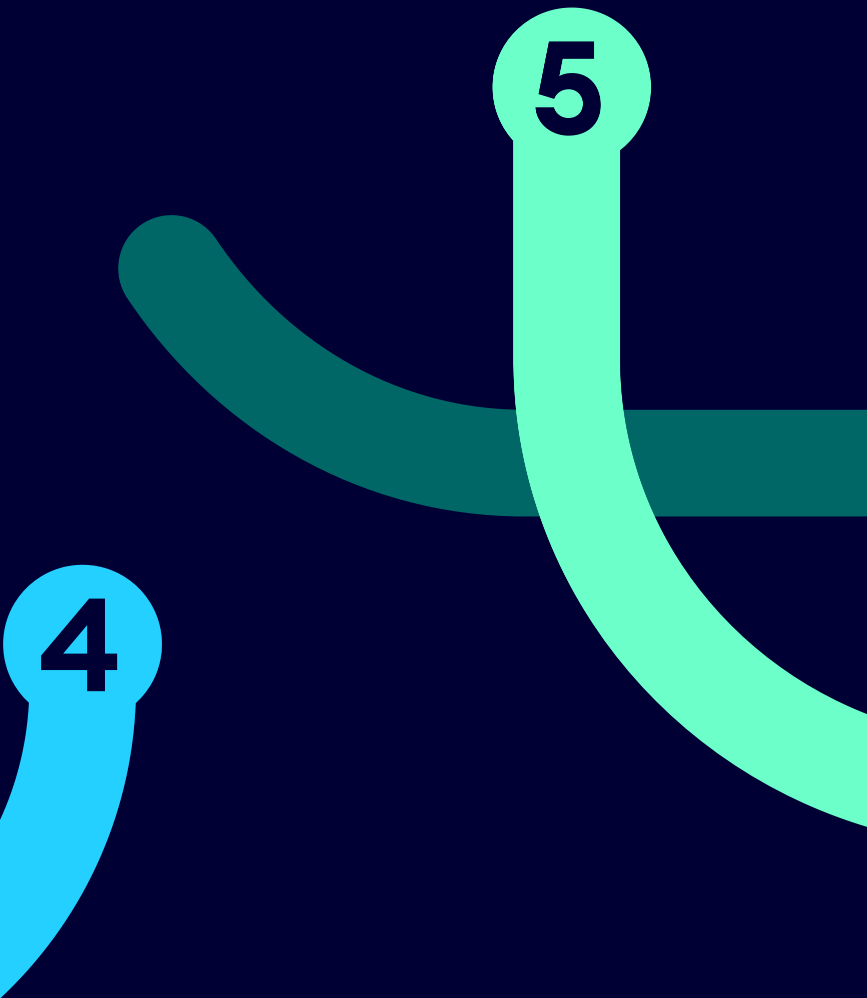
XM Cyber

Whitepaper

A Practical Guide to Getting Started With CTEM



If you spend your working time in the vulnerability and exposure management space, chances are you've heard about The Gartner Continuous Threat Exposure Management framework (CTEM). This new way of addressing the full scope of issues that can affect an organization's security posture is being adopted by organizations looking to better close the gap between the never ending tide of CVEs, misconfigurations, identity-based issues and Active Directory issues – i.e., cyber exposures – and address them in the most efficient manner to reduce the risk of cyberattack.

But why is there a need for yet another approach to managing vulnerabilities and exposures, what are the goals of the CTEM framework, what are some challenges you may need to overcome and how can you construct a comprehensive program of your own? In this paper, we'll explore all of these issues as well as many others, to give you everything you need to get started with building your own CTEM program, if you haven't done so already.

In the Beginning (of Vulnerability Management)...

Addressing the many types of issues organizations face each day is like trying to piece together an intricate, complex patchwork; there are multiple layers and facets, some of which stretch to provide adequate coverage, and some of which over time, begin to fall short. While vulnerability management has been a mainstay of this construct for years, as attackers have changed their attack strategies, and attack surfaces grow and become more complex, the shortcomings of this approach become more apparent.

Problems with Legacy Vulnerability Management Tools

Modern vulnerability management tools can identify vulnerabilities, i.e., issues that are assigned CVSS scores. Vulnerability management programs integrate a variety of security tools, such as vulnerability scanners, threat intelligence, and remediation workflows, to provide a more efficient and effective solution to protect against security risks. But as mentioned above, CVEs only cover a small slice of the issues that put organizations at risk – they fail to include the misconfigs, identity issues and Active Directory issues, i.e., exposures, that we see regularly exploited in attacks.

So even with all of these advancements, organizations still face numerous challenges when it comes to managing the full scope of issues that actually put them at risk and are thus still unable to answer these all-important questions:

Do we know what needs to be fixed first?

Can we actually validate that the fixes are needed to reduce risk?

Can we get the fixes we need?

Can we do this all on a continual basis?

To better answer those questions, CTEM provides a new framework.

What is Continuous Threat Exposure Management Framework by Gartner?

According to the Gartner report, "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."

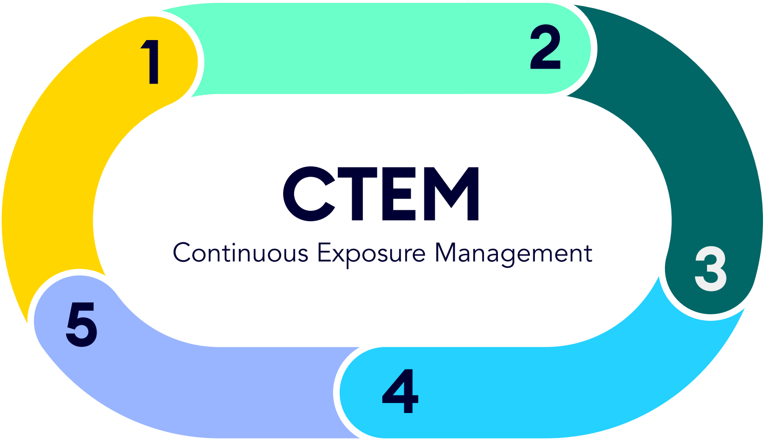
According to the Gartner® report, Implement a Continuous Threat Exposure Management (CTEM) Program, (Gartner, 21 July 2022,) "Technology-centric attack surfaces and vulnerability self-assessment projects generate rarely-actioned reports and long lists of generic remediations. Vulnerability management programs rarely keep up with the aggregate volume of their own organization, leading to quickly expanding attack surfaces". A bit later on it states: "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."

One of the biggest challenges in security today is that teams often aren't even aware of the threats they are up against. They throw efforts in multiple directions, frequently without seeing tangible results.

A comprehensive CTEM program can help you continually see your attack surface and improve security posture by identifying and remediating potentially problematic areas. This ability to see exposures and their potential to be leveraged is a key element in gaining the attacker's point of view.

The 5 Stages of CTEM

So now let's have a look at the 5 stages of CTEM according to Gartner. All of the stages are required for the program to function as intended, so don't try leaving any out, no matter how tedious or insignificant a step may seem.



1 Scoping

According to Gartner, “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.” The report further notes that, “More developed vulnerability management projects generally include good initial scoping for internal, on-premises and owned assets.”

4 Validation

According to Gartner, “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.” Gartner also notes that the objectives for Validation step includes to “assess the likely “attack success” by confirming that attackers could really exploit the previously discovered and prioritized exposures.”

2 Discovery

According to Gartner, “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.”

5 Mobilization

According to Gartner, “to ensure success, security leaders must acknowledge and communicate to all stakeholders that remediation cannot be fully automated.” The report further notes that, “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.”

3 Prioritization

According to Gartner, “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.” Gartner further notes that “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.”

The (MANY!) Benefits of CTEM

According to Gartner, "By 2026, organizations prioritizing their security investments based on a continuous exposure management program will be three times less likely to suffer from a breach." So clearly, vulnerability management is no longer sustainable and it's crucial to start to think towards this continuous paradigm, wherein organizations take measurable actions to detect and prevent potential threats and vulnerabilities on a consistent basis.

Additionally, we believe organizations should implement CTEM in order to:

✓ Prioritize Threats

Having a comprehensive CTEM program enables organizations to prioritize threats according to their potential business impact. This allows you to evaluate the severity and damage potential of every threat, and then allocate resources accordingly. Thus, security teams are empowered to not only prioritize more significant risks, but also use resources more efficiently and respond more quickly to the most potentially damaging threats.

✓ Gain Actionable Insights

CTEM was designed to help organizations derive actionable insights from threat intelligence in real time. With this, security stakeholders can remediate issues immediately and effectively, in a much more targeted and timely way.

✓ Proactively Manage Risk

By enabling proactive handling of vulnerabilities and threats based on continuous monitoring of digital infrastructure, CTEM changes the risk management equation. This is a far more holistic approach to cybersecurity that moves security focus away from reactive, and markedly enhances cyber defense.

✓ Augment Cyber Resilience

Organizations implementing a CTEM program continuously reassess and improve their defenses. This type of iterative refinement results in more robust cyber resilience, since organizations are able to draw conclusions from every assessment, then adapt defenses accordingly.

✓ Enhance Adaptability

CTEM programs are inherently adaptive, helping organizations respond to emerging or evolving technology and cyber threats. This means that protection is both continuous and relevant, which is critical in a rapidly-changing digital landscape.

✓ Align Security with Business Objectives

Within the construct of a CTEM program, organizations can align to cybersecurity best practices with their business objectives. Incorporating strategic business goals enables organizations to ensure that security is a goal-enabler, instead of a stumbling block.

CTEM Challenges You May Encounter and How to Overcome Them

Setting up a CTEM program is a fantastic initiative, but organizations often bump up against some challenges in implementation that should be addressed beforehand in order for execution to be successful. Accounting for them earlier on in the implementation stages could save time and frustration down the road. Let's have a look at the three main issues that need to be addressed and some possible solutions.

Getting IT and Security on the Same Page

Security and IT teams don't always speak the same language. In implementing CTEM, this can translate into a lack of understanding of who from IT will be responsible for implementing needed remediations and not being aligned on SLA expectations, among other issues.

› How to Overcome:

Bring stakeholders from IT and other non-security teams into the conversation. Share the goals you're trying to achieve to build a clear understanding of what is being done and get their input to see what they'll need from you or other teams to make their lives easier. Additionally, sharing news of cyber attacks with them will help them become more aware of the business impact their actions have, and how it actually ties back to their part of the business.

Seeing the Overall Picture

One of the goals of CTEM is to unite all different areas, from Cloud, to AD, to software vulnerabilities, to network security, etc. In practicality, that means aggregating all information from these various disciplines and using it to understand priorities and responsibilities.

But getting a baseline of understanding is challenging as each of these areas requires different expertise. You don't want to wind up with a program that’s been carefully built and executed but fails to understand the risks that each area presents – or worse, forgets to include any particular area of issue.

› How to Overcome:

Define someone as the “go-to” – the one person (or group of people) who can get the big picture and become a high-level master at understanding how all the covered areas converge and impact each other. This person doesn't need to understand how each tool works or what each category of security issue encompasses, but they should be able to understand the overall perspective to ensure all areas are accounted for and are continually addressed by the professionals who do have deep and nuanced expertise in their own domain.

Managing Diagnostic Overload

Each of the disciplines mentioned above, and quite possibly beyond, have their own tools which yield alerts. And so while a primary objective of CTEM is to streamline all of the information stemming from these tools, the byproduct is extraneous noise.

› How to Overcome:

Understand that fixing everything is impossible, and thus you need to prioritize and become as efficient as possible. To do this, focus on the scopes and exposures most likely to be exploited by an attacker and which could lead to the greatest business impact.

Operationalizing CTEM with XM Cyber Exposure Management

At XM Cyber, we've been talking about the concept of continuous exposure management for years now, even before the term CTEM was coined. We recognize that the only way to address the challenges listed above is to be able to identify all of the attack paths that can be exploited across your hybrid environment.

To do so, though, requires accounting not just for CVEs, but for all other exposure types, including misconfigurations that open doors for attackers, identity and credential exposures, and Active Directory issues, to name a few.

Once discovered, XM Cyber's Continuous Exposure Management platform then maps all exposures across hybrid cloud environments onto a single attack graph, so that Security and IT teams can understand how their critical assets are at risk, and what needs to be done to reduce the risk.

XM Cyber does this by identifying dead ends and choke points. Dead ends are exposures that while exploitable, do not enable attackers to progress their lateral movement to critical assets. This insight saves teams from expending enormous time and effort, as research has shown that as much as 75% of all exposures lead to dead ends. Instead of focusing on dead ends, security and IT teams can focus on choke points, which are exposures where multiple attack paths converge. By prioritizing those exposures to be addressed first, teams can close down the most amount of attack paths with the least amount of effort, optimizing their risk reduwwwction efforts.

Attack graph analysis offers a contextual understanding of threats that greatly reduces the friction between IT and Security by aiding informed decision-making and – especially – remediation prioritization. This allows Security teams to clearly demonstrate the danger of any given vulnerability it prioritizes, and enables IT to allocate remediation resources in good conscience, which is the core of mobilization between teams. Then the impact of the efforts can be shown to demonstrate that the remediations were validated and yielded the right outcomes.

Conclusion

In short, in our view, establishing a well planned and executed CTEM program helps organizations foster a common language of risk for Security and IT. This means that the level of each exposure becomes clear, and the handful of exposures that actually pose risk among the many thousands that exist can be addressed in a meaningful and measurable way.

Establishing a comprehensive Continuous Threat Exposure Management program should be on every company's 2024 list of goals. It's a nuanced and rigorous undertaking but will be highly worth it in the end. Use the best practices and strategies in this guide to help achieve your organizational CTEM objectives in this upcoming year.

Source: Gartner, Implement a Continuous Threat Exposure Management (CTEM) Program, Jeremy D'Hoinne, Pete Shoard, Mitchell Schneider, 21 July 2022.

XM Cyber is a leader in hybrid cloud exposure management that's changing the way organizations approach cyber risk. XM Cyber transforms exposure management by demonstrating how attackers leverage and combine misconfigurations, vulnerabilities, identity exposures, and more, across AWS, Azure, GCP and on-prem environments to compromise critical assets. With XM Cyber, you can see all the ways attackers might go, and all the best ways to stop them, pinpointing where to remediate exposures with a fraction of the effort. Founded by top executives from the Israeli cyber intelligence community, XM Cyber has offices in North America, Europe, Asia Pacific and Israel.