cymulate

SOLUTION BRIEF

Exposure Prioritization

Vulnerability Management Lacks the Proof of Exploitability

Security teams are overwhelmed by the large number of potential exposures found in their organizations, so they look for ways to prioritize and reduce their patching workloads. Traditional vulnerability prioritization strategies usually hinge on the Common Vulnerability Scoring System (CVSS) and may include threat intelligence regarding known exploits, active campaigns and industry threats. However, these factors often lack the insights to evaluate exposures in the context of an organization's distinct environment. Organizations require vital information that standard vulnerability management programs and tools don't provide.

Start Prioritizing with the Context of Security Control Effectiveness and Business Impact

With market-leading **breach and attack simulation**, Cymulate validates control effectiveness with production-safe attack techniques that target the vulnerability and potential exposure. The Cymulate platform also includes **continuous automated red teaming** to map attack paths and visualize impact of a successful attack.

Cymulate prioritization also considers the business context of effected assets, systems and applications. Cymulate groups assets to one or more pre-defined "business contexts," groups of assets that share similar impacts on the organization's risk. These contexts include business units, product lines, subsidiaries, regions or other relevant groupings to evaluate risk more granularly.

> Cymulate helps us prioritize exploitable vulnerabilities in our environment. By integrating with our vulnerability management products and running Cymulate assessments, we can easily discover which vulnerabilities are an actual threat to our organization.
>
> - Kevin Roberts, Information Security Analyst, Nedbank

Solution Benefits

Reduce exposure risk

Prioritize high-risk exposures and remediate them quickly, preventing the likelihood of exploitation.

Focus on validated exposures

Simulate attacks on your security controls to understand which exposures are actually exploitable.

Optimize security operations

Reduce the patching workload and maximize team productivity by focusing on high-impact remediation activities.

Accelerate mitigation

Mobilize teams to action with a clearer understanding of a vulnerability's operational and business impact.

Threat Intel Provides Context to Active Campaigns

When prioritizing exposures, the Cymulate platform also applies the latest threat intelligence. Daily threat feeds update Cymulate with the active threat campaigns, targeted industries and effected geographies – all mapped back to the exposure and attack techniques validated with breach and attack simulation. This Cymulate analysis for exposure prioritization also includes updates from the Known Exploited Vulnerabilities catalog maintained by the U.S. Cybersecurity and Infrastructure Security Agency to elevate the severity based on exploits in the wild.

Streamline and Prioritize Mitigation Tasks with a Remediation Plan

The Cymulate platform correlates threat exposures with security control effectiveness, threat intel and business context to prioritize true exposures and produce detailed remediation plans that include:

- Explanation and evidence of the exposure
- Effected assets and their business context
- Guidance for remediation, such as configuration updates for infrastructure, clouds, applications and controls
- Custom mitigation rules to add threat detection in endpoint and SIEM
- Integration with ticketing systems to mobilize action

Integrate with Vulnerability Management

tenable | RAPID7 insightVM | CROWDSTRIKE | Qualys | Microsoft Defender Vulnerability Management

> 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

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.

Get a Demo