cymulate

Continuous Threat Exposure Management (CTEM)

From theory to practical implementation

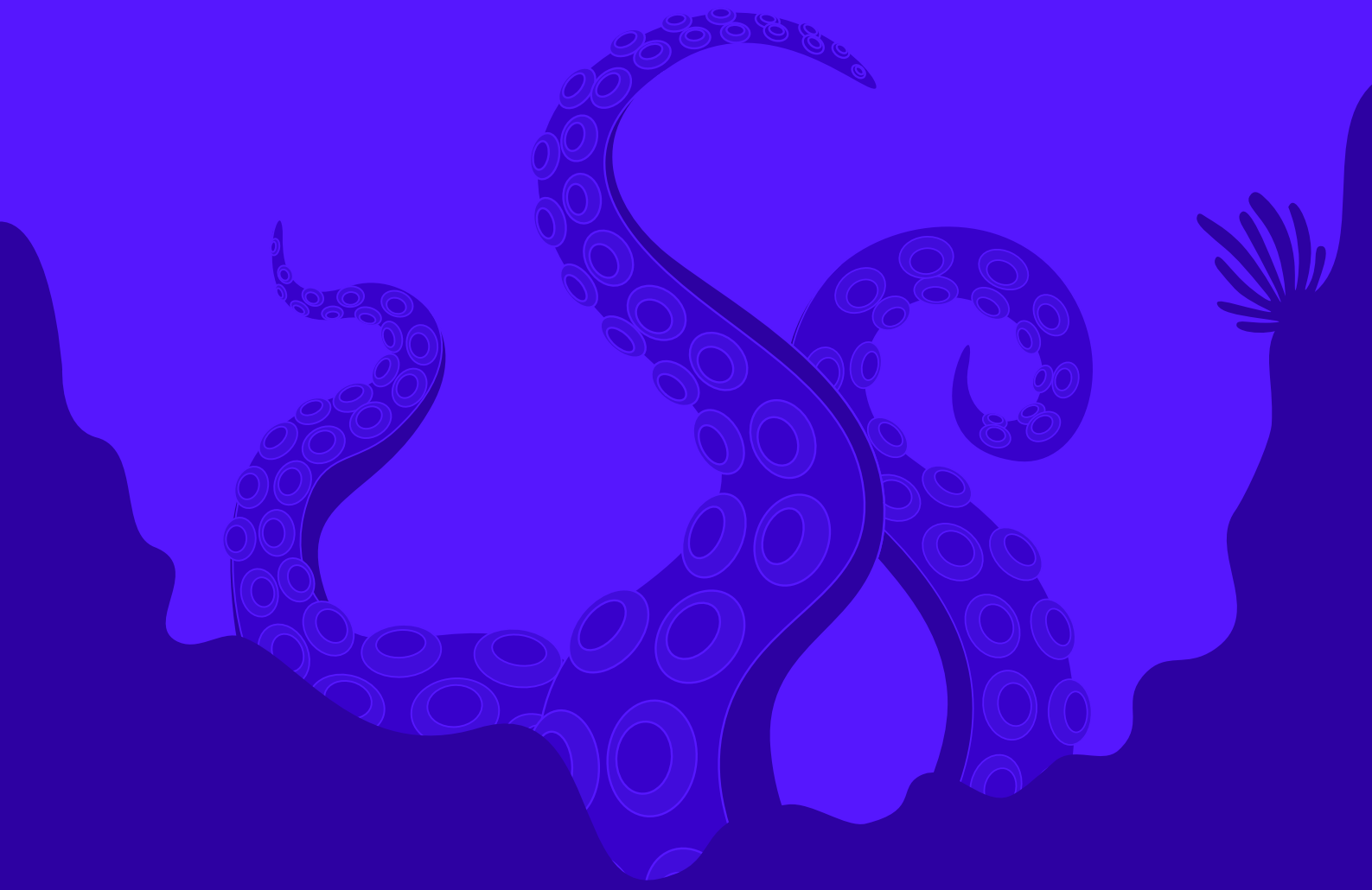


Table of Contents

01
Introduction

As cyber threats continue to increase, security leaders are under growing pressure to clearly communicate cyber risk exposures and improvements to business stakeholders, senior leadership and the board or their authorized committees. However, traditional vulnerability and risk management approaches often fail to provide the visibility and context needed to hold a strategic business conversation about security.

Gartner has created the continuous threat exposure management (CTEM) approach to bridge this gap by recommending a business-focused methodology for managing cyber risk. In order to create a common language for business and technical teams to work from, CTEM provides contextual visibility into threats and security posture and correlates the risks to business values. Leadership can then make data-driven decisions aligned with business objectives.

The cyclical nature of CTEM translates into continuously validating controls and optimizing defenses based on the impact in risk reduction. This builds measurable cyber resilience over time. Automatically generated reports intelligible to business stakeholders are the direct result of the security improvements quantification. These quantified security posture improvements, that include the impact on the reduction of exposure to risk, are key to advise business stakeholders.

This whitepaper guides security leaders through the essential elements of a CTEM program and how to drive measurable results with a pragmatic implementation.

> **Continuous threat exposure management is a pragmatic and effective systemic approach to continuously refine priorities and walk the tightrope between two modern security realities. Organizations can't fix everything, nor can they be completely sure what vulnerability remediation they can safely postpone.**
> Source: How to Manage Cybersecurity Threats, not Episodes (Gartner)

02
What is CTEM?

Continuous threat exposure management (CTEM) is a cyber risk management program that takes a proactive and iterative approach to identify, assess and reduce exposure to cybersecurity risk through ongoing cycles of scoping, discovery, prioritization, validation and mobilization.

Introduced by Garner in July 2022, it puts focus on continuous review to prevent security drift. The repeating cycles correlating technical exposure with business priorities define risk scores. These findings are the base of a remediation schedule prioritized by both technical and business stakeholders' main concerns.

03

Why is CTEM Needed Today?

Despite rising investments in cybersecurity infrastructure, the cost and frequency of breaches steady increase shows no sign of slowing down.

CTEM and exposure management represent a cyber strategy shift toward proactive programs that seek out and mitigate likely threats before they impact the organization. CTEM provides the framework for security leaders to deliver effective controls, fewer incidents and an improved ROI from cybersecurity investments.

CTEM stands apart from purely technical programs like vulnerability management because it adds a business perspective to technical improvements. It addresses communication gaps between business executives and cybersecurity leaders that often result in misaligned priorities. It facilitates holding business-aligned cybersecurity conversations by:

- **Translating technical findings into business insights** – CTEM contextualizes technical data into risk management dashboards and reports tailored for business leaders, in addition to technical reports.
- **Connecting technical data to business risk** – CTEM analyzes exposure to risk based on business criticality and potential impact, not just vulnerability scores.
- **Prioritizing remediation based on business needs** – CTEM aims to identify and rank initiatives by their ability to reduce both organizational risk and impact on essential business functions.
- **Measuring security improvements** – CTEM quantifies reductions in risk exposure over time, providing concrete metrics on security program progress.
- **Aligning resource allocation to business objectives** – CTEM focuses resource allocation to high-impact initiatives closely aligned to strategic business goals and risk appetite.

> Organizations with more proactive and risk-based vulnerability management, such as vulnerability testing, penetration testing or red teaming, experienced lower than average data breach costs compared to organizations that relied solely on the industry standard Common Vulnerabilities and Exposures (CVE) glossary and the Common Vulnerability Scoring System (CVSS).
>
> Generally, proactive risk management efforts involve the organization's IT security team adopting the perspective of a potential attacker to determine which vulnerabilities are exploitable and can cause the most harm.
>
> Source: 2023 IBM Cost of Breach report

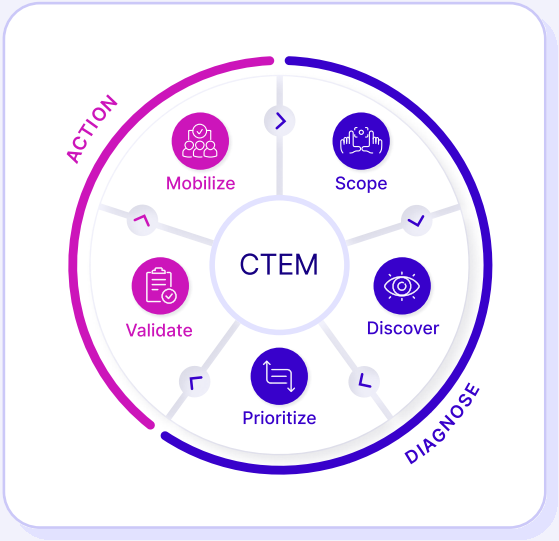
04
Gartner CTEM in Five Steps

Gartner articulates CTEM in five distinct steps belonging to either the diagnosis or the action stage.

The five steps in a CTEM program are not designed to create a one-way process. For example, validation will provide unexpected discovery and must be considered in prioritization.

Where possible, new discoveries should be placed into future cycles, but that is not always an available option – especially if the newly discovered asset is critical to the business context under review in the current cycle. Organizations should feel free to judge each new issue, item, or concern either as part of the current cycle (requiring a step back in the process), or as the basis for a new cycle, as needed.

The diagnosis phases cover the scoping, discovery and prioritization steps. CTEM also includes action stages for validation and mobilization.



In the logic of Gartner's CTEM approach, the first three steps aim at identifying which areas of the business are covered in a CTEM cycle, correlating the insights of the scoping process, and identifying the related assets. These functions are critical in order to understand the system architecture and determine the potential business impact of exploitable security gaps. This knowledge can then be used to devise an action plan prioritized to optimize the defense of the assets and systems in the current cycle.

Step one: scoping

The first step of the CTEM program involves defining what areas of the business will fall within the cycle itself. As any organization is sub-divided into multiple business areas (sales, product/production, accounting, human resources, etc.), it would be unlikely that attempting to perform CTEM on the entire organization at once would lead to successful outcomes. What will fall within an individual scope will differ from organization to organization. Smaller organizations may choose to scope by the function of the division (e.g., sales or accounting) or by infrastructure (e.g., on-prem or cloud). Larger organizations may find it necessary to sub-divide functions further into specific contexts (e.g., sales operations, field sales, contract management, etc.).

Scoping is important because it allows the organization to define what will fall under review during the current cycle, reducing the number of variables involved. It also allows for newly discovered assets to be properly classified as belonging to the current cycle or assigning them to a future cycle.

> **The number of discovered assets and vulnerabilities is not success itself. Accurate scoping based on business risk and ability to remediate is far more valuable.**
>
> Source: Predicts 2023: Enterprises Must Expand from Threat to Exposure Management (Gartner)

Scoping allows for organizations to define the business context that will be under review. This allows for proper classification of assets that may be indirectly related to the current cycle but still pose significant exposure to risk for the current cycle if successfully attacked.

Because of the intertwined nature of the scoping process, both business and technical stakeholders must be active partners in this component of the cycle. Business stakeholders define the context used to set the boundaries of the cycle, while technical stakeholders define the systems and platforms which are believed to be functional components of that context – subject to discovery.

Step two: discovery

The discovery step requires a deep understanding of the systems and assets in the scope of the CTEM current cycle and their risk profiles. In this phase, security teams focus on understanding their attack surface by:

- Identifying assets and systems
- Associating those systems to business and operational needs
- Scanning for vulnerabilities
- Identifying system and control misconfigurations
- Monitoring for security drift (deviation from established security baselines and standards)

Discovery and assessment should be an ongoing process for any security operations team with continuous monitoring. In these cases, technical stakeholders can align the assets and findings with a business context, move the new discoveries into a future cycle if they lie outside of the current context, or add them to the scope if they directly impact the current context.

> **While many discovery processes initially focus on areas of the business that were identified during scoping (Step No. 1), they should proceed to identify visible and hidden assets, vulnerabilities, misconfiguration, and other risks.**
> Source: How to Manage Cybersecurity Threats, Not Episodes (Gartner)

Step three: prioritization

The prioritization step defines the urgency and importance of exposures based on system topology, configuration and criticality correlated with mission/business-critical systems. Rather than relying on statistically defined severity scores alone, the prioritization step should be based on a combination of factors such as severity, exploit prevalence, available controls, mitigation options and business criticality, to reflect potential impact on the scope resilience. Prioritization should include factors such as the potential impact on high-value assets, compensating controls and segmentation, to evaluate the likelihood of exploitation. It should also include shared resources, taking into account that factors from other business contexts may impact the current context as well. The resulting prioritized remediation schedule should focus on tackling the high-impact exposure first.

> **Even a clearly articulated list of prioritized treatments (e.g., patches, signatures, configuration changes) might not be enough to trigger the required collaborative approach to remediating the highlighted issues.**
> Source: Implement a Continuous Threat Exposure Management (CTEM) Program (Gartner)

Step four: validation

The validation step aims to assess the likelihood of attack success, estimate the potential impact, and test the organization's response to identified threat activity against assets in the current cycle.

This often requires a mix of technical assessments such as penetration testing, breach and attack simulation, red teaming, and attack path analysis. Security teams must then connect the output of these technical assessments to business risks, so they can re-convene with business stakeholders to determine whether the exposure risk is legitimate and should be mitigated.

In the context of the CTEM program, this validation phase also shapes and sharpens a plan of action to be taken for both security efficacy and organizational feasibility.

> **The scope of the validation should include not only the relevant threat vectors, but also the possibility of pivot and lateral movement. It should also go beyond security controls testing, and evaluate the efficacy of procedures and processes.**
> Source: Implement a Continuous Threat Exposure Management (CTEM) Program (Gartner)

Step five: mobilization

The mobilization step consists of assigning tasks and allocating resources to enact the remediation plan defined during the validation step. While automated remediation may be desired, it can also lead to failure in reduction of risk or even increasing the exposure to risk of the business context under review.

As any specific remediation action may have several methods that can be applied to form a resolution, determining which path of action is the best fit for each situation is still – at this point – an operation that requires human intervention. For example, applying a patch to a system which may disable a feature critical to a business process will result in business leadership requiring the patch be un-done, leading to more exposure to risk overall. Conversely, strengthening a compensating security control to block access to the vulnerable code without disabling the needed feature will result in success.

The mobilization step aims to facilitate the application of CTEM insights by streamlining approval and implementation procedures, as well as mitigation strategies. Primarily, this is accomplished by having both business and technical stakeholders cooperating on the mobilization efforts. Technical stakeholders define possible remediation strategies and their impact on infrastructure. Business stakeholders review that information and advise the technical stakeholders on feasibility without disruption to the business context itself. This necessitates the establishment of clear communication protocols and formalized cross-team approval processes.

As an organization further evolves in the use of the CTEM process, tools and platforms which can automatically share the necessary information between business and technical stakeholders can allow for more flexibility and greater overall speed.

Successful CTEM programs mobilize teams to implement the prioritized remediation through the culmination of:

- Defining the relevant attack surface
- Confirming exploitability
- Defining possible remediation pathways
- Forecasting potential business impact of exposure risk
- Forecasting potential business context impact of remediation pathways

> **The objective of the 'mobilization' effort is to ensure the teams operationalize the CTEM findings by reducing friction in approval, implementation processes, and mitigation deployments.**
> Source: Implement a Continuous Threat Exposure Management (CTEM) Program (Gartner)

> **To rely entirely on the promise of automated remediation in the program will lead to inevitable failure.**
> Source: Implement a Continuous Threat Exposure Management (CTEM) Program (Gartner)

05
Implementation Challenges

Gartner is correct when defining CTEM as a program and not a technology or market. As with any cybersecurity program, security leaders will face both business and technical challenges when implementing CTEM in their organizations.

Data integration

CTEM relies on aggregating findings from disparate security tools spread across the environment. Manually collecting, correlating and analyzing all this data is highly cumbersome and labor-intensive. Without automated ingestion and normalization, attaining the required centralized visibility remains elusive.

Lack of context

Most security tools provide technical findings without any indication of their business relevance. This makes it challenging to know which vulnerabilities endanger the completion of business priorities and demand expedited remediation. Without insights connecting exposures to business criticality, effective prioritization is unattainable.

Justifying priorities

The proliferation of data from multiple and disparate tools adds complexity to linking the potential impact of identified security gaps to their exploitability and potential business impact. Risk scoring must consider context as well as technical and business factors.

Deciding on the appropriate mitigation

Security automation systems may recommend a single solution when multiple options often exist. There may be more than one "fix" or even no acceptable fix due to business interruption. In such cases, business stakeholders must authorize an exception or exclusion to remediation after carefully weighing exposure to risk, or alternately authorize changes to business processes to remove the exposed system, platform, application, etc.

Driving action

Simply generating data insights is not enough. Without a parallel efficient process to direct the responsible teams to remediate findings based on priorities, this information is of limited value. An integrated workflow that includes ticketing and automation is invaluable to drive action but may not be currently available within the organization.

Measuring progress

Without objective ways to quantify improvements in security posture over time, it is challenging to demonstrate reduced risk exposure and communicate program successes to leadership. This phenomenon is compounded if leadership, the board, etc., are not proficient in the technology under review, requiring translation between technical and business concepts.

Effectively implementing CTEM requires overcoming these challenges. One method for doing so is leveraging the capabilities of platforms like Cymulate, which provide centralized data ingestion, aggregated asset inventory, context-based risk scoring, integrated remediation workflows and progress measurement.

06

From Theoretical CTEM to Practical Implementation

To move from theoretical definition to actual implementation, Cymulate recommends adapting the CTEM approach to fit organizational realities.

Gartner divides CTEM into distinct diagnosis and action stages. In practice, though, those phases often blend together. Once the scope is defined, insights gained during subsequent phases frequently loop back in a way that may not follow Gartner's perfect linear path.

This implementation guide builds off the CTEM methodology to provide guidance on applying CTEM's principles pragmatically toward the ultimate goal of exposure management. While organizations should approach CTEM as a program, technologies such as attack surface management (ASM), breach and attack simulations (BAS), continuous automated red teaming (CART), and exposure analytics are essential elements of an exposure management program.

Scoping

The CTEM process is designed to be cyclical, with the scope refined during each cycle based on insights from the previous iteration. For the initial scoping step, representatives from every potentially impacted department should participate, including operational, finance, legal, R&D, HR and more. Their respective input ensures that assets and processes are evaluated from a cross-functional perspective.

Scoping decisions require balancing business risk, asset criticality and security capabilities. Active involvement of business stakeholders and leadership is key to identifying the highest value business processes, mapping sensitive data flows, pinpointing mission-critical systems and defining risk appetite. This cross-functional collaboration enables implementing a CTEM program tailored to organizational risk priorities and resources.

The scoping step lays the foundation for CTEM's success by establishing value for both business and technical stakeholders. Tight alignment of scoping and mobilization reduces friction, approval and implementation of remediation actions and security improvements.

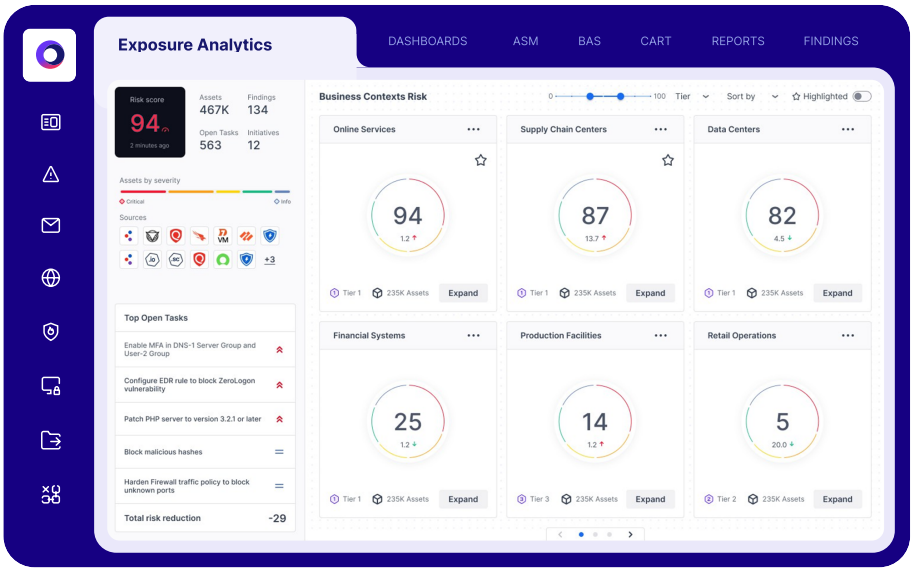
Key takeaways: scoping

- Define critical business and technical processes included in the current focus for exposure management review
- Map high-value business assets, such as services, applications, and data sources, as well as security architecture, trust boundaries and sensitive data flows
- Define risk appetite, priorities and target improvements
- If available, measure and baseline current security posture for assets and systems in the defined scope for the current cycle

The Cymulate advantage: scoping

While scoping will always remain a function of people and processes to align stakeholders, exposure analytics can facilitate collaboration in the scoping phase of an exposure management program. By aggregating data across the infrastructure and security stack and correlating those with custom-defined business values, Cymulate provides security and business leaders with a unified view of security, operational, and business value intricate relationships.

Exposure analytics baselines existing risk and security controls as a starting point for future improvement. With data-driven insights mapped to business priorities, stakeholders can lead informed discussions to determine an appropriate scope that balances critical assets, cyber risk and resource constraints.



The Cymulate dashboard displays exposure scores for defined business contexts.

Discovery

The discovery step entails comprehensively identifying and cataloging all assets, processes, configurations, vulnerabilities and security gaps within the defined CTEM scope. Gartner emphasizes that discovery goes beyond basic asset inventories or vulnerability scans to include misconfigurations of systems and controls and other security gaps.

Even though this might imply including some amount of validation before the validation step, we recommend introducing offensive tools such as attack surface management (ASM) at this stage to identify unmanaged assets (Shadow IT) and other objects that apply to the business context but were not previously known.

ASM tools analyze the environment from an attacker's perspective, cataloging all exposed assets and scanning the attack surface for vulnerabilities and weaknesses. This includes discovery of misconfigurations in Active Directory, multiple cloud platforms and other critical areas of CTEM discovery.

Breach and attack simulation (BAS) also has a role to play in the discovery and identification of exposure risks. BAS tools test security control configuration and effectiveness, testing identity and access policies and entitlements to find security gaps, exploitable vulnerabilities and flawed control configurations.

With data and security finding spread across multiple tools, exposure analytics is then needed to create a holistic view of assets with the intelligence to analyze how each asset impacts the overall exposure to risk of the business context in scope.

Key takeaways: discovery

- Discover internal and external-facing assets, identify vulnerabilities and misconfigurations and map attack paths
- Scan internal and external attack surfaces for vulnerabilities, misconfigurations and security weaknesses
- Audit security controls configuration and runtime effectiveness
- Evaluate identity and access policies and entitlements
- Perform breach and attack simulations to find potential security gaps
- Aggregate and correlate data and findings to create a risk-profiled asset inventory

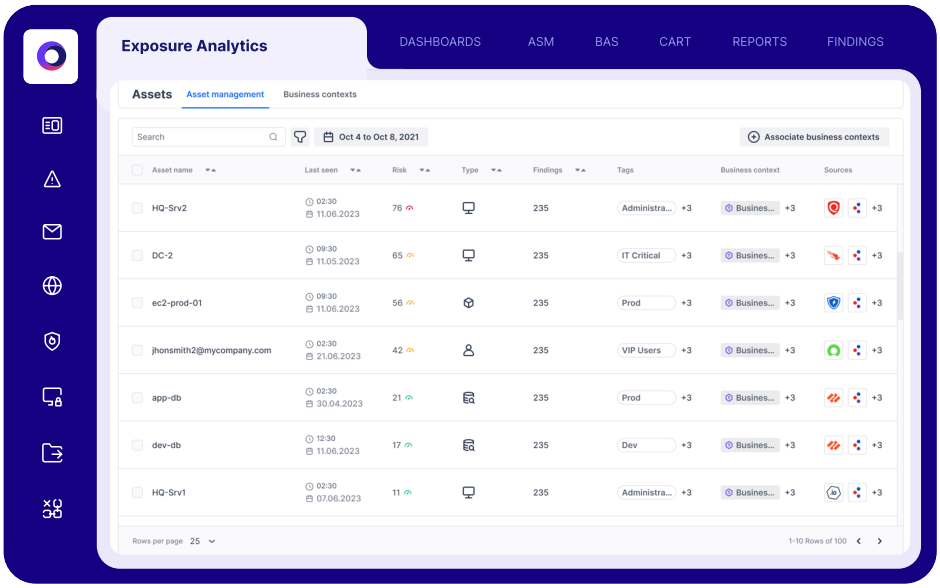
The Cymulate advantage: discovery

The Cymulate platform is unique in providing integrated ASM, BAS, continuous automated red teaming (CART), and exposure analytics capabilities. This combination of functions can provide comprehensive visibility into an organization's threat exposure during CTEM discovery.

ASM covers both internal and external attack surfaces to continuously discover new assets, identify vulnerabilities and misconfigurations, and map attack paths to reveal an organization's exposure and understand the attack surface.

BAS and CART identify control misconfigurations, gaps and weaknesses that can be successfully used in an attack with production-safe assessments that test control efficacy.

Exposure analytics provides a consolidated solution for CTEM discovery by aggregating assets and security findings from both Cymulate and third-party technologies, infrastructure and controls; such as vulnerability scanners, configuration management data bases, cloud providers, endpoint managers, endpoint protection and more. With this holistic view of assets and findings, Cymulate provides a risk-profiled asset inventory and potential exposure risk.



Exposure analytics includes a risk-profiled asset inventory that aggregates assets and their findings from both Cymulate and third-party controls, systems and infrastructures.

Prioritization

The goal of the prioritization step is to focus resources on addressing the most significant threats first. This does not mean less significant risks will be ignored but rather that each potential exposure will be addressed over time, and in their order or priority based on both technical and business factors.

The prioritization step consists of classifying and ranking exposure risks uncovered during discovery according to potential business impact instead of relying only on the criticality score attached to a vulnerability score report, which may not align with their actual in-context exploitability or impact. Cybersecurity vendors offer a few different approaches to enable prioritization. Gartner highlights vulnerability prioritization technology (VPT) as one technical tool to complement Common Vulnerability Scoring System (CVSS) scores with threat intel and other third-party data to provide context such as the active external threats targeting the vulnerability.

> **As part of a CTEM program, not only is the prioritization of risk remediation enabled, but also the rationale for the reduction in priority based on the topology/configuration/criticality of the systems under examination.**
>
> Source: Implement a Continuous Threat Exposure Management (CTEM) Program (Gartner)

However, exposure management is more than just documented Common Vulnerabilities and Exposures (CVEs). CTEM program discovery also includes misconfigurations, control weaknesses and other gaps that require prioritized remediation or mitigation, or may even reduce the priority of the remediation.

Prioritization should also consider the effect of compensating controls and segmentation. However, manually validating attack paths is resource intensive, impractical and likely to yield incomplete and misleading results; yet validation of attack paths is critical to determining true impact in-context. Automated validation of controls, attack paths and full kill-chain scenarios provide essential insights for prioritization. This is an example of where Gartner's CTEM program will not always be a linear progression from one phase to the next.

Findings from penetration tests, control assessments and red teaming are typically classified in the validation phase, but these results refine priorities based on empirical evidence of exploitability and potential impact focuses prioritization. Exposures successfully exploited during validation processes may warrant higher prioritization, while those blocked by compensating controls or effective segmentation can be deprioritized.

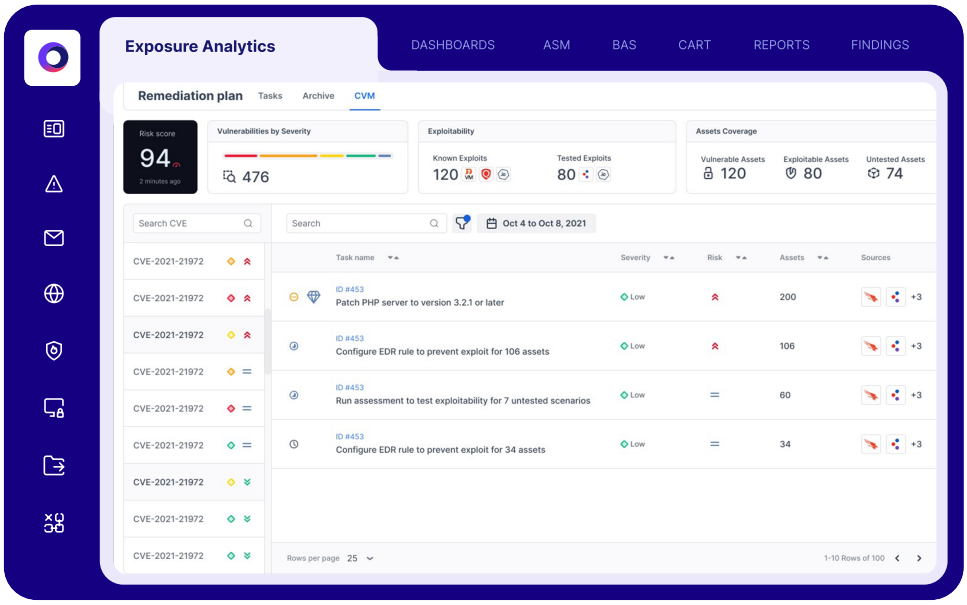
Key takeaways: prioritization

- Perform threat modeling and impact analysis of possible breach scenarios
- Calculate objective risk scores based on exploitability and impact factors
- Correlate exposures to key business assets and processes they could affect
- Consider mitigation options and select remediation that effectively addresses risk with minimal disruption to business operations

The Cymulate advantage: prioritization

ASM, BAS and CART provide contextually weighted risk scores based on exploitation potential validated through attack simulations.

Exposure analytics enhances vulnerability management by integrating data from vulnerability scanners and validation tools to provide exposure visibility and prioritization. Rather than relying on CVSS scores alone, it correlates validated findings with business context to calculate exposure scores for each security gap, taking into account compensating controls, factual exploitability in context and business impact. This validation-informed perspective ensures resources are optimized toward addressing real versus theoretical risks.



Exposure analytics dashboard displays the number of vulnerable assets, the reduced number for exploitable assets and the recommended remediation process

Validation

In practice, the prioritization and validation steps both involve testing and confirming the actual exploitability of identified vulnerabilities and security gaps. When using exposure management tools such as ASM, BAS and CART during the discovery and prioritization step, validation insights are considered in the prioritization step.

Regardless of the chronological inclusion of validation in the CTEM process, the validation stage answers the critical question “how would our defensive controls cope and how would response processes perform?”

By focusing on the actual exploitability of uncovered security gaps, the validation step requires security teams to adopts the attacker’s perspective to validate attack paths and test controls (and compensating controls) for the effectiveness in preventing or responding to threats.

> **Expanding and automating a cybersecurity validation (CyVal) approach via CTEM is key to a successful exposure management program. One approach to starting CyVal is to implement breach and attack simulation (BAS) or automated penetration testing tools, and expand progressively to a workflow of systematically taking the attacker’s view to validate whether an attack would be successful.**
>
> Source: Top Strategic Technology Trends for 2024 (Gartner)

Key takeaways: validation

- Test internal and external assets exploitability
- Assess security controls' efficacy and their ability to reduce the exploitability of uncovered vulnerabilities
- Validate attack paths
- Verify that the prioritization schedule is aligned with the actual security gaps' criticality
- Confirm the business impact of potential remediation strategies

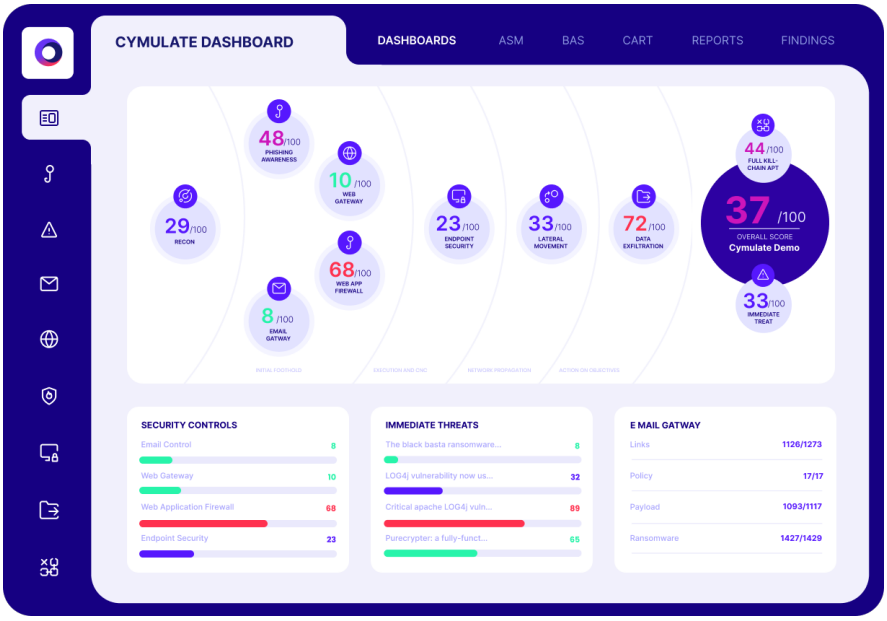
The Cymulate advantage: validation

Cymulate facilitates starting validation during discovery with integrated capabilities from internal and external ASM, BAS and CART tools to empirically validate exposures. The aggregated results of their respective attack simulations provide a comprehensive validation-informed perspective to refine priorities.

BAS thoroughly validates security controls and cyber resilience through extensive scenario libraries mapped to MITRE ATT&CK. With production-safe execution of real-world threats, BAS quantifies exposure criticality, highlights control gaps and delivers actionable remediation guidance. Flexible scheduling enables both on-demand and automated testing to continuously improve defenses.

Complementing BAS, CART provides an automated adversary to validate controls and find weaknesses across the entire cyber kill chain. CART scales testing with production-safe network, endpoint and social engineering attacks. Its flexible framework supports custom scenarios leveraging MITRE ATT&CK. Repeatable CART assessments efficiently confirm remediation of issues over time.

With BAS and CART, Cymulate automation allows frequent and comprehensive assessments to continuously improve defenses throughout the CTEM cycle.



Mobilization

The mobilization step covers orchestrating and driving risk reduction through people, process, and technology improvements based on validated priorities. Gartner emphasizes mobilization should not be limited to technical security changes but also include securing budget and resources to execute mitigations and tracking progress and contributions to risk reduction.

> When a diagnostic tool also suggests a 'fix,' it might not necessarily be the best one for the organization, or it might not be acceptable for business leaders. There is no way for a tool or a security process to guess what will be adequate for other teams.
>
> Source: Implement a Continuous Threat Exposure Management (CTEM) Program (Gartner)

> Through 2026, unpatchable attack surfaces will grow from less than 10% to more than half of the enterprise's total exposure, reducing the impact of automated remediation practices.
>
> Source: Predicts 2023: Enterprises Must Expand from Threat to Exposure Management Research (Gartner)

Cooperation between technical and business stakeholders can put plans in action and remove roadblocks. Those plans include budget allocation, business processes modifications and pre-approved downtime for systems updates and upgrades. This step can be time and labor intensive, depending on the extent of the exposures discovered, processes requiring modification and the level of technology or expertise that must be acquired. At the conclusion of mobilization and mitigation, an exposure management program should measure its exposure risk with metrics that align with business priorities and demonstrate security resilience.

Key takeaways: mobilization

- Secure budget and resources to execute mitigations and update policies, procedures and training
- Eliminate unnecessary data, apps, technologies, privileges and access
- Patch prioritized vulnerabilities
- Add new controls and capabilities where needed
- Improve monitoring and response proficiency
- Enhance architecture designs and compensating controls

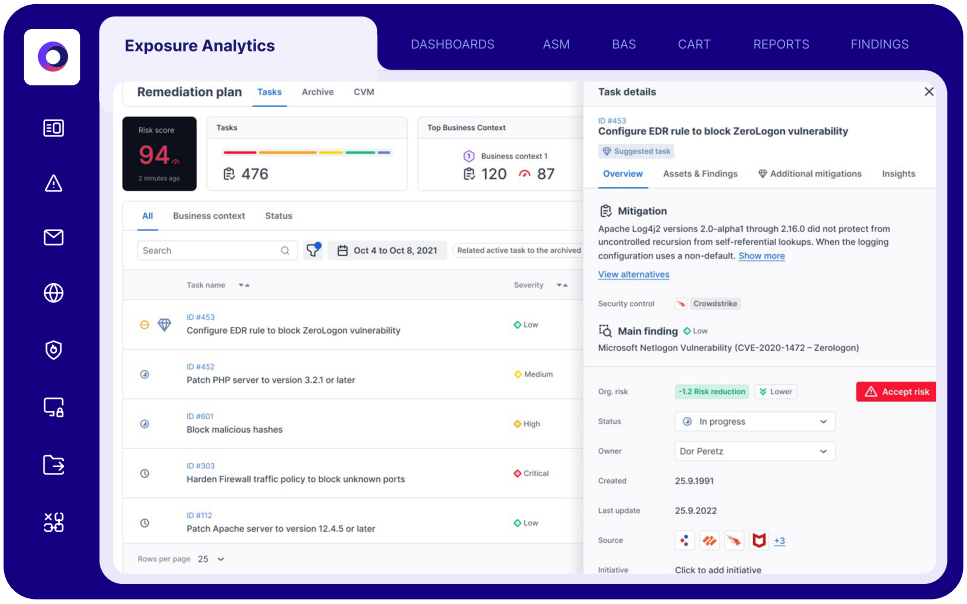
The Cymulate advantage: mobilization

Exposure analytics leverages its risk scoring and asset inventory to generate prioritized remediation plans that maximize risk reduction. The plans factor in urgency, severity, compensating controls and business impact to recommend the most impactful mitigations.

When possible, exposure analytics forecasts risk outcomes by modeling the effect of potential remediations.

Integrated ticketing streamlines mitigation management and drives accountability, while customizable dashboards provide unified visibility into posture risks and trends to communicate progress. Together, this allows for efficiently translating CTEM insights into continuous improvements.

Cymulate provides security posture baselines that security leaders use to communicate exposure risk and cyber resilience to executives and boards. Additionally, exposure analytics provides a unified view of ongoing efforts to lower and control exposure to risk, validating the mobilization process as changes go into effect.



Cymulate provides a remediation plan that includes remediation options, forecasted improvement to risk and connection to the context of business risk.

07

CTEM Benefits

Security and business leaders that successfully implement CTEM increase the maturity and effectiveness of their cyber programs with technical, business and operational benefits that combine into reduced exposure risk and improved security posture. Here are five ways CTEM enables organizations to move from primarily reactive to primarily proactive security, continuously improving defenses in alignment with business needs:

Business alignment

CTEM translates technical findings into business insights, enabling data-driven decisions aligned to business objectives and improved communication between security and executive teams.

Continuous validation

Ongoing CTEM activities like breach simulations and red team exercises validate security controls and posture continuously versus point-in-time audits.

Efficiency at scale

Automating CTEM steps like discovery, validation and data correlation allows assessments at higher frequency and comprehensiveness while efficiently scaling across the environment.

Actionable insights

CTEM not only reveals gaps and weaknesses but also provides clear prioritized guidance and integrated workflows to accelerate remediation.

Measurable resilience

CTEM metrics and trend reports provide tangible visibility into reduced risk exposure, creating objective measures of security posture improvements over time.

Consolidated visibility

Rather than introducing more siloed tools, platforms which integrate multiple CTEM processes streamline and connect workflows across capabilities for greater efficiency.

08

How Cymulate Contributes to CTEM Implementation

The table below summarizes how the Cymulate platform maps to CTEM methodology:

CTEM	Cymulate Technology	Scoping
Scoping	Exposure analytics	Measure and baseline cyber resilience and exposure risk for specific business contexts, providing insights that assist security leaders define program scope with focus and measurable goals.
	ASM	Discover assets. Identify vulnerabilities and misconfigurations. Map attack paths. Monitor dark web to find stolen or leaked information, such as compromised passwords, credentials, intellectual property, or other sensitive data.
Discovery	BAS	Identify control weaknesses with assessments that test control effectiveness.
	Exposure analytics	Aggregate discovered assets from multiple sources including ASM, endpoint security, configuration management databases, and the cloud and IT infrastructure. Profile the risk of each asset based on the security findings reported across security controls. Extract data about the coverage of security controls for each asset, including the specific policies applied for each asset by each control.

CTEM	Cymulate Technology	Scoping
Prioritization	ASM, BAS, CART	Vulnerability prioritization, security control optimization, and remediation planning are based on individual ASM, BAS, or CART findings and remediation recommendations.
	Exposure analytics	Contextualized vulnerability prioritization correlates vulnerability findings (of multi-vendor aggregated data) with business context and security control effectiveness.
Validation	BAS	Validate control effectiveness and security posture to determine the likelihood of attack success, estimate potential impact and measure response capabilities.
	CART	Automate testing for vulnerability validation, what-if scenario, targeted and custom-testing within a flexible framework for repeatable and scalable testing.
Mobilization	Exposure analytics	Analyze data to understand various program or response outcome options and establish baselines that track performance and risk profiles. Remediation plans connect mitigation options with technical findings and context of business risk.

09
Conclusion

The transition to threat exposure management is in full swing, reflecting both compliance regulation updates and recommendations from think tanks ranging from Gartner to the World Economic Forum. This proactive approach to cybersecurity recognizes that security teams need more than just new list of priorities. CTEM provides a framework that differs from traditional security operations because it adds scoping for business context and validation to understand if (and how) existing security controls mitigate the threat – all part of a continuous process. The Cymulate Exposure Management Platform brings this together with best-in-class automated security validation and an open platform to work vulnerability scanners, cloud security, security controls and IT infrastructure.