cymulate

Vulnerability Management Must Evolve to CTEM:

A Technical Guide for Today's Threat Landscape

Vulnerability Management (VM) Challenges

Overwhelmed with limited resources

Overwhelming and growing list of patches

With thousands of common vulnerabilities and exposures (CVEs) published every year, traditional vulnerability management (VM) teams struggle to keep pace. They are faced with a continuous patching backlog and spend too much time identifying issues vs. assessing and remediating.

Resource constraints

With limited resources, VM teams juggle patch management, compliance reporting and a host of other security duties. To stay resilient against threats, they need an efficient and effective solution to prioritize and allocate resources.

Ineffective prioritization

Relying solely on public threat feeds, many VM teams lack a clear picture of which vulnerabilities matter the most to their own organization. Even with data on exploitability and asset criticality, the critical threat validation piece to assess their actual security posture is missing. They lack insight into how their existing security defenses and detection tools reduce or amplify risk for these vulnerabilities.

VM teams have a long list of critical patches, but which ones are actually critical and which ones can be safely delayed?

The Reality of Security

With organizations being constantly overwhelmed by an ever-growing number of vulnerabilities combined with limited resources, it makes it nearly impossible to address them efficiently. The resulting gap between detection and remediation combined with a lack of clear visibility into which patches are most critical leaves businesses exposed.

5%

of vulnerabilities **patched** each month

Source: Bitsite

60%

of breaches involve **unpatched** vulnerabilities

Source: Gartner

32%

of SecOps say **they have too many exposures to prioritize**

Source: Gartner

The Hard Truth

Organizations cannot immediately patch every vulnerability and do not know which ones are most critical. Security teams do not know what patches can be safely delayed.

The Solution

Continuous Threat Exposure Management

While many teams are expanding to exposure management to consider the broader attack surface and non-CVE exposures, only continuous threat exposure management (CTEM) provides the framework and process to answer the critical questions of:

1. What must be patched **now vs. scheduled** for the next update?
2. Is the perceived severity already mitigated with **existing security controls**?
3. How can security teams proactively build **threat resilience** through mitigation?

CTEM goes beyond standard find-prioritize-fix processes to include **threat exposure validation**, which adds the context of what's exploitable in the environment.

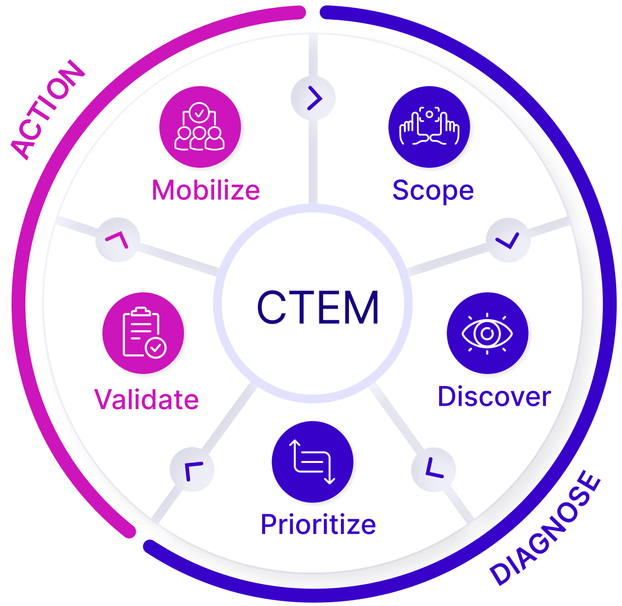
Threat exposure validation is the critical missing piece in many platforms that claim full CTEM. It delivers organizations data-driven evidence on how an attacker can exploit the vulnerability by evading specific security controls and policies.

With insight into both the exposure and defense readiness, security teams gain the insight needed to prioritize effectively by escalating the most critical exposures and de-escalating those of lower significance. By proactively remediating high-priority threats, organizations strengthen their resilience and enhance overall prevention and detection.

Defining Vulnerability Management vs CTEM

Traditional vulnerability management is periodic and reactive, whereas CTEM is continuous and risk-driven. Vulnerability management focuses on answering the question “what are my vulnerabilities?” and CTEM addresses “what exposures truly matter?”

	Vulnerability Management Reactive and periodic	**Continuous Threat Exposure Management** Proactive, continuous and risk-driven
Scope	Not applicable. Broadly applies to all assets and systems managed by IT.	Focus on critical business processes and functions.
Discover	Users run scans to find network and asset vulnerabilities, either weekly or monthly.	Go beyond vulnerability scanning to identify all potential exposures in cloud, SaaS, data, identity and more.
Prioritize	Prioritize vulnerabilities from CVSS scores – may include some level of exploitability and business impact.	Aggregate all sources of exposure and stack rank based on context of threat, business impact, what can be patched and what can be mitigated.
Validate	Not applicable. No exposure validation.	Demonstrate real-world exploitability with attack simulations that validate your prevention and detection controls allowing organizations to prioritize what truly needs fixing.
Mobilize	Track remediation tickets of patches and generate compliance reports.	Collaborate with business owners to determine which exposures require immediate remediation, while enabling security teams to strengthen defenses through improved security controls.



How to Evolve to CTEM

The steps an organization should take to evolve to a CTEM program

Evaluate Your Current Landscape

Begin by identifying and assessing your existing security tools, technologies and processes to understand how your organization currently discovers, prioritizes and mitigates exposures. This baseline will help you determine your strengths, redundancies and inefficiencies.

Pinpoint and Prioritize Gaps

Once you have a clear picture of your current state, identify the critical gaps that hinder your ability to continuously manage and reduce threat exposure. These could include blind spots in asset visibility, fragmented data sources, a lack of integration across tools or ineffective collaboration across security teams.

Define a Strategic, Business-Aligned Scope

Focus your CTEM efforts where they will deliver the greatest impact. Align your scope with business priorities, such as protecting high-value assets or meeting compliance requirements. Start with a manageable segment to demonstrate quick wins and ROI. If successful, this will enable the expansion and maturation of your CTEM program.

Incorporate Threat Validation

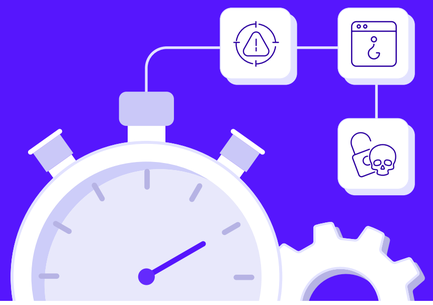
Incorporate threat validation in your exposure prioritization process to ensure your most critical threats are being mitigated. This will allow you to understand if you already have existing threat prevention and/or detection in place for your identified security gaps.

Expand to Continuous Threat Validation

Implement continuous threat validation to continually test and evaluate how well your security controls are preventing and detecting against attacks.

Prioritize Exposures Effectively with Threat Validation

Unifying complex factors into the Cymulate severity risk score



Vulnerability Context

Describes the CVE, which includes the identification number, components, vectors, impact, severity score and available patches.

What is the vulnerability, how it is executed, what is the criticality level and is there an available patch?

Threat Intelligence

Describes the threat information for a CVE, which includes the information on known exploits and threat actors.

Has this vulnerability been exploited before, and what are the threat actors?

Business Context

Describes the affected business assets that the vulnerability affects. Example – domain controllers are likely to be defined as critical risk level.

Which of my assets are affected by this vulnerability and what is the business assigned and tolerated risk level?

Threat Prevention & Detection

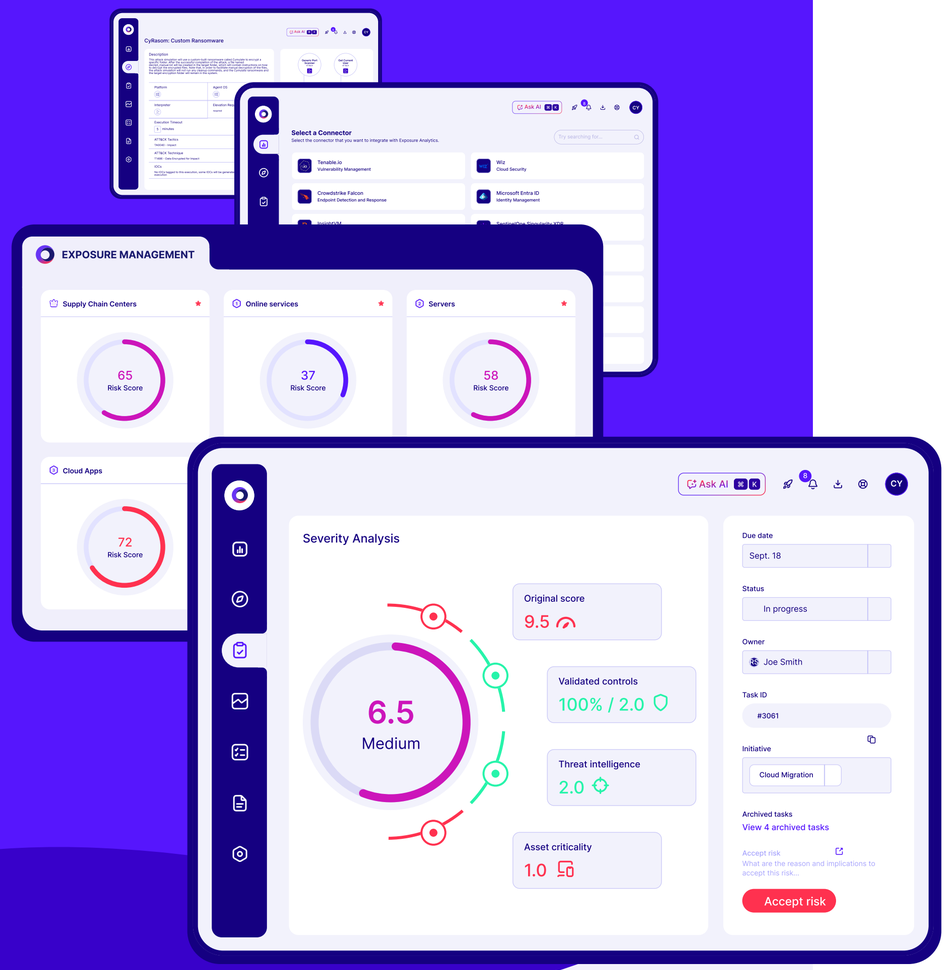
Delivers insight into the CVE's impact in the organization's environment with existing (or lack of) threat prevention and detection from security controls in place.

How can an attacker exploit the vulnerability and do you already have security policies providing security prevention or detection coverage?

"Only 34% of organizations prioritize vulnerabilities and exposures effectively."

Source: Gartner

The Cymulate Advantage



Cymulate Exposure Management Platform

AI-powered CTEM with threat validation

The Cymulate platform integrates exposure data and automates threat validation to assess risk, optimize security defenses and improve threat resilience. It integrates with assessment tools and continuously tests and validates security controls against the latest advanced threats and the full kill chain of attack techniques. With AI and automation, security teams are equipped to quickly and easily find and fix their security gaps and vulnerabilities that can be exploited. **Cymulate will allow your organization to:**

- Prove resilience to the most advanced cyber attack based on actual security policies
- Optimize security controls
- Accelerate detection engineering
- Measure and baseline security posture
- Monitor and alert on security drift
- Improve threat resilience

Integration with Vulnerability and Security Technologies

Enables effective exposure prioritization

Vulnerability Management Tools

Cymulate **integrates with vulnerability management systems** to provide a complete picture of an organization's assets and exposures. This ingested exposure data is correlated with simulated attack tests and calculates true risk scores.

Sample Integrations with new integrations added regularly

tenable · RAPID7 insightVM · Qualys. · SentinelOne · CROWDSTRIKE · Windows Defender

Security Technologies

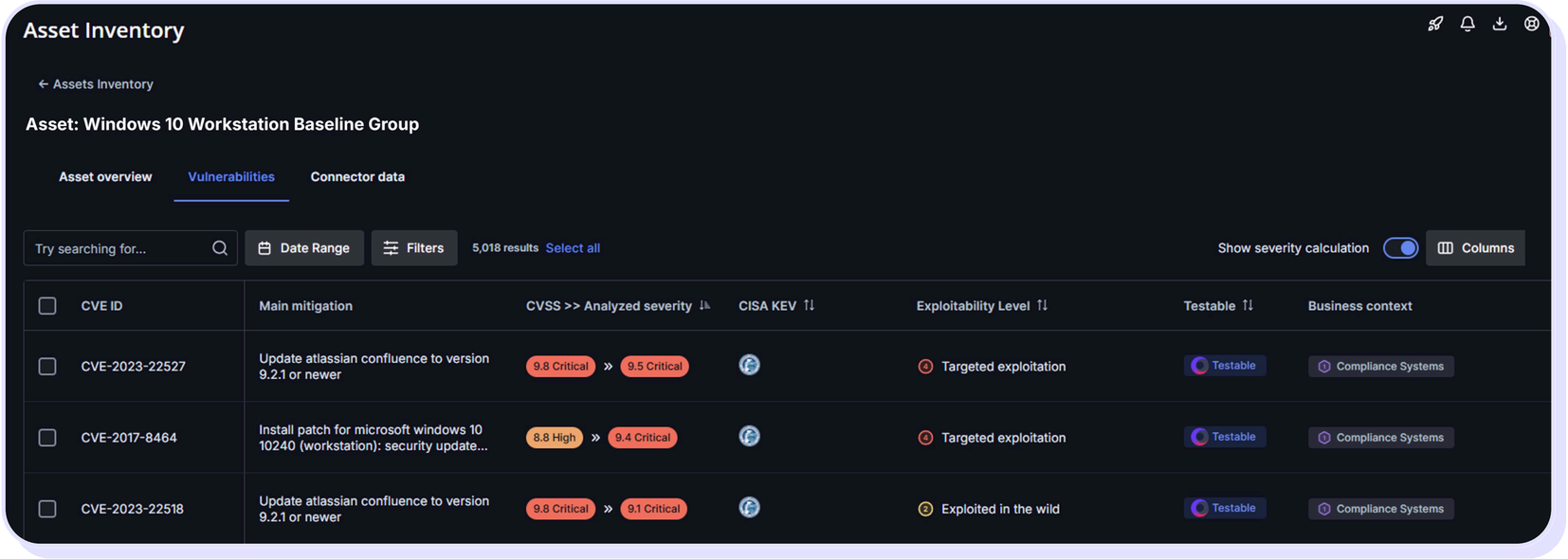
Cymulate **integrates with security technologies** across the architecture to test and validate an organization's existing prevention and detection. These findings are correlated with exposure and vulnerabilities so organizations can mitigate their most critical security gaps, optimize controls and improve threat resilience.

- Endpoint Security (AV / EDR)
- Secure Email Gateway (SEG)
- Network Security (IDS / IPS)
- Cloud Security (CWPP, Cloud IDS)
- Secure Web Gateway (SWG)
- Data Loss Prevention (DLP)
- Kubernetes / Containers (K8S)
- Web App Firewalls (WAF)
- SIEM / SOAR Detections

Consolidated View of Exposures

Validate your real exposures with attack simulation

The Cymulate platform example below highlights how each ingested asset lists the associated vulnerabilities (CVEs), main mitigation, original CVSS score, Cymulate severity risk score, if it is related to a CISA KEV, exploitability level, if it is testable (i.e., can be validated for existing prevention and detection with attack simulation) and associated business context. There are additional columns that can be shown, such as CVE name, number of affected assets and connector source, to name a few.

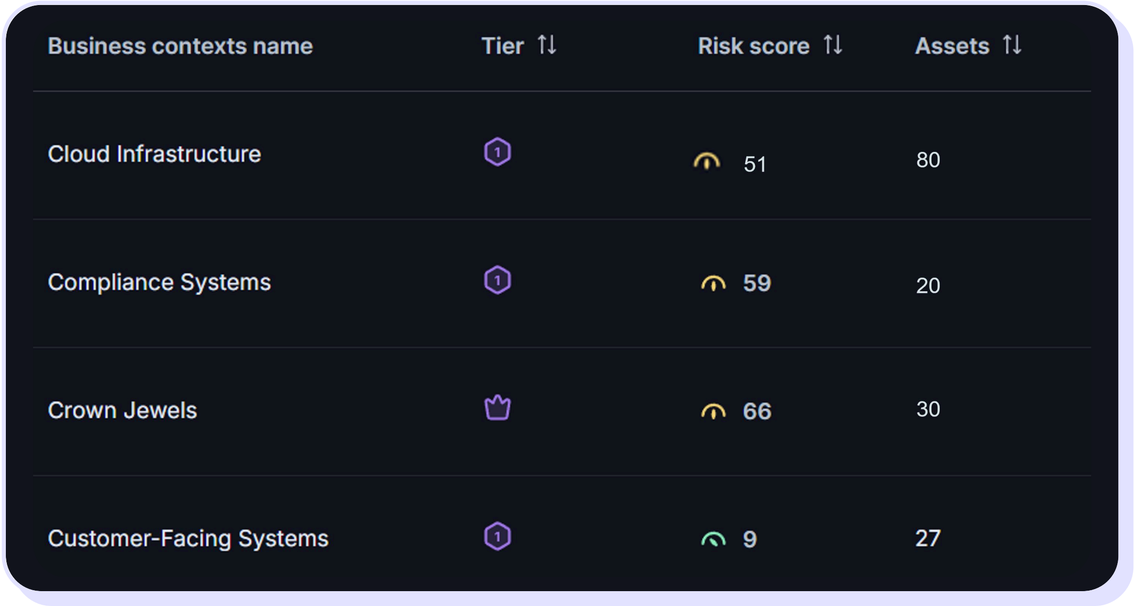


Contextual Asset Vulnerability Dashboard

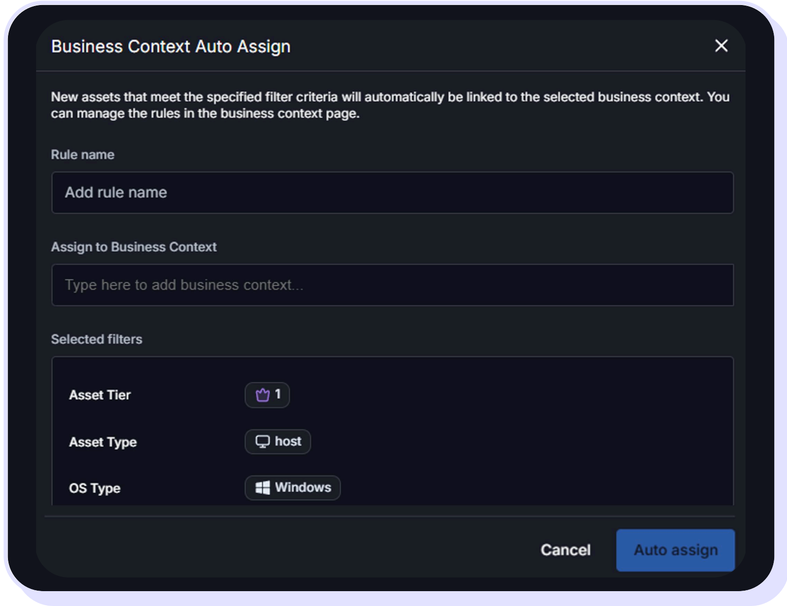
Associating Assets and Exposures to Business Contexts

Associating assets and exposures to business contexts

Cymulate allows all assets to be categorized into the appropriate business context risk level (critical, high, medium and low). This enables the business impact risk level to be factored into the Cymulate severity risk score calculation. Rules can be configured automatically or manually to ensure all assets are categorized accordingly.



Defining Business Contexts

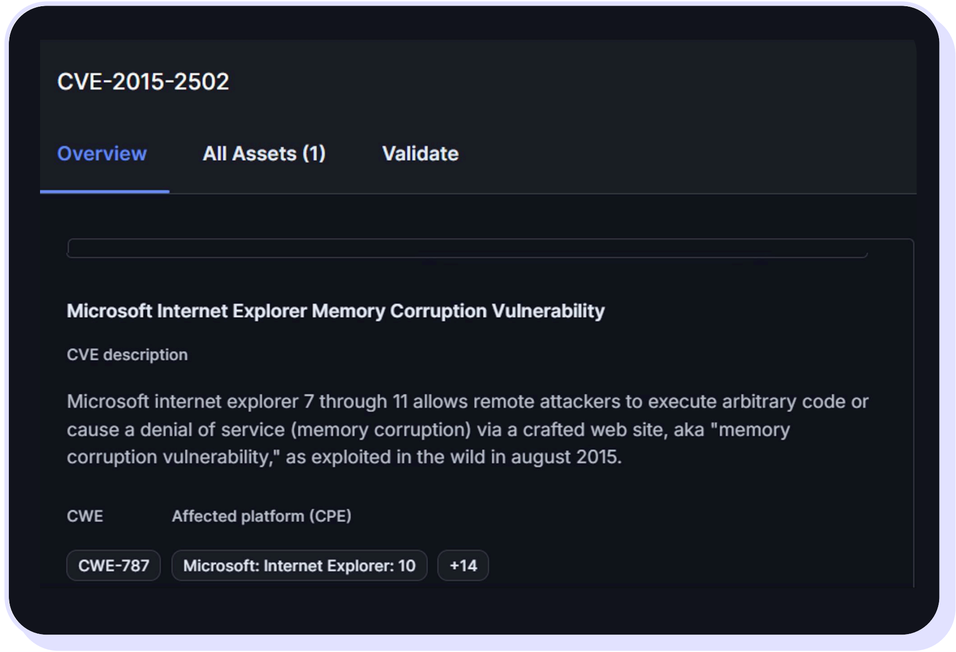


Business Context Auto Assign Rules

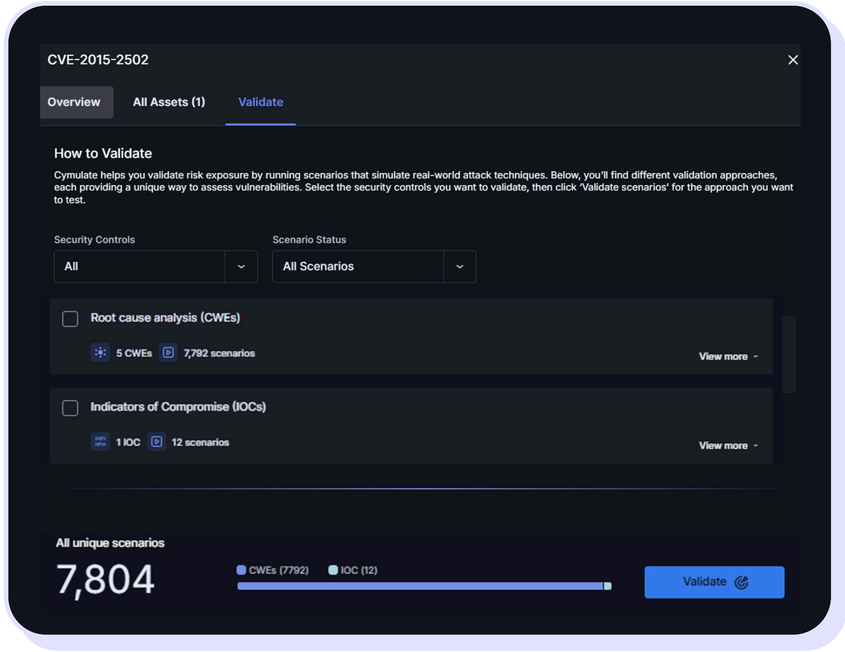
Correlating Vulnerabilities to Attack Scenarios

Cymulate platform automates the correlation

The Cymulate platform automatically correlates and lists all attack scenarios that are associated with each vulnerability. Once these attack scenarios are executed, the existing prevention and detection findings are factored in the severity risk score calculation, which reflects the organization's actual risk, not theoretical risk.



CVE Overview



Attack Scenarios Automatically Correlated to CVE-2015-2502

Cymulate Severity Risk Score Calculation

Know your actual risk with threat validation

Below are the components that are factored into the Cymulate severity risk score, which prioritizes remediating the most critical exposures. Unlike static scoring models, the severity risk factors in the original CVSS score, threat intelligence, security validation results and business impact. This ensures severity reflects not only the technical weakness but also how exploitable it is in your environment.

Original score

The normalized base score taken from CVSS for vulnerabilities or from the Connector for other exposure types.

Threat intelligence

The likelihood for the vulnerability to exploited in the wild or associated with APT groups.

Detection ratio

How well existing security controls detect the vulnerability associated attack scenarios, calculated from automated exposure validation.

Prevention ratio

How well existing security controls block the vulnerability associated attack scenarios, calculated from automated exposure validation.

Asset criticality

Business impact weighting based on the organization defined asset business context risk levels.

Cymulate Severity Risk Score Calculation

From critical to contextual – true operational risk

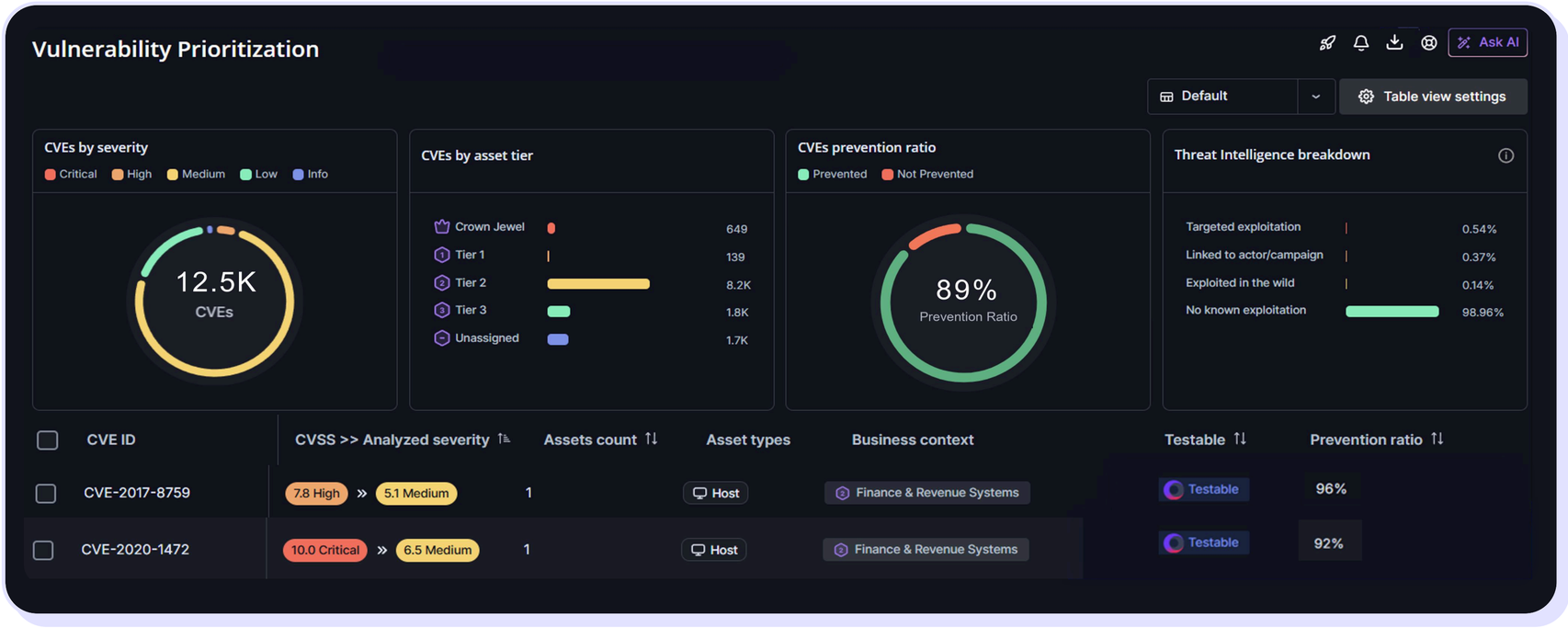
In this example, the CVE was originally rated Critical with a CVSS score of 9.3. After applying the Cymulate contextual severity analysis, which incorporates real-world detection and prevention coverage, threat intelligence insights, and asset criticality, the rating decreased to Medium with a score of 6.6. This new score reflects its true operational risk.

Cymulate CVE Severity Analysis Calculation

Revealing & Prioritizing Vulnerabilities that Matter the Most

Cymulate vulnerability prioritization dashboard

Organizations receive automated and actionable dashboards to view metrics and filter on their most critical vulnerabilities to prioritize effectively. This allows organizations to see which vulnerabilities have been escalated and de-escalated.

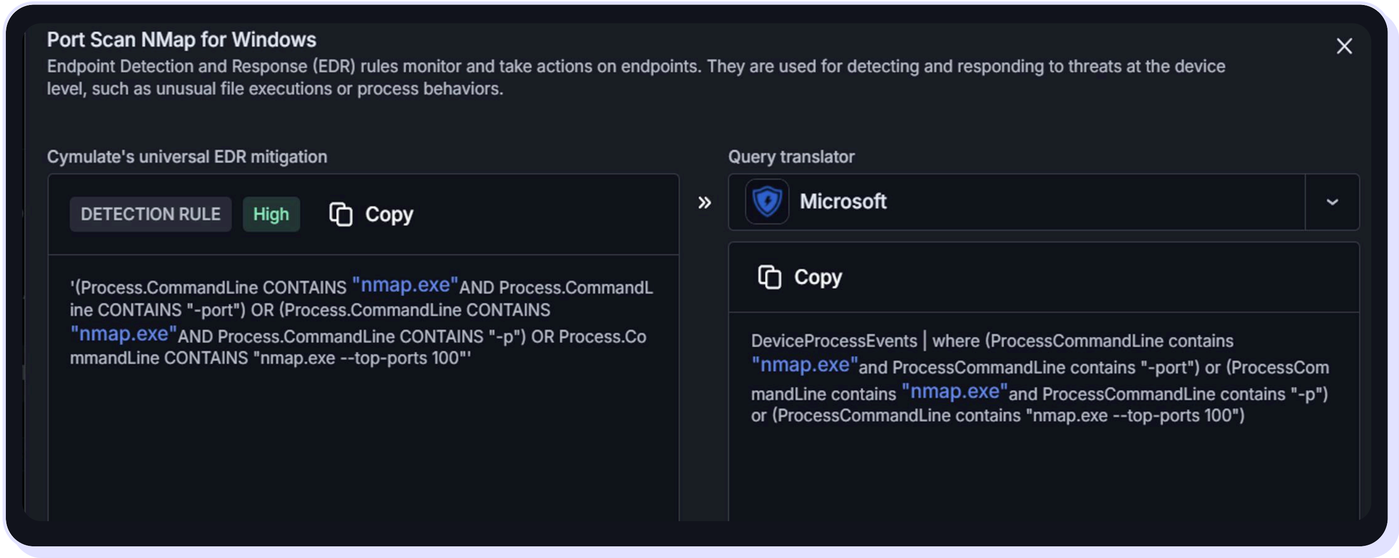


Risk-Based Vulnerability Prioritization Dashboard

Mobilizing with Patching and Remediation

Close the gaps. Improve threat resilience.

The Mobilize phase of the CTEM is all about taking action following the Validate phase. At this stage, organizations implement remediation and mitigation measures to address validated security gaps, prioritizing those that pose the highest risk. Typical actions include deploying patches or updates to eliminate vulnerabilities, enhancing detection rules to improve visibility, adjusting endpoint protection policies, and applying network configuration changes. This could also include accepting the risk, if necessary. The goal is to ensure that every validated finding translates into measurable risk reduction through timely and effective mitigation steps.



Example Auto-generated Vendor Specific Detection Rule

In this example, Cymulate automatically generated the EDR detection rule and formatted to easily add to Microsoft Defender for Endpoint. Adding this new rule will ensure that security scans executed with the nmap security scanning tool are detected.

The Promise of Full-Context CTEM

With a comprehensive CTEM program, organizations and security teams are more efficient and more resilient. Organizations can expect lower remediation costs, fewer security breaches and increased alignment with compliance regulations.

-52%

Fewer Critical Exposures

Decrease in critical and high severity exposure through validated exposure scoring

AVG. of CYMULATE CUSTOMERS

>90%

Threat Prevention

Improvement in threat prevention rate from 70% to 90% for a 20-point increase

AVG. of CYMULATE CUSTOMERS

>50%

Improvement in Detection

Optimize threat detection rate with SIEM rule analysis and recommended detection rules

AVG. of CYMULATE CUSTOMERS

+81%

Improved Threat Resilience

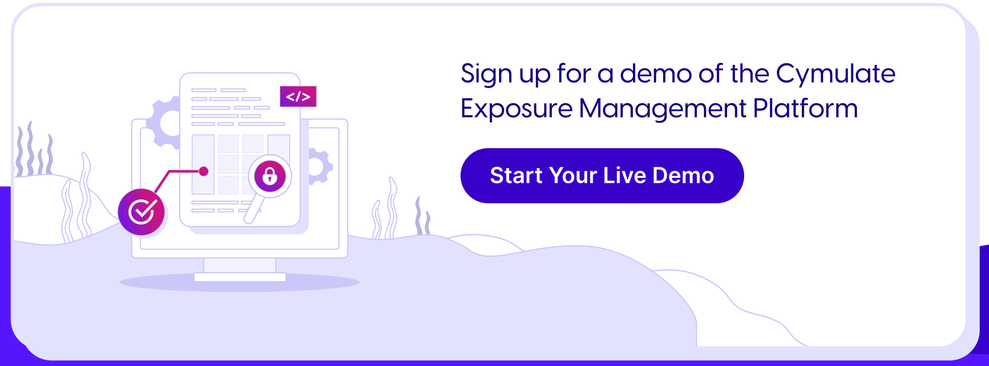
Measurable improvement in cyber risk in 4 months

TRANSPORTATION CASE STUDY

In Summary

Organizations must evolve VM to CTEM

Discover how the Cymulate platform empowers your CTEM journey by helping you identify and prioritize your most critical exposures, optimize the effectiveness of your security controls and continuously improve your overall threat resilience.



Sign up for a demo of the Cymulate Exposure Management Platform

Start Your Live Demo

cymulate

About Cymulate

Cymulate is the leader in exposure management that proves the threat and improves resilience. More than 1,000 customers worldwide rely on the Cymulate platform to prove, prioritize and optimize their threat resilience as they make threat validation a continuous process in their exposure management programs. Cymulate integrates with assessment tools and continuously tests defenses against the full kill chain of attack techniques providing cybersecurity teams with the automation and insights to prove and optimize threat resilience; accelerate detection engineering; drive continuous threat exposure management; and measure and baseline security posture. Prove the threat. Improve resilience. For more information, visit www.cymulate.com.