Mastering CTEM with Hyver's Exposure Assessment and Mitigation

CTEM (Continuous Threat Exposure Management) is a framework that CIOs, CISOs, and security and risk leaders are adopting as a proactive approach to improve security posture and effective remediation, as well as reduce the likelihood of a breach. In fact, **according to Gartner, the promise for organizations prioritizing CTEM investments is that by 2026, they will be three times less likely to experience a breach**. This is one explanation for the overwhelming 75–90% CTEM adoption rate among security leaders.

CTEM is a five-step framework that Gartner defined to enable organizations to identify, prioritize, validate, and remediate security threats in real time, ensuring a continuous cycle of cyber exposure mitigation.

In this guide, we'll break down the five stages of CTEM and explore how Hyver, CYE's exposure management platform, enables security leaders to plan, operationalize, and mature their CTEM programs to better protect their business.

01

Scoping

Defining Critical Assets and Attack Surfaces

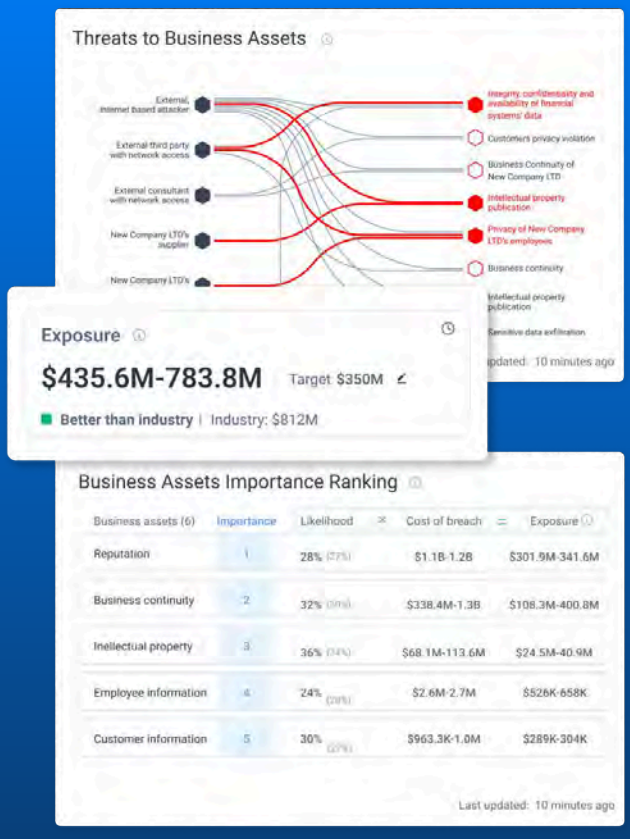
Scoping involves identifying the critical assets, systems, and applications that need protection. It's crucial to define the attack surface, prioritize critical business operations, and align security efforts with organizational goals.

How Hyver Helps

Hyver incorporates accuracy and prioritization in the scoping stage. Utilizing the attack graph, Hyver maps relationships between assets, threats, misconfigurations, and vulnerabilities to visualize an organization's attack surface. Combining the security data with the analytics output allows security leaders to see likely attack vectors from different threat sources to the organizations' business critical assets (BCAs).

With Hyver's executive dashboard, security leaders and executive management can view the financial impact of their organizations' risk. This includes direct and indirect costs of a breach, likelihood of breach, cyber exposure, and cybersecurity maturity according to industry frameworks.

This situational awareness translated into financial impact helps with understanding threat exposure tolerance, defining remediation strategy, and prioritizing mitigation plans with executives and relevant operational teams across the organization.



02

Discovery

Identifying Vulnerabilities and Threats

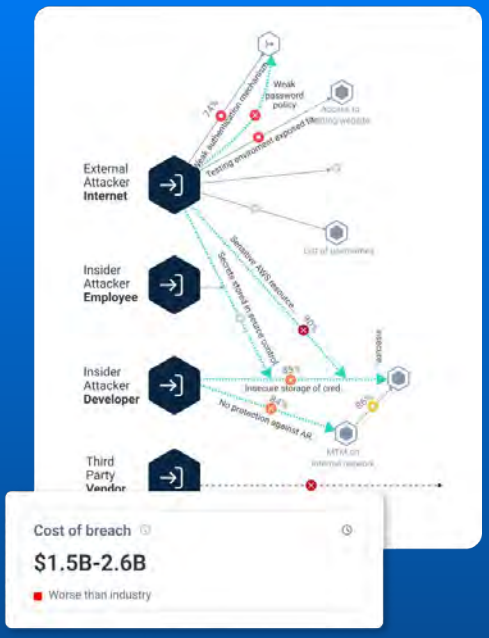
Discovery focuses on continuously monitoring infrastructure for vulnerabilities, misconfigurations, and security gaps across endpoints, networks, cloud environments, and applications.

How Hyver Helps

Hyver continuously updates an organization's attack surface through automated asset discovery, external attack surface scanning, and native integration into cloud environments. Hyver also integrates with organizations' security tools to identify digital and cloud-based assets, vulnerabilities, and misconfigurations. The platform enables uploading third-party organizational assessments to identify additional weaknesses such as missing processes or policies.

In addition, Hyver integrates cyber threat intelligence data from multiple sources. It utilizes the MITRE ATT&CK framework for threat modeling to link TTPs with the organization's identified vulnerabilities and weaknesses and assign the likelihood of exploitability.

Hyver also assigns a risk level and calculates an exposure reduction (monetary) value for discovered findings (vulnerabilities), estimating how much the organization's exposure is reduced when a finding is fixed without relying on other fixed findings.



Hyver integrates cybersecurity maturity into exposure assessment by associating it with findings, security processes, and technology assets, primarily security tools. Maturity is an essential part of Hyver's cost of breach estimation, because it considers the ability of a company to detect, respond, and recover faster from a breach. This directly impacts the overall estimated business loss an organization will suffer from a breach. Hyver utilizes industry frameworks such as NIST CSF, the organization's findings, technologies, processes, and ratings to calculate an organizational maturity score and enable creating mitigation actions to improve maturity and mitigate risk.

Hyver's ingestion of findings and assets from multiple sources ensure continuous updates to threat exposure mitigation actions.

CYE

03

Prioritization

Risk-Based Threat Ranking

Not all threats are created equal. Prioritization ensures that security teams focus on vulnerabilities that pose the highest risk to business operations rather than chase every potential issue.

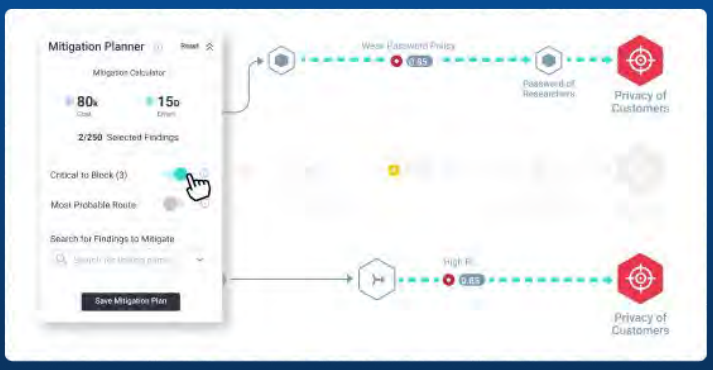
How Hyver Helps

Hyver applies a risk-based scoring model aligned with industry frameworks such as NIST, CVSS, and MITRE ATT&CK to ensure threats are ranked based on business impact reflected in financial terms.

By automating risk prioritization, Hyver helps organizations assess vulnerabilities based on exploitability, asset criticality, and potential business disruption. With predictive analytics, it evaluates the likelihood of exploitation, allowing security teams to focus on the most pressing threats first.

Hyver's unique priority algorithms consider several factors when determining the most critical findings that will reduce cyber exposure. They include a finding's severity based on Hyver's analysis as critical to block, the likelihood that it will be exploited, a monetary value for exposure reduction, the organization's cybersecurity maturity level, and the importance of the business asset to the organization.

Hyver enables teams to create, manage, and prioritize mitigation strategies to help organizations mitigate cybersecurity incidents caused by various cyber threats. Such mitigation plans can be created based on reduced exposure, cost, time to resolve, and/or team effort. This allows security leaders to define optimal mitigation actions tailored to their organizations' risk tolerance and resources.



04

Validation

Testing and Simulating Real-World Attacks

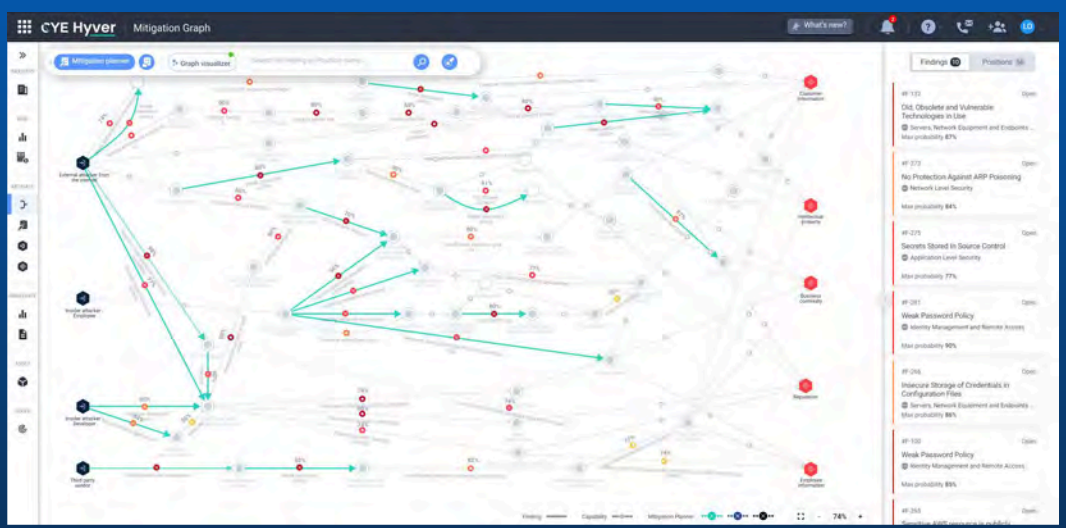
Validation ensures that prioritized threats are actively tested to determine their real impact. Security teams use penetration testing, red teaming, and attack simulations to verify vulnerabilities before remediation.

How Hyver Helps

Security and IT teams can review the prioritized list of vulnerabilities (findings) in Hyver by addressing the highest priority vulnerabilities first.

Security analysts can use both automated tools and manual efforts to research vulnerabilities, verify their associated risks, and accept or reject them based on the results. They can also use the graph visualizer on the attack graph to show how attack routes are affected by fixing specific vulnerabilities. In addition, they can simulate the impact of including or excluding specific findings in the maturity calculations. This helps strategize mitigation efforts to improve maturity.

The outcomes of mitigation actions can be viewed on Hyver's dashboards and mitigation graph. Hyver also offers retest validation services for specific vulnerabilities, as well as full organizational assessments including penetration testing, red teaming, and TXX simulations.



05

Mobilization

Rapid Response and Remediation

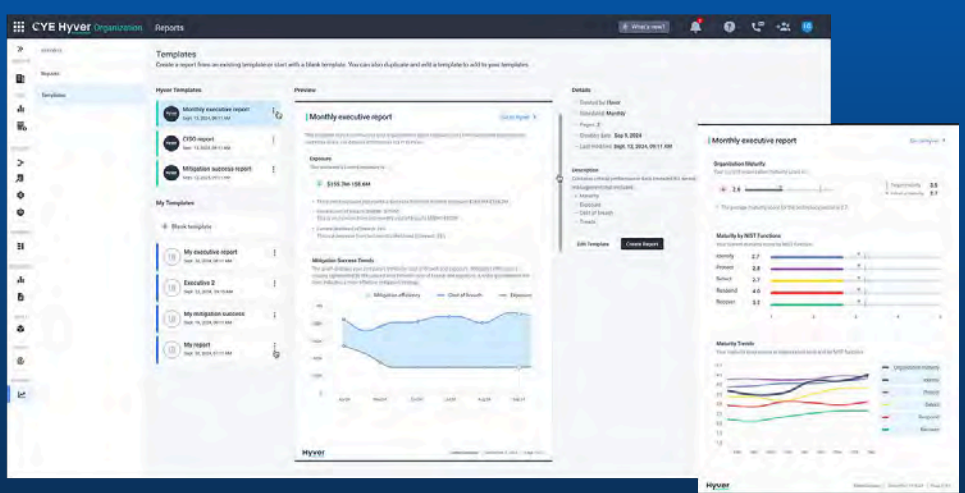
Once security gaps are validated, organizations must quickly respond and remediate them. Mobilization ensures that security and IT teams collaborate effectively to deploy fixes without disrupting business operations.

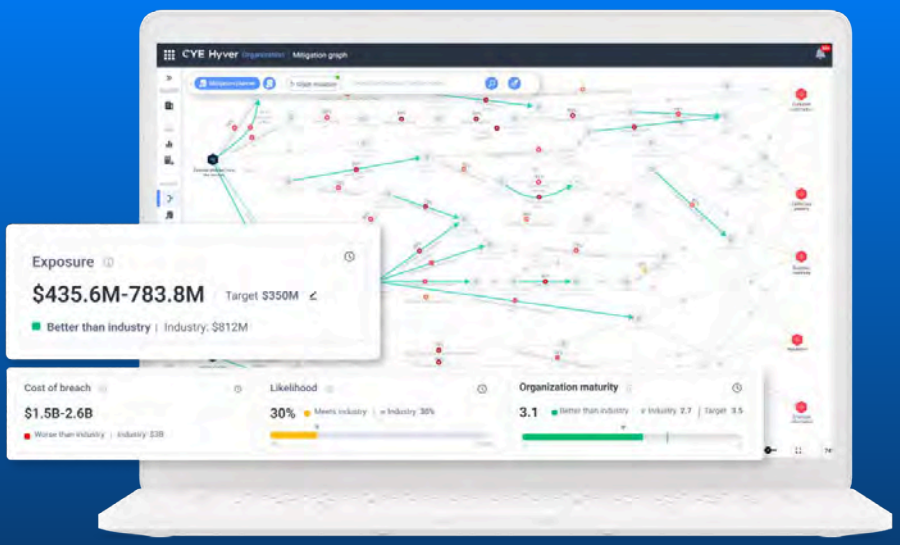
How Hyver Helps

Hyver accelerates response and mitigation plans to reduce organizations' threat exposure. These plans include actions and tasks that are assigned to different teams to address accordingly.

Dashboards feature continuous monitoring and offer visibility into remediation progress, ensuring security teams stay proactive in addressing threats before they escalate. Teams can visualize attack routes in Hyver's mitigation graph before and after applying fixes to vulnerabilities. Moreover, Hyver integrates with ServiceNow and Jira so that teams can operationalize prioritized mitigation plans without disrupting business operations.

Real-time reports are accessible, ensuring that executives and management teams stay informed. These reporting capabilities include templates for board and operational teams, as well as the ability to configure them according to the organization's operations and business processes. Reports can be scheduled and stored on Hyver, allowing easy tracking through all the stages of exposure management.





Want to see Hyver in action?

Schedule a demo today to experience how Hyver can revolutionize your cybersecurity strategy through continuous threat exposure management (CTEM).

Conclusion

In an era when cyber threats are growing more sophisticated, CTEM with Hyver is a transformative solution, redefining exposure management with a data-driven approach. With CRQ at its core, Hyver empowers security teams to gain clarity on their most likely exploited threats, prioritize mitigation actions, and demonstrate cybersecurity's financial impact in monetary terms. As businesses navigate a complex and ever-growing threat landscape, embracing a financial impact-driven remediation strategy is a must, allowing for control in line with risk tolerance.

Trusted by industry leaders around the globe

About CYE

CYE's exposure management platform, Hyver, transforms the way security teams protect their organizations. With CRQ at its core, the platform reveals enterprises' exposure in financial terms, visualizes the most exploitable attack routes to critical business assets, and creates mitigation plans tailored to each business. CYE's customized reporting enables the sharing of vital board-level metrics and validating exposure reduction over time. In addition, CYE improves cybersecurity maturity by mapping weaknesses and defining targets based on industry frameworks. Founded in 2012 in Israel with operations around the world, CYE has served hundreds of organizations across industries globally. Visit us at cyesec.com.

© 2025 CYE, All rights reserved. www.cyesec.com | info@cyesec.com
1000 North West Street, Suite 1410, Wilmington DE 19801, United States
1 Ballards Lane, London N3 1LQ, UK | Abba Eban 10, Herzliya 4615200, Israel