Vulnerability Prioritization Technology
Solution Brief

Unmanageable Number of Vulnerabilities

Vulnerable software is the leading attack target for cybercriminals. The mix of legacy and old operating systems, opensource code, M&As, and third-party software, as well as the continuously changing threat environment leaves companies exposed. With the increasing number of Common Vulnerabilities and Exposures (CVEs), patching methodologies solely based on the Common Vulnerability Scoring System (CVSS) create long and risky patching windows that are costly and unmanageable. The IT team in charge of patching have additional responsibilities and should focus on patching vulnerabilities that can actually be exploited.

Reduce Risk and Cost with Cymulate's Vulnerability Prioritization Technology

Different vulnerabilities pose different risk levels; some are more difficult to exploit, and they also vary by impact. Cymulate's Vulnerability Prioritization Technology (VPT) integrates with common vulnerability scanners to continuously provide organizations with the visibility and context they need to create an action plan based on prioritization for risk reduction. Based on simulated and emulated attacks, it complements severity with exploitability and accounts for the effectiveness of compensating security controls in an environment.

Vulnerability Prioritization Technology empowers organizations to:

Benefits

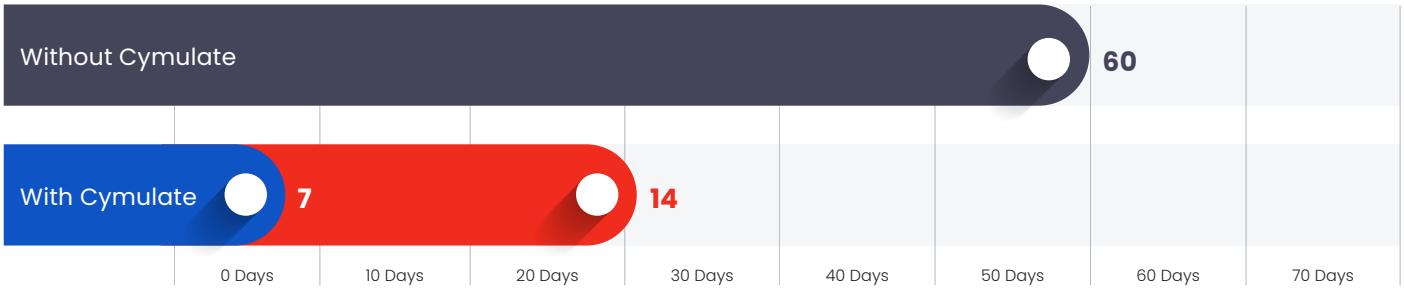
Improve Staff Workload Management

Cymulate enables organizations to correlate the criticality of vulnerabilities with the value of assets and the likelihood that they will be exploited. This allows companies to optimize patching prioritization, reduce the patching workload, and maximize team productivity. For example, if the same asset appears in multiple simulated attacks, then instead of patching multiple vulnerabilities, an organization can focus its remediation efforts on strengthening the controls surrounding that one asset.

Reduce Exposure Time

It takes an average of 60 days to patch a critical risk vulnerability (2022 Vulnerability Statistics Report, Edgescan) leaving companies open to attacks during this time. Vulnerability scanners don't provide context about a vulnerability's business impact, so companies rely only on CVSS scores to prioritize patching. On average, Cymulate detects and evaluates a vulnerability within approximately 7 days. The platform adds context to the vulnerability, so organizations understand immediately the impact the vulnerability has on its risk level and the business as a whole. Organizations prioritize and patch high-risk vulnerabilities immediately, drastically reducing the risk of their exposure.

Vulnerability Exposure Window *



Detect Vulnerability Average Patching Window Detect Vulnerability and Average Patching Window

* This chart is for illustrative purposes only.

Minimize Costs

Cymulate enables security leaders to make data-based decisions about their cybersecurity risk, resulting in correlating their patching schedule to their tolerable level of risk. Once they understand each vulnerability's level of risk and incorporate compensating controls into the equation, they decide how fast or slow the vulnerability needs to be remediated, prioritize accordingly, and minimize patching costs.

Potential Yearly Cost Reduction for a Large Enterprise

100%

Patch **100%** of all endpoints and **100%** of business-critical vulnerabilities within two weeks **$5M/Yr**

OR

75%

Patch **75%** of all endpoints and **95%** of business-critical vulnerabilities within four weeks **$1M/Yr**

Cymulate

How It Works

Cymulate's VPT dashboard enables handling high-risk, mission critical vulnerabilities first in a short period of time. Knowing what's essential to patch first and what doesn't require immediate attention or resources, leads to a more robust cybersecurity posture and a better sense of control.

01

Validate

Continuously run the latest threats and purple-team exercises to determine whether security controls are effectively blocking malicious payloads known to exploit existing vulnerabilities.

02

Analyze

Create a contextualized view on attack results per CVE:

- Was the vulnerability exploited successfully in the environment?
- What assets were affected?
- Can security controls be finetuned to protect the assets instead of patching the vulnerability?

03

Remediate

Go patch! Update your patch management policy according to the report to quickly reduce risk and save time and costs. Finetune any compensating security controls where necessary to address low risk vulnerabilities.

04

Track

Track your patch management policy's progress with the Cymulate ticketing system integration. By managing security tasks from within the Cymulate platform, security and IT teams can respond to patching vulnerabilities faster, more efficiently, and stay focused on what is most critical to the organization.

About Cymulate

Cymulate was established with the vision of empowering security professionals to make better decisions faster, based on real-time data. Founded and led by an elite team of cyber researchers with world-class experience in offensive cyber solutions, Cymulate is determined to become the golden standard for security professionals and leaders to know, control, and optimize their cybersecurity posture end to end. Trusted by hundreds of companies worldwide, Cymulate constantly enhances its methods to prepare organizations for any attack scenario or campaign. With Cymulate, organizations continuously measure security performance in real-time, shore up defenses, and assure operational effectiveness. **Measuring your cybersecurity performance is fundamental towards creating a more secure organization!**

Contact us for a live demo, or get started with a free trial

Start Your Free Triel

Headquarters: Maze St 3, Tel Aviv 6578931, Israel | +972 3 9030732 | info@cymulate.com | US Office: +1 212 6522632