DATA SHEET

Cymulate Exposure Management

Prioritization and Remediation

Focus on *Your* Exploitable Exposures

Without validation, exposure management is just vulnerability management by another name – a long list of theoretical risks, lacking context, overwhelmed by volume and blind to what can actually be exploited.

Cymulate Exposure Management automates threat validation, so you can move from theoretical to actionable by proving which risks are truly exploitable in your environment. By leveraging findings from attack simulations run through Cymulate Exposure Validation, you gain empirical proof of threat resilience to confidently prioritize and mobilize remediation efforts where they matter most.

This scoring process enables true exposure management by driving collaboration across security functions. Armed with evidence of what's truly exploitable, SecOps, red teams and vulnerability management teams share a validated view of exposure and risk. With proof as a common language, teams reduce friction, work more efficiently and focus remediation efforts on the exposures that matter most.

Score Exposures with Validated Prevention & Detection

Cymulate Exposure Management analyzes and scores exposures and vulnerabilities by considering your threat resilience to exploits that target the exposure. Cymulate Exposure Management first consolidates exposure findings by integrating with vulnerability scanners and other exposure discovery tools and then correlates those exposures with Cymulate Exposure Validation attack simulation findings.

The result is a stack-rank of all exposures based on **validated exposure scoring** that considers:

- Proof and evidence of threat prevention and/or threat detection
- Threat intelligence for known exploits, threat actors and active campaigns targeting your industry
- Business context and asset criticality

Unified Inventory of Assets and Exposures

Cymulate integrates with your existing security and IT tools to build a comprehensive view of assets and exposures across your environment. The asset inventory aggregates a list of components and resources within your infrastructure that are monitored and managed for security purposes.

The list of exposures contains in-depth information about each exposure, including details on impacted assets, status, related tasks, data from integrations, associated Common Vulnerabilities and Exposures (CVEs) and exploitability details. This centralized inventory provides the context needed to assess risk accurately and act decisively.

Benefits

52% ↓ in critical exposures

Prioritize exposures based on exploitability with proof of threat resilience and effective mitigation.

60% more efficient prioritization

Automation and workflows to stack rank exposure with evidence of risk.

Escalate high-risk, low-severity

Elevate low and medium exposures that are exploitable and impact critical assets.

> We integrated Cymulate with our vulnerability management to validate each vulnerability and understand if there are compensating controls in place protecting us. It helps us focus and prioritize the high-risk vulnerabilities that are exploitable in our environment.
>
> - Raphael Ferreira
> Cybersecurity Manager, Banco PAN

Business-Aligned Asset Classification

Categorize your aggregated assets based on business impact to enable more precise risk prioritization. Automated filters and tagging assign assets to defined business tiers, highlighting your most critical systems (“crown jewels”) and aligning exposure scoring with organizational priorities.

Risk-Based Exposure Prioritization

For every discovered exposure in your environment, Cymulate Exposure Management delivers a **severity analysis** that goes beyond basic CVSS scoring. Exposure analysis is based on proof of exploitability and on a combination of threat intelligence, the affected asset’s business context and the original CVSS (Common Vulnerability Scoring System) score. This combination of data enables you to begin prioritizing exposures based on their potential impact on your organization.

If Cymulate Exposure Validation has testing data related to the exposure, that proof of prevention and/or detection is included in the analysis. If there’s no history of validation for that exposure, Cymulate Exposure Management provides the option to launch attack simulations that exploit the exposure and prove the current state of your detection and prevention. Post assessment, Cymulate calculates a **validated exposure score** based on detection and prevention ratios and feeds this score into the severity analysis.

In this example, CVE-2025-1017 was initially rated a critical risk (9.3 CVSS), but Cymulate attack simulations revealed strong detection and prevention. This information, combined with threat intelligence and asset criticality, fed into a Cymulate severity analysis that delivered a more contextual assessment. As a result, the exposure risk score was reduced to medium (6.6).

Focused and Streamlined Remediation

With stack ranking of exposures, Cymulate helps you focus your remediation efforts on exposures that can penetrate your defenses and provides remediation guidance that optimizes control effectiveness. The platform also allows you to rerun the assessment to easily validate remediation.

Why choose Cymulate?

Put the “T” in CTEM

Make threat validation a continuous process with collaboration across security operations, threat intel and vulnerability management teams.

Focus on Real Threats

Prioritize remediation on exposures and vulnerabilities that are actively targeted and exploitable as proven by threat validation.

Improve Decision Making

Move from asset-centric to impact-centric prioritization, aligning security with business risk for improved decision making.