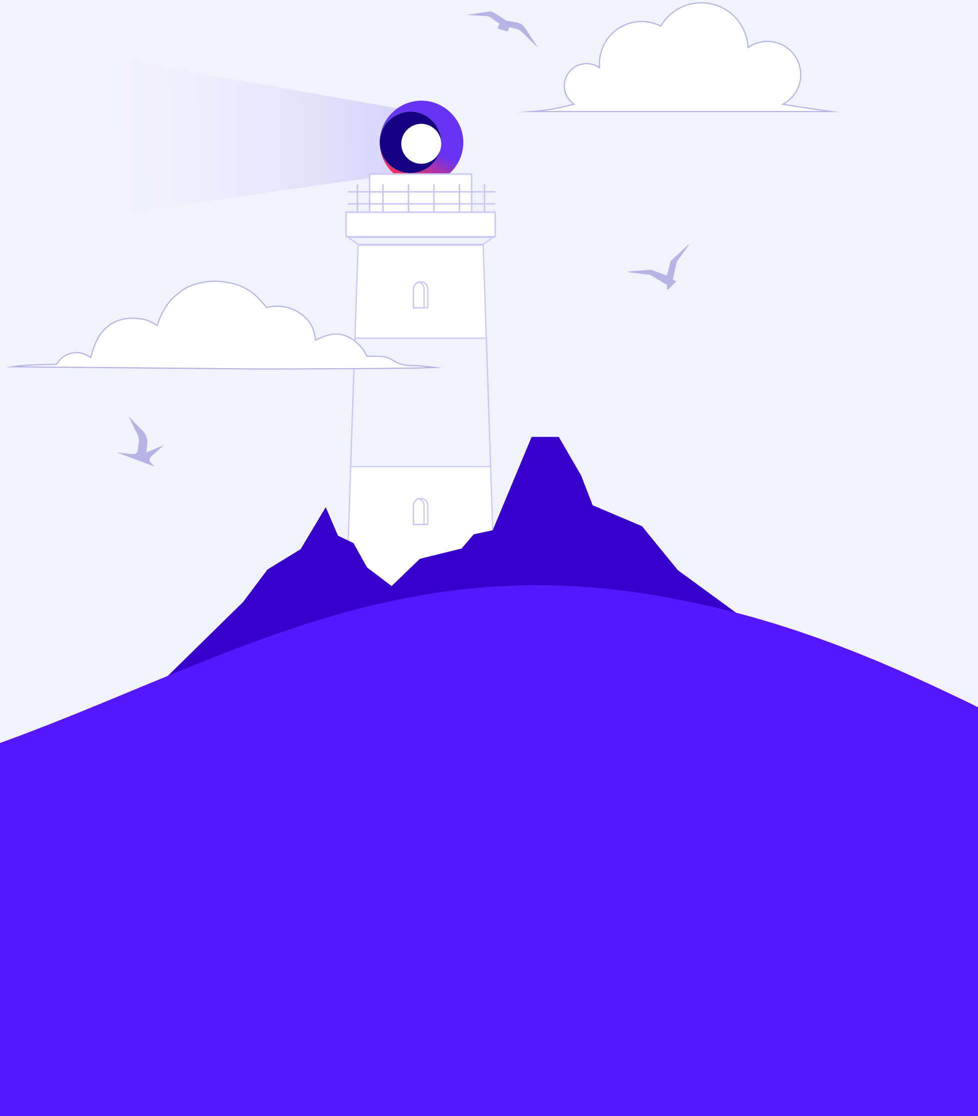
cymulate

Putting the Validation in Exposure Management

Four best practices to drown out the noise and focus on the (truly) exploitable



The SecOps Challenge

Change, Uncertainty and No Control

SecOps teams have it rough. Every day, they are responsible for the security effectiveness of their organization. At the same time, they are dealing with constant change, continuous uncertainty and a growing lack of control. Why? Attack surfaces are in a state of flux, with about 300 new services added every month. These services alone account for nearly 32% of new high or critical exposures for organizations. This is compounded by the fact that 111 new vulnerabilities are reported every day by the National Vulnerability Database. And only 5% of vulnerabilities are being patched each month.

Are the right vulnerabilities being patched? Are security controls being tested and tuned on a regular basis? Can critical exposures across dynamic and ephemeral IT environments be identified? This perfect storm means SecOps teams are struggling to keep pace while 70% of CISOs feel at risk of suffering a material cyber attack.

And it doesn't end there.

Security silos exacerbate uncertainty

While SecOps teams struggle with the daily evolution of threats, dynamic changes to environments and exponential growth of vulnerabilities, they're also faced with the internal struggle of working in silos.

Different teams focused on different silos results in a lack of visibility into the end-to-end problem and solution. With no consistent, hard data to analyze or use for reporting, SecOps teams are left:

Blind to real gaps and exposures

Unable to prioritize the riskiest threats

Unsure if security controls are working

Unable to remediate quickly (if at all)

If any of this sounds familiar, you're not alone. There's got to be a better way to harden defenses and navigate the dynamic threat landscape.

The Evolution to Exposure Management

The only way to overcome these challenges is to adopt a new approach to cybersecurity – one that is proactive and preemptive. Exposure management gives you an attacker's view of security gaps and insight on how security controls and processes respond to threats that target those weaknesses.

By implementing this proactive security measure into an ongoing process within your security program, you evolve into continuous threat exposure management (CTEM).

To build and execute a continuous effort to optimize both the short-term response and the long-term security posture, Gartner® created the CTEM framework that integrates scoping, discovery, prioritization, validation and mobilization.

A failure to validate

With the industry evolving to exposure management, traditional security vendors moved quickly to position their existing products as exposure management platforms. There's just one problem – they ignore the role of validation and the essential function of exposure management that filters the potentially thousands of vulnerabilities and exposures down to the truly exploitable by validating how defensive controls prevent, detect and respond to threats that target the exposure.

This flawed approach to exposure management ignores the fact that you already spend millions every year on security controls.

The reality is no one platform can cover the depth and breadth of exposure management on its own – this requires ecosystems built on open integrations. Most CTEM solutions are just repackaging the same old vulnerability management technologies under a new name, so they introduce the same challenges to security teams:

- Too many high-severity points of threat exposure that can't be fixed
- Closed systems that can't consolidate and correlate data from security controls and other systems
- And most of all, no validation to prove that the exposure is actually exploitable in your environment

CTEM without full security validation can't see the full benefit of exposure management because it fails to consider how your controls, systems and process respond to the threat. Without security testing of the threat, there's no real knowledge of what's truly exploitable in your environment.

Full Context Reveals True Exposures

Are you ready to take back control of your cyber defenses, break down security silos and put an end to the constant uncertainty? The solution is to validate what's truly exploitable for you, know what to fix first and how to optimize your controls.

CTEM without security control validation will leave you guessing and working with theoretical threats instead of focusing on real exposures in your environment.

You need a full-context exposure management platform. This will empower you to focus on the truly exploitable by validating security controls and proving real threat exposure with the full context of security control effectiveness, active threat intelligence and business impact.

Four Ways to Take Back Control of Your CTEM

Focus on your true exposure

The first step toward exposure management can be as simple as correlating the vulnerability or exposure with control effectiveness. This analysis provides the proof and evidence of your true exposure. Get the full context by adding threat intelligence for active campaigns and the business context of effected systems to understand business impact and criticality.

Validate your controls

To provide that correlation and proof of true exposure, you can't rely on your outdated penetration test. Continuously test and validate security controls and the exploitability of threat exposures with real-world attack simulations based on the latest active threats.

Optimize your defenses

Prioritize response plans for exposures validated via the correlation of threat assets and existing controls with guidance and insights to harden your defenses. Build custom mitigation rules and get automatic control updates.

Prove your cyber resilience

Benchmark and trending data provide a comparison against industry and sector peers. Map results of attack behaviors to NIST and MITRE ATT&CK frameworks.

The Bottom Line

Your evolution to exposure management can't be more of the same failed approaches to vulnerability management. You have options, and the ability to take back control, stop the uncertainty and maintain security that adapts to the constant cycle of change. But this all hinges on the right approach and the right technology that proves the exploitability of the exposure specific to your environment.

Remember: CTEM that doesn't correlate exposure prioritization with full security validation isn't enough. Your security controls are the crux of your defense, and the true risk of any threat can only be understood with the added context of attack paths and the effectiveness of existing controls.

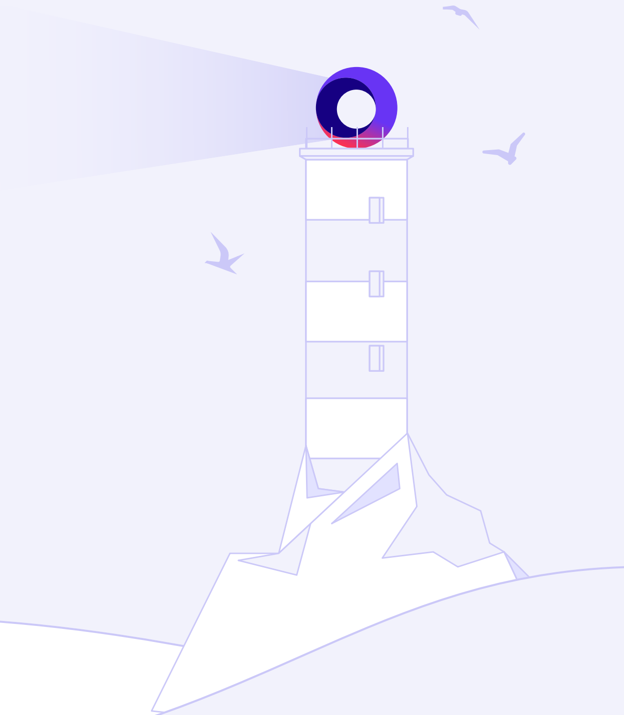
You need a full-content exposure management platform that enables you to:

Focus on your true exposure

Validate your controls

Optimize your defenses

Prove your cyber resilience



Learn More About Exposure Management

Continuous Threat Exposure Management (CTEM)

From Theory to Practical Implementation

DOWNLOAD WHITEPAPER

Schedule a Demo
Get a private demo to see the benefits for your organization

REQUEST A DEMO

About Cymulate
Cymulate, the leader in exposure management and security 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 500 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.