Implement a Continuous Threat Exposure Management (CTEM) Program

Published 21 July 2022 - ID G00763954 - 21 min read

By Jeremy D'Hoinne, Pete Shoard, **and 1 more**

Enterprises fail at reducing their exposure to threats through self-assessment of risks because of unrealistic, siloed and tool-centric approaches. Security and risk management leaders must initiate and mature a continuous threat exposure management program to stay ahead of threats.

Overview

Key Findings

- Zero-day vulnerabilities are rarely the primary cause of a breach. The most successful protection approach combines preparation for unknown threats with a risk reduction strategy, emphasizing publicly known vulnerabilities and identified control gaps.
- Technology-centric attack surfaces and vulnerability self-assessment projects generate rarely-actioned reports and long lists of generic remediations. Vulnerability management programs rarely keep up with the aggregate volume of their own organization, leading to quickly expanding attack surfaces.
- Testing attack feasibility with security posture validation initiatives improves score-based prioritization. However, prioritized lists alone are rarely enough to mobilize nonsecurity teams and remediate the issues due to insufficient business context and accountability considerations.
- Maintaining a dynamic and current security posture over time is a key challenge when tackling exposure management programmes. The key to a mature programme is a strong workflow through smarter — not full — automation nor remediation.

Recommendations

As a security and risk management leader responsible for security operations, you should:

- Ensure that exposure management outputs contribute to multiple parts of the security and IT organizations by designing a programme for managing a wider set of exposures, rather than simply inventorying and processing telemetry from multiple disparate vulnerability assessment tools.
- Establish regular repeatable cycles as part of your continuous threat exposure management programme, with each cycle adhering to a five steps process — scoping, discovery, prioritization, validation and mobilization — thus guaranteeing consistent threat exposure management outcomes.
- Tackle threat exposure using emerging areas like attack surface management and security posture validation. When growing in maturity, start including assets that the organization has less control over, such as SaaS applications, data held by supply chain partners and suppliers' own dependencies.
- Integrate continuous threat exposure management (CTEM) with organizational-level remediation and incident workflows that go beyond security-specific automated technical fixes to ensure that the required cross-team collaboration becomes standard.

Strategic Planning Assumption

By 2026, organizations prioritizing their security investments based on a continuous exposure management programme will be three times less likely to suffer from a breach.

Introduction

This document was revised on 26 July 2022. The document you are viewing is the corrected version. For more information, see the Corrections *page on gartner.com.*

Every organization owns some kind of vulnerability management program, ranging from ad hoc, emergency patches to more comprehensive asset and vulnerability inventory. Traditional approaches are no longer keeping up with quickly evolving business needs and expanding attack surfaces. Exposure extends beyond vulnerabilities. Even taking a risk-based vulnerability management (RBVM) approach might not be sufficient. Fixing every known vulnerability has always been operationally infeasible, and odds have worsened as digital transformation has accelerated the expansion of the attack surface.

As organizations update their IT and security programs to follow the evolution of work practices, they now have to manage a growing attack surface due to their technological environments becoming increasingly complex and dispersed, both on-premises and in the cloud. New technologies and business initiatives(such as SaaS applications), new ways to generate revenue, operational technology (OT), Internet of Things (IoT), cyber physical systems (CPS) and supply chain touchpoints pose new threats.

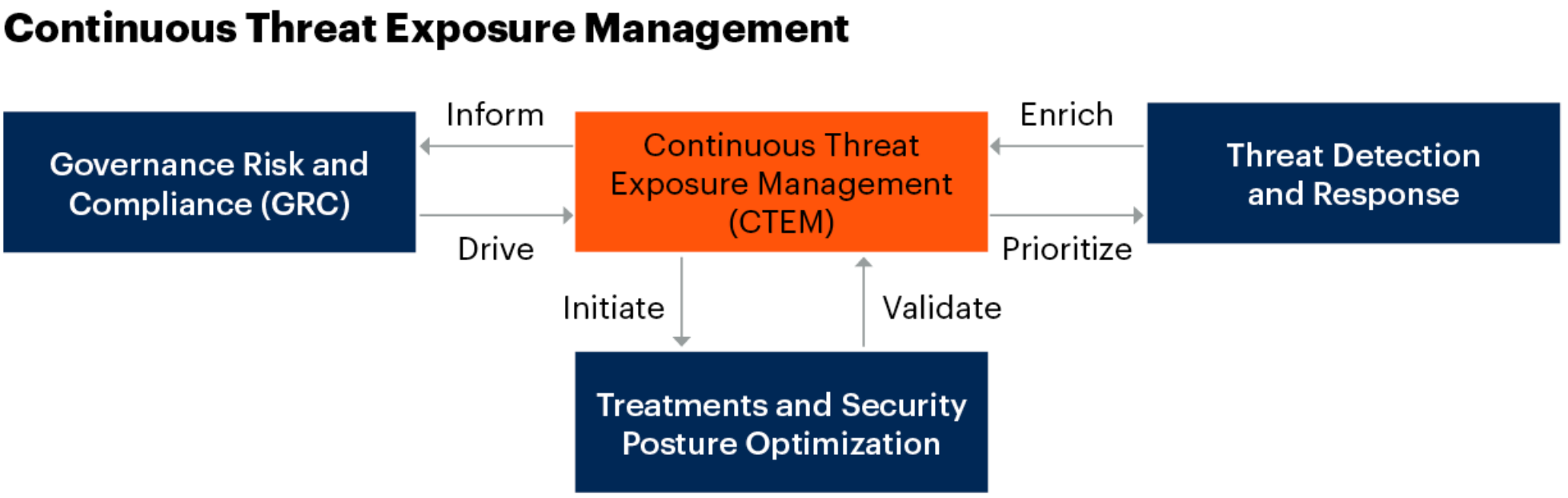
Security leaders always look for improved frameworks and tools for reducing their cybersecurity risks. This includes a shift from a preventative-only approach to more mature, strategy-augmenting-preventative controls with detection and response capabilities. Previous approaches to managing the attack surface are no longer keeping up with digital velocity — in an age where organizations can't fix everything, nor can they be completely sure what vulnerability remediation can be safely postponed. CTEM is a pragmatic and effective systemic approach to continuously refine priorities, walking the tightrope between those two impossible extremes (see Figure 1).

A continuous threat exposure management (CTEM) programme is an integrated, iterative approach to prioritizing potential treatments and continually refining security posture improvements.

The objective of CTEM is to get a consistent, actionable security posture remediation and improvement plan that business executives can understand and architecture teams can act upon. Unsustainable promises of machine learning, enabling fully automated incident response and attack containment, often creating a business accountability challenge. It is important to recognize that business risk appetite informs the selection of remediation for cybersecurity issues through a combination of fixes and mitigative controls. Splitting "treatments and posture improvements" from the exposure management program acknowledges these challenges but also emphasizes the cross-team requirements for efficient posture improvements (see "CTEM and Security Posture Optimization" below).

Similarly, a CTEM program operates with a specific time horizon. It follows the governance, risk and compliance (GRC) mandates and can inform shifts in the long-term strategy, but is free of some of the real-time constraints imposed in the threat detection and responses activities of the security operations center (SOC) team.

Figure 1: Continuous Threat Exposure Management



Source: Gartner
763954_C

Gartner

Description

Gartner observes that even the larger and more mature organizations are ready to evolve their existing vulnerability management program, but lack a structured workflow and only implement some of the steps described in this research. To start, a revised set of objectives and a new workflow are necessary.

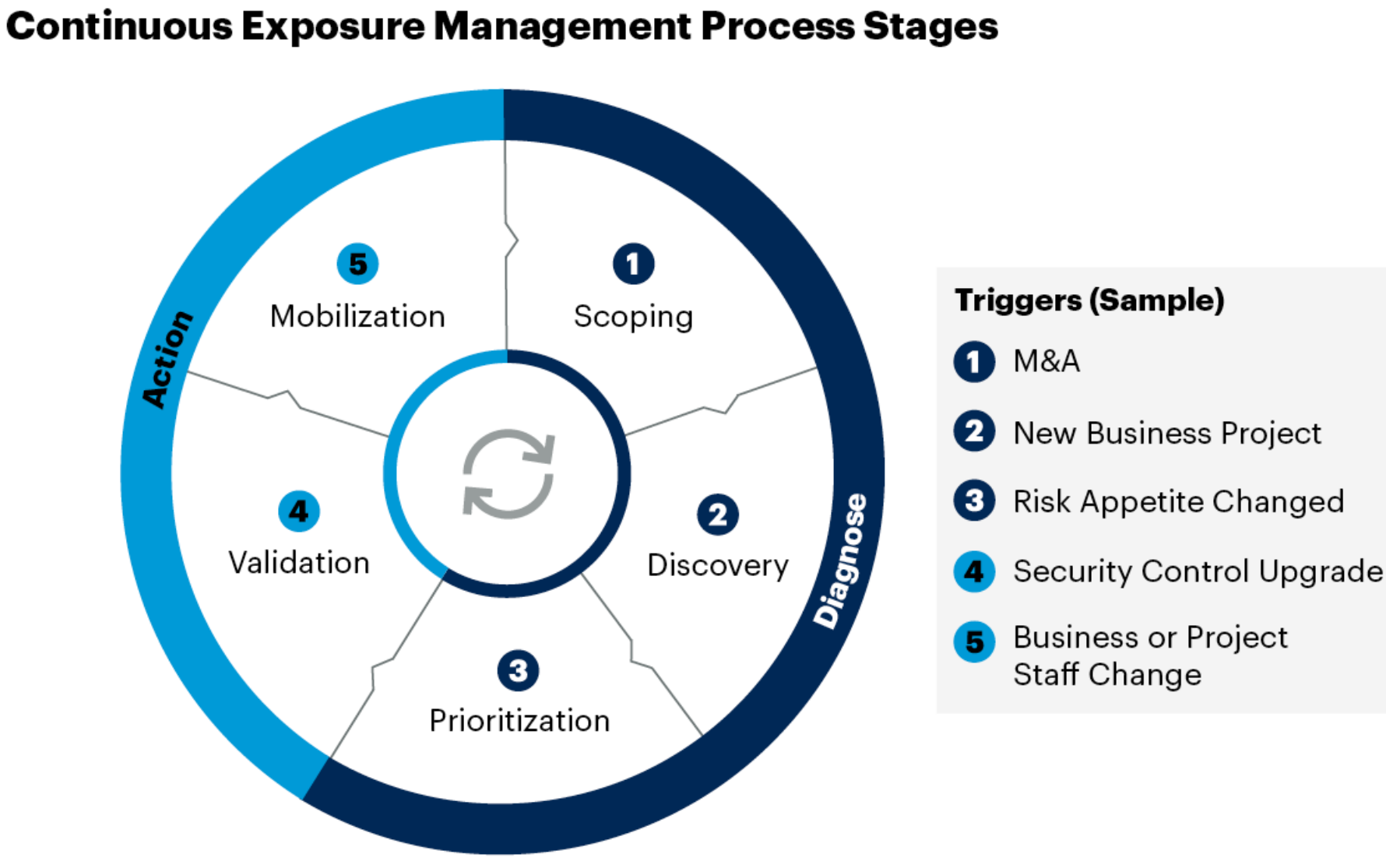
Objective of a CTEM Program

Continuous Threat Exposure Management (CTEM) programme is a set of processes and capabilities that allow enterprises to continually and consistently evaluate the accessibility, exposure and exploitability of an enterprise's digital and physical assets.

At any stage of maturity, a CTEM cycle must include five steps to be completed: scoping, discovery, prioritization, validation and mobilization (see Figure 2). Organizations building a CTEM program use tools to inventory and categorize assets and vulnerabilities, simulate or test attack scenarios and other forms of posture assessment processes and technologies. It is important that a CTEM program has an effective and actionable path for infrastructure teams, system and project owners to take action on findings (covered in the section below: Exposure is More Than Just Posture).

CTEM is cyclical. External factors, such as new business initiatives, organizational changes or newsworthy attack techniques might trigger CTEM processes, but not necessarily starting with the first step of the cycle (see Figure 2). In addition to vulnerability prioritization and remediation, organizations are able to get tremendous value in learning both the positive and negative lessons from going through the CTEM stages.

Figure 2: Continuous Exposure Management Process Stages



Source: Gartner
763954_C

A CTEM program should be the first step in identification and planning for resolution. It requires cross-team collaboration and federation of responsibilities and accountability, particularly where the assessment, tracking, management and remediation of exposure is shared between the participants in the process. For example, security operations can be in charge of assessing, tracking and managing exposure, while infrastructure and operations teams and enterprise architecture functions are responsible for acting on it. One of the main benefits of running a CTEM program is the more structured and repeatable workflow.

Remediation is rarely as simple as suggested, and security leaders need first to mobilize everyone and ascertain if the resolution of an issue might be responsible for creating other friction or issues with operational business functions (aka "cure is worse than the disease"). This is why the CTEM program is necessary. It enables treatments and security posture optimization that go beyond the traditional patching, signatures and playbook outcomes, and are also capable of maturing independently from the CTEM program.

CTEM Is Not a Tool, It's a Program

In their effort to build a multifunction platform, security leaders should not get trapped into the vendor's platform narrative, replacing the necessity to address all the assigned objectives of a CTEM program, with their approach of building a multifunction platform.

The virtue of a multifunction platform spanning across multiple components of the framework exists, but the purpose of the platform might influence its design. An attack surface dashboard, from an attack simulation or penetration testing platform, will aim at quickly pivoting to the testing component. The same dashboard from a vulnerability prioritization technology (VPT), external attack surface management (EASM) or digital risk protection service (DRPS) product will focus on setting up priorities for remediation.

Organizations in the process of starting their cybersecurity mesh architecture (CSMA) journey will recognize a shared philosophy. As the CTEM program matures, it becomes a key source for the security intelligence layer of the CSMA design (for more on CSMA, see How to Start Building a Cybersecurity Mesh Architecture).

A CTEM program might exploit results from automated assessment technologies but it is important to reiterate that piling up assessment reports or simply buying a consolidated platform promising to "do it all" will be insufficient. Security operation history teaches us that relying solely on tools creates inevitable diagnostic fatigue and lacks business context for relevant prioritization or successful remediation.

CTEM might suggest "treatments," such as technical mitigations, but "remediation" implies that the suggested course of action must also pass through the standard processes for risk acceptance, as well as operational viability.

The convergence of several of these CTEM markets, driven by the providers' appetite for new customer revenue and the fear of providers to see their product become a feature, might add to the initial confusion. Security leaders can avoid this trap by evaluating individual components as if they deployed them as a stand-alone product, then evaluate the value of the platform integration separately.

The Five Steps of the CTEM Cycle

A CTEM program, although repeatable, is governed by five core stages. Each of these stages performs a different function for the benefit of the entire program, each is also required to repeat during every iteration.

The importance of a CTEM program, when compared to previous functions, such as vulnerability management (VM), is that it considers the "why" and "how" elements of what is discovered. Importantly, the scoping exercise, before a discovery exercise, is designed to keep the focus on what is important to the business. CTEM is not a purely risk-driven exercise either. Transforming a traditionally diagnostic function into an actionable set of outcomes requires clarity regarding objectives.

Scoping

For large organizations, the scope of the attack surface exceeds the typical focus of vulnerability management programs and needs to evolve to encompass an extended set of assets — from traditional devices, apps and applications, to less tangible elements (such as corporate social media accounts, online code repositories and integrated supply chain systems). An effective way to address this is to identify an initial scope, which should include a plan to prove value to stakeholders and later expand as the program progresses.

To define and later refine the scope of the CTEM initiative, security teams need first to understand what is important to their business counterparts, and what impacts (such as a required interruption of a production system) are likely to be severe enough to warrant collaborative remedial effort.

More developed vulnerability management projects generally include good initial scoping for internal, on-premises and owned assets. A CTEM program goes beyond self-inflicted vulnerabilities and also takes the "attacker's view," beyond the traditional common vulnerabilities and exposures "(CVEs)" (see also Using Security Testing to Grow and Evolve Your Security Operations). When trying to find the right scoping for a CTEM program pilot, good candidates include:

- **External attack surface** — It combines a relatively narrow scope (for most organizations) and a growing ecosystem of tools.
- **SaaS security posture** — While tool maturity is still lacking, increasing remote workforce led to more critical business data hosted on SaaS, ensuring easier communication about the risks.

Later cycles could expand to include:

- **Digital risk protection** which adds greater visibility into the attack surface.
- **Dark and deep web sources** to identify potential threats to critical assets and provide contextual information on threat actors and the tactics and processes utilized to conduct malicious activity.

Discovery

Once scoping is completed, it is important to begin a process of discovering assets and their risk profiles. Priority should be given to discovery in areas of the business that have been identified by the scoping process, although this isn't always the driver.

Exposure discovery goes beyond vulnerabilities: it can include misconfiguration of assets and security controls, but also other weaknesses such as counterfeit assets or bad responses to a phishing test.

> **Confusion between scoping and discovery is often the first failure when building a CTEM program. The realization that the number of discovered assets and vulnerabilities is not success itself, accurate scoping based on business risk and potential impact is far more valuable.**

As many discovery processes go beyond the initially stated scope — to identify visible and hidden assets, vulnerabilities, misconfiguration and other risks — the burden shifts to the "prioritization" step, where additional "noise cutting" is necessary.

Prioritization

The goal of exposure management is not to try to remediate every issue identified nor the most zero-day threats, for example, but rather to identify and address the threats most likely to be exploited against the organization.

Organizations cannot handle the traditional ways of prioritizing exposures via predefined base severity scores, because they need to account for exploit prevalence, available controls, mitigation options and business criticality to reflect the potential impact onto the organization. More mature organizations should apply the lessons learned from conducting and expanding their vulnerability management program.

Prioritizing the treatment of exposures needs to be based on a combination of the urgency, severity, availability of compensating controls, risk appetite and level of risk posed to the organization. In other words, organizations should determine their high-value assets (where critical business value is located) depending on whether there are existing security controls in place and the likelihood of the asset being exploited by an adversary, and then focus treatment efforts where appropriate.

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. This clearly articulates the organization's approach to address the mission-/business-critical systems as a priority, but to also react to unusual or exceptional events, such as zero-days and/or critical vulnerabilities requiring immediate response, and to demonstrate improvement.

> **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.**

This is why the validation and mobilization steps of CTEM are key to success.

Validation

In a security program context, "validation" is the part of the process by which an organization can validate how potential attackers can actually exploit an identified exposure, and how monitoring and control systems might react. Validation generally uses controlled simulation or emulation of attackers' techniques in production environments. While not limited to attackers' techniques, the "validation step" often relies on manual assessment activities, such as red team exercises, to extend its reach. In a CTEM context, it also includes the verification of the suggested treatments, not only for security efficacy, but also for organizational feasibility.

The validation step should achieve three objectives:

- Assess the likely "attack success" by confirming that attackers could really exploit the previously discovered and prioritized exposures.
- Estimate the "highest potential impact" by pivoting beyond the initial footprint and analyzing all potential attack paths to a critical business asset.
- Identify if the processes to respond and remediate the identified issues can be both fast enough and adequate for the business.

A good validation process needs to overcome a few challenges. It requires a mix of technical assessments (e.g., pentesting, red teaming, breach and attack simulation and attack path analysis), but also organizational acceptance. Each organization needs to determine the minimum level of accuracy that will convince all business stakeholders to remediate. This will influence the tool selection and the required procedures.

Then, 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.

Mobilization

To ensure success, security leaders must acknowledge and communicate to all stakeholders that remediation cannot be fully automated. Many mature organizations have hit the limits of so-called "automated remediation" as technical treatments are very often limited to patching, a basic threat detection rule or a configuration change in a security control. Fully automated reaction, recommended by a tool, might be appropriate for the most obvious and unobtrusive issues. This can be an acceptable first step but is rarely where security teams struggle.

To rely entirely on the promise of automated remediation in the program will lead to inevitable failure, because consequences of any attempt to remediate falls beyond the sole responsibility of the security teams:

- There is more than one "fix" (runtime control, patch)
- There is no acceptable "fix" (business interruption)

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 acceptable for other teams.

Mobilization: the act of organizing or preparing something, such as a group of people, for a purpose [1]

Security tools that might be involved in a CTEM program would almost always suggest only one solution where there may be many. Choosing between these suggested solutions is only predicated on a portion of the available information. 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. It requires organizations to define communication standards (information requirements) and documented cross-team approval workflows. It also requires having business leaders on board and involved (see Cyber-Risk Appetite: How to Put the 'Business' in 'Managing Cybersecurity as a Business Decision').

At higher maturity, "mobilization" also requires an evolution of the tools to better integrate together so that they can deliver context to other parts of the organizations, such as the incident response team.

Benefits and Uses

A CTEM program is one part of a comprehensive set of security and risk management programs, aligned with different time horizons and objectives:

- **Survive breaches —** Detecting and responding to attacks requires near-real-time action capabilities. This is the responsibility of security operations teams focused on defensive approaches ("blue team") and is outside of the scope of CTEM, but can be enriched by the knowledge gained from a CTEM program.
- **Minimize risks —** This rarely happens in real time. Business constraints might prevent the implementation of a "quick fix," and for most organizations, there are simply too many pending issues. That's why the CTEM program helps prioritize risk reduction actions and optimize resource usage.
- **Improve resilience —** Requires long-term investments and design thinking that might take years to implement. The CTEM program might better inform the overall strategy.

CTEM and Security Posture Optimization

In its most basic form, the mobilization phase of a CTEM program triggers the consequent treatment and optimization processes as simply a ticket in an IT service management tool. This is initiated with the intention of implementing a remedy to an issue through a technical control, such as a protection signature ("virtual patch"), or request for a system patch. The various tools supporting CTEM will often suggest these basic remediations.

But to be robust, security posture optimization needs to:

1. Integrate lessons from the CTEM program to drive the efficiency of the suggested treatments.
2. Support multiple scenarios, including when remediation is neither easy nor automatable.

The “Mobilize” steps from a CTEM program ends with the approval of required changes, the commitment of necessary resources and an agreed timeline. The optimization of the security posture starts with the integration of these remediations into the planning to meet these timelines.

Risks

Exposure Is More Than Just the Posture (of Your Assets)

Traditionally, security posture refers to what organizations can control and more easily improve. It also sounds more active and drives excessive hunger from vendors and leadership. But it doesn’t mean it is easy, especially when the maturity of security controls is not high enough yet.

With the adoption of cloud services teams, security and infrastructure teams now have to monitor an extended number of settings and configurations that, if done incorrectly, may expose sensitive data and services. Therefore the process of managing your posture involves the correct combination of analyzing your attack surface, identifying high-risk vulnerabilities and validating your visibility and responses in relation to things that are important to the business.

The total exposure goes beyond that and also includes what is outside of direct control, such as supply chain risks from partners storing the organization’s data in their environment (see Table 1). Running a CTEM cycle creates the opportunity to incorporate the learning from each of the steps in the design of future product releases.

Table 1: Persistent and Transitory Exposure Outside of an Organization’s Direct Control

Persistent ↓	*Transitory* ↓
▪ Select the most business-relevant controls ▪ Implement and configure controls ▪ Patch and maintain vulnerabilities	▪ Identify and mitigate identity compromise ▪ Identify and reduce data exposure ▪ Identify and mitigate risks in third-party SaaS applications

Source: Gartner

Changing processes, removing/hiding visible data and removing persistent exposures by correcting misconfiguration, patching vulnerabilities and adding controls reduces the attack surface to the transitory exposure, which can then be better addressed.

Adoption Rate

Organizations often start addressing threat exposure by expanding their existing vulnerability management initiatives by:

- Using a tool-centric approach
- Adding findings from external attack surface management (EASM) and breach and attack simulation (BAS) products
- Focusing on actions belonging to the “discovery” and “prioritization” steps, in a useful, but relatively unstructured approach

As organizations want to mature their CTEM program they also need to improve on its weakest components, which are frequently the “Prioritization” and “Mobilization” steps.

Figure 3 below shows how the maturity of individual steps might differ and evolve at different speeds. As always, “quick wins” help the security teams to raise awareness about the program itself and are important. However, unbalanced progress might drastically limit the benefit of the program, especially when the “Mobilization” step spends a long time in establishment.

Figure 3: High-Level Maturity Model for a CTEM Program

High-Level Maturity Model for a CTEM Program

	Establishing	Advanced	Optimized
Scope	All business assets	High-Risk Business Functions	Business-Risk Driven
Discover	Fixed Asset List	Vulnerability Assessment	Composed Risk Discovery
Prioritize	Tool Scoring	Framework Aligned	Outcome-Driven
Validate	Passive Diagnostics	Red Teaming	Purple Team
Mobilize	(Virtual) Patch Prioritization	Remediation Framework	Secure-By-Design

Source: Gartner
763954_C

Gartner

Alternatives

Organizations can approach exposure management in a less structured way, by taking actions on each of the three pillars, based on more fragmented projects (see Figure 4). Well-conducted projects will help improve the security posture of the organization. However, insufficient coordination and siloed objectives increase the likelihood of “dashboard fatigue.”

Figure 4: Market View of Exposure Management

Components of Exposure Management

Exposure		
Attack Surface	**Vulnerability**	**Validation**
Internal	Prioritization	Targeted
External	Classification	Comprehensive
Digital Risks	Awareness	Compliance

Source: Gartner
763954_C

Gartner

Depending on the organization’s size and SOC process maturity, they might starts at various level of maturity for each of the pillars below:

- **Attack surface management** — "What does my organization look like from an attacker's point of view, and how should it find and prioritize the issues attackers will see first?" (see Innovation Insight for Attack Surface Management).

- **Vulnerability assessment** — "What software is present and what configuration has my organization set that will make it vulnerable to attack?"

- **Posture validation** — "What would happen if an attacker carried out a campaign against my organization's infrastructure, how would its defenses cope and how would processes perform?" The validation pillar addresses this question by leveraging breach and attack simulation and automated penetration testing tools.

Recommendations

- Design a program for managing a wider set of exposures that are likely to affect business priorities, rather than simply inventorying and processing vulnerabilities.
- Ensure that exposure management outputs contribute to multiple parts of the security organization, offering insights for secure-by-design programs, enrichment for security incidents and response efficacy.
- Tackle threat exposure with emerging areas like attack-surface management and security posture validation to complement existing vulnerability management programs.
- Take a phased approach to deploying technologies to support a CTEM program, starting with technology familiarization and expanding into risk gap analysis.
- Integrate CTEM with organizational-level remediation and incident workflows that go beyond security-specific automated technical fixes, and require cross-team collaboration as standard.
- When growing in maturity, start including in the CTEM program: assets that the organization has less control over, SaaS applications, data held by supply chain partners and suppliers' own dependencies.

Representative Providers

Sample markets that contribute to a CTEM program:

- External attack surface management (EASM)
- Cyber asset attack surface management (CAASM)
- Digital risk protection service (DRPS)
- Vulnerability Assessment (VA)
- Vulnerability prioritization technology (VPT)
- Breach and attack simulation (BAS)
- Penetration and testing as a service (PTaaS)
- Automated pentesting and red teaming

Evidence

Gartner inquiries covering VM, BAS, Pentest, MTD

[1] Mobilization, Cambridge Dictionary.