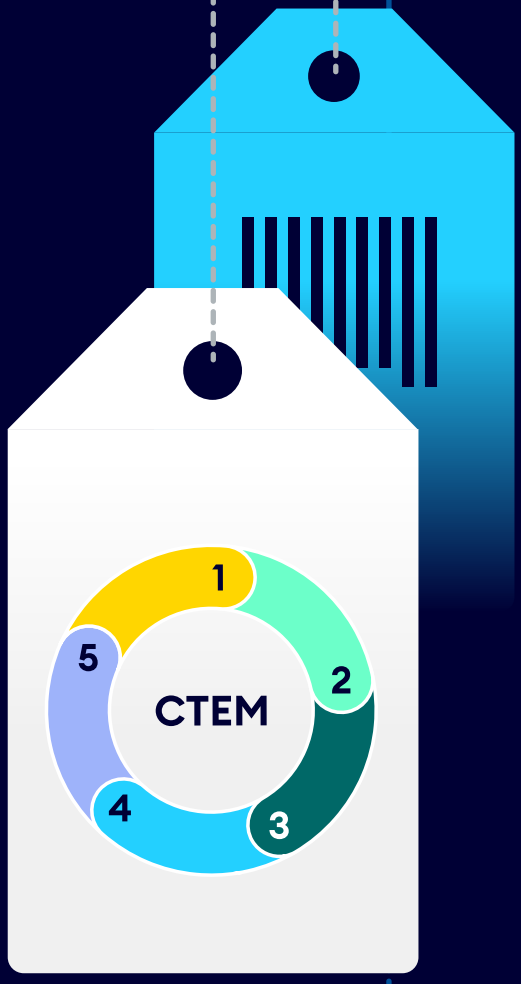
XM Cyber

Buyer's Guide to Meeting and Maintaining CTEM

Building the Framework for Continuous Threat Exposure Management



Introduction – The Challenge Of The Remediation Gap

Addressing the many security exposures and vulnerabilities organizations face each day can be very challenging. With so many factors contributing to the vast increase in issues that need to be addressed, such as an ever expanding attack surface, relentless attackers, and the increasing complexity of cloud environments, it often seems like defenders have limited ability to keep up with the onslaught of issues to be remediated. And while Vulnerability Management tools have been a key part in taming this beast, the shortcomings of this approach become more apparent all the time.

In 2023, more than 28902 vulnerabilities were identified, 3821 more than were identified in 2022. This is a trend that has been repeated year after year, with more CVEs identified in 2022 than in 2021 and so on. And though the number of issues in need of triaging and addressing continues to climb, the capacity to – in actuality – address them has not necessarily increased.

Moreover, CVEs only represent a fraction of the issues that can put assets at risk. Issues such as weak credentials, misconfigurations and other weaknesses account for the vast majority of issues that can put organizations at risk.
To quote Gartner®,

"Traditional approaches are no longer keeping up with quickly evolving business needs and expanding attack surfaces. Exposure extends beyond vulnerabilities."

(Gartner, Implement a Continuous Threat Exposure Management (CTEM) Program,
By Jeremy D'Hoinne, Pete Shoard, Mitchell Schneider 11 October 2023)

This growing chasm between the number of issues an organization needs to address and their ability to address them is referred to as the remediation gap. In a recent study of 300 CISOs and decision makers at enterprises, 82% of respondents acknowledged the increasing gap between the number of issues to be remediated and their ability to address them.

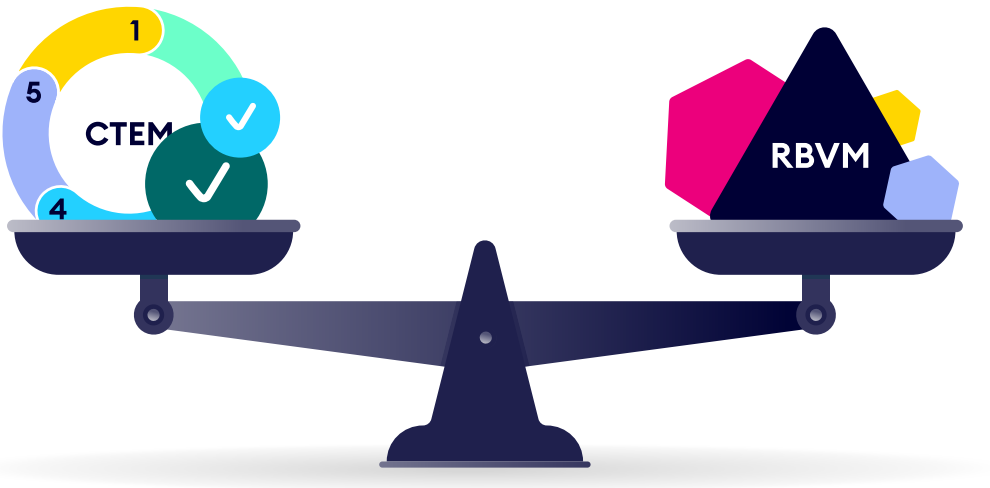
Addressing The Remediation Gap With Exposure Management

In this light, improving security posture and reducing risk can seem like far off goals. Simply making a dent in the massive remediation gap may feel like an impossible task. So, as these shortcomings of a vulnerability management-based approach have become apparent, organizations have moved to exposure-based approaches.

Exposure Management provides a holistic view across the modern attack surface, enabling organizations to better understand their true risks and make better business decisions. By understanding the most impactful exposures, security teams become better positioned to address cyber risk. Exposure Management is a proactive approach so organizations can keep pace with a constantly shifting threat landscape and the implications for your organization's needs.

Effective management of exposures consists of a multistep process that is conducted by Security and IT teams on a continual basis. Many solutions aim to address one or more parts of this process that need to be conducted as part of any Exposure Management program

Here we'll have a look at some of the most common tools in use today and their advantages and disadvantages.



Risk-Based Vulnerability Management (RBVM)

Advantages

Risk Based Vulnerability Management is designed to help organizations limit risk through the strategic prioritization of vulnerability remediation. These tools assess existing cybersecurity vulnerabilities and determine the amount of risk each vulnerability poses to business-critical assets based on known exploitation of vulnerabilities "in the wild". RBVM tools usually use measurements like EPSS and CVSS to gauge the criticality and exploitability of each CVE in the wild.

Disadvantages

Automating this process is essential, given the scale involved, which is why they've existed for decades. But still, defenders using these tools are overwhelmed with the job of managing cyber vulnerabilities. Even large, well-funded organizations can't patch all the vulnerabilities they discover. There are simply too many vulnerabilities, and there are systems that can't be patched, as well as supply chain dependencies. Critically, RBVM is limited to prioritizing only vulnerabilities (CVEs), and doesn't discover misconfigurations and over-privileges, leading to blindspots across the hybrid environment.

Red Team Exercises

Advantages

Red Team exercises are performed to achieve specific goals, such as evaluating the ability of attackers to reach business-critical applications. According to IBM, Red Teaming is "heavily focused on emulating an advanced threat actor using stealth, subverting established defensive controls and identifying gaps in the organization's defensive strategy. The value of this type of engagement can be derived from a better understanding of how an organization detects and responds to real-world attacks."

Disadvantages

Red Team exercises are valuable to (a) identify and uncover one or more particular attack paths to critical assets and (b) test the ability of defenders to detect the attackers. However, they're manual exercises that are expensive and only performed periodically. Also, they don't uncover all the attack paths that could be taken, or prioritize the fixes required to prevent them. In other words, they are good for testing existing defenses, but poor for making regular, comprehensive posture recommendations.

Cloud Security Posture Management (CSPM)

Advantages

Cloud Security Posture Management (CSPM) solutions identify misconfiguration issues and compliance risks in the cloud. CSPM helps monitor cloud infrastructure for exposures and gaps in security policy enforcement. Given the growth in the combined IaaS, PaaS and SaaS markets, this is clearly an area of importance. In fact, experts project that 99% of records compromised in cloud environments will be the result of user misconfigurations and account compromise. Some CSPM tools also extend to CIEM (Cloud Infrastructure Entitlements Management) and are able to identify over-privileges across multi-cloud environments.

Disadvantages

However, most organizations, especially large ones, have environments consisting of remote employees, on-premises assets, and multiple cloud vendors. So a CSPM is fundamentally a piecemeal solution. It doesn't provide a holistic view into their security posture, and it can't prioritize remediation efforts organization-wide. This is particularly important since many attacks involve compromising a combination of remote assets, on-premise assets, and cloud assets.

Breach And Attack Simulation (BAS)

Advantages

Breach and Attack Simulation (BAS) solutions offer a different approach for performing automated security testing and validation. Some BAS tools challenge the existing security infrastructure, while others are designed to test existing security controls to ensure they are working as expected. Breach and Attack Simulation, Pen Testing, and Red Teaming all simulate attacks to hypothesize the outcomes of real-world scenarios. They are used to assess and find issues that need to be addressed.

Disadvantages

Their use, though, is limited by the operational risk they create, as running these live tests can put the security team at risk of creating performance issues - or worse, outages - on production systems. These tools are used periodically across a fraction of the overall environment, leveraging only a subset of all possible attack techniques. While still valuable for finding issues, this approach is incomplete.

Identity And Access Management (IAM) And Identity Threat Detection And Response (ITDR) Tools

Advantages

Identity and Access Management (IAM) and Identity Threat Detection and Response (ITDR) solutions are laser focused on identities. These are critical to an organization's security posture, since most attacks take advantage of an identity vulnerability somewhere along the attack path, especially in cloud environments.

Disadvantages

However, they don't include an evaluation of non-identity exposures, or any ability to determine potential attack paths to critical assets. Thus, their view into an organization's environment is limited.

Penetration Testing

Advantages

Penetration testing is similar to Red Team exercises as both use a testing methodology to assess an organization's cyber defenses. However, pen testing is typically performed periodically during well understood timeframes, and typically looking for known vulnerabilities. Pen tests assess if applications, networks, platforms, and systems can be breached, and are used to find issues that need to be addressed.

Disadvantages

As with Red Team exercises, pen testing suffers from an inability to assess the full environment, and it only provides a point-in-time assessment – one that's lacking in prioritization, and almost immediately out of date. Penetration testing results will deliver highly confident results for a limited scope, but with a highly manual effort.

External Attack Surface Management (EASM)

Advantages

External Attack Surface Management (EASM) is the process of continuously discovering and inventorying the risks of external assets to potential breaches. It's fully focused on the initial breach points of an attack – your IT environment's "external surface".

Disadvantages

As such, it's conducted from outside your environment, and it provides no insight into further steps an attacker would take beyond that initial breach. It's also limited in terms of prioritization (only based on CVSS and EPSS) not accounting for the impact these could have on the internal network and critical assets.

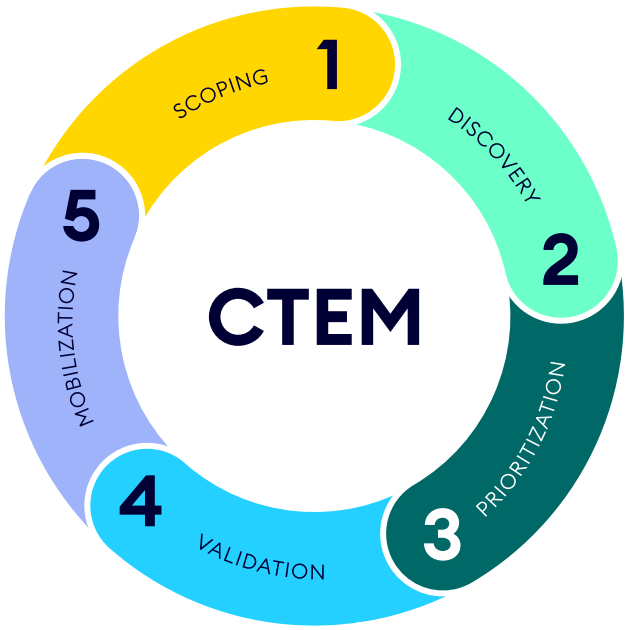
The Move To A Continuous Threat Exposure Management (CTEM)-Based Approach

Organizations need to shift from addressing individual threats to proactively managing threat exposure. With the ever-expanding threat landscape in mind, the CTEM framework helps organizations identify vulnerabilities and exposures, evaluate them, prioritize them based upon their risk to critical assets, and monitor progress as they implement remediation activities.

CTEM continually assesses an organization's entire ecosystem–including networks, systems, assets, and more–to identify exposures and weaknesses with the goal of reducing the likelihood of these weaknesses being exploited. A CTEM program can enable continual improvement of security posture by identifying and remediating potentially problematic areas before attackers can exploit them.

The "continuous" element of CTEM refers to a give-and-take relationship between the CTEM program and the associated risk remediation efforts, wherein data stemming from both aspects informs processes to make ever-more optimal decisions about how to manage exposure risk. According to Gartner in their report Implement a Continuous Threat Exposure Management (CTEM) Program, Published 21 July 2022, "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."

As opposed to vendor-specific tools, CTEM is a systematic approach that enables organizations to effectively prioritize potential threats and remediation efforts. As such, organizations leverage multiple tools to achieve their objectives of continually reducing risk and improving security posture. CTEM allows organizations to aggregate the exposures, place them into context according to actual risk (based on how an attacker can exploit the current configuration of their environment), and prioritize remediation activities. Far less time is spent fixing exposures that don't matter and organizations can quantify the impact of their efforts.



The 5 Stages Of A CTEM Program

As mentioned earlier, a CTEM program is made of 5 stages, each of which is essential to the success of the program. There is no "skipping" stages as each stage serves as a foundation and informs the next stage. Here is a look at the 5 stages:

1

Stage 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 says, "More developed vulnerability management projects generally include good initial scoping for internal, on-premises and owned assets."

2

Stage 2 – Discovery

Continuing on, Gartner says, "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."

3

Stage 3 – Prioritization

About stage three, Gartner says: "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 notes "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."

4

Stage 4 – Validation

Says 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 notes 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."

5

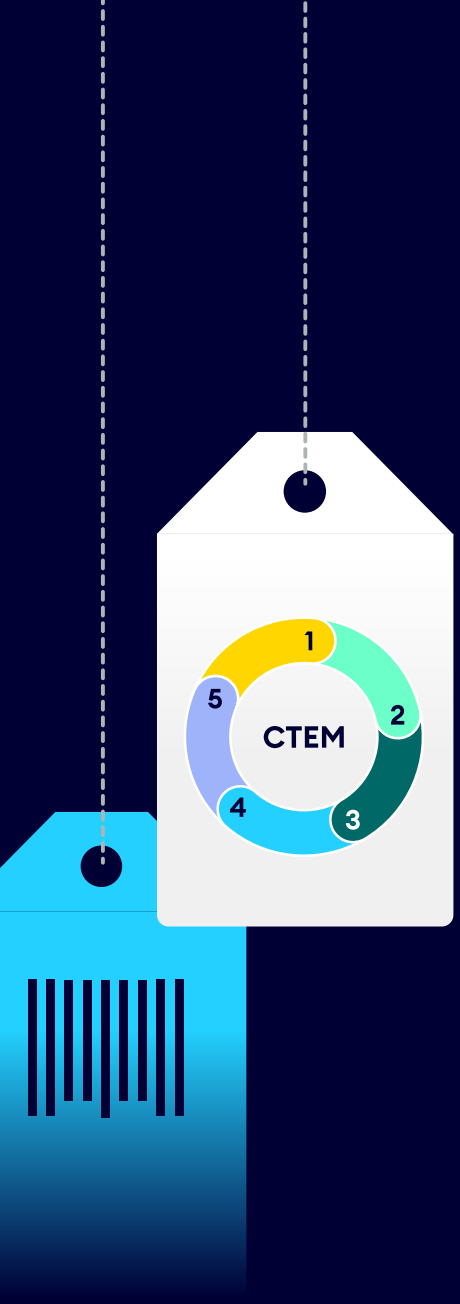
Stage 5 – Mobilization

In this stage, according to Gartner, "to ensure success, security leaders must acknowledge and communicate to all stakeholders that remediation cannot be fully automated." It also says, "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."

What We Believe You Should Look For In Evaluating Tools To Meet And Maintain CTEM

Scoping the threat landscape of critical assets	Can the solution identify critical assets in YOUR environment and map the risks posed to them?
Breadth of exposure detection	What different types of exposures does the solution encompass, such as traditional vulnerabilities, misconfigurations, identity issues, and more?
Environmentally comprehensive	Does the solution cover all workstations, entities, virtual machines, containers, user activity, cloud resources, applications, and configurations, etc., as part of analysis to ensure you can see all ways your organization is at risk to plan prioritized remediation efforts? Does it discover exposures across the attack surface, within your perimeter and beyond it?
Risk contextualization	How well does the solution combine its knowledge of exposures, network paths, and critical assets into a view of potential attack paths in YOUR environment? And how does it display this information for defenders so that both security and IT teams understand the value of their remediation efforts?
Remediation prioritization	Does the solution analyze potential attack paths and prioritize them by the impact they pose to critical assets, so you know what to fix to disrupt the most damaging attack paths first?
Remediation efficiency	Can the solution build attack graphs of multiple attack paths in order to identify intersections (choke points) that can be fixed to block multiple attack vectors?
Remediation assistance	With its knowledge of exposures and attack paths, can the solution provide concrete remediation guidance to implement fixes, improving both consistency and efficiency?
Remediation alternatives	Some exposures cannot be fixed, whether because of legacy systems or other limitations. Can the solution leverage the attack path to propose alternatives that will address the risk on the one hand and adjust to limitations on the other?

Continuous evaluation	Given that IT environments are constantly changing, does the solution perform continuous evaluations to detect new exposures and new attack paths that will appear? Does it also keep up to date with the latest vulnerabilities and attack techniques? And can it track changes in security posture over time?
Measuring KPIs for exposure management	What was the impact of remediation on your security score?
Executive reporting	Can the solution combine organization-wide risk assessments and trending information into executive-level reporting, to answer such questions as, "Where are we most vulnerable?" and, "How is our risk posture improving over time?"
Operational safety and impact	How easy is the solution to deploy and manage? And what potential risks, if any, does the deployment have on your production environments?
Security Control Monitoring	Can the solution provide comprehensive, real-time visibility into cybersecurity posture in terms of risk reduction, productivity gains, and cost avoidance?
Scalability	Is the tool able to meet the requirements of large and diverse enterprises?
Integration with ticketing	Does the solution integrate with Jira or other ticketing systems to be able to track progress of requested remediations?
Another way to evaluate vendors is to consider these questions, and how different vendors answer them:	• Which of my critical assets are at risk today? • What paths would allow an attacker to reach them? • Where are all the exposures in my environment? • Which ones are most important to remediate to protect my critical assets (i.e. choke points)? Which are least important (i.e. dead ends)? • How can you show me an overall score or assessment of my posture in protecting my critical assets? Can you help me demonstrate improvement over time?



Why Do Organizations Choose XM Cyber For CTEM?

As we see it, XM Cyber's Continuous Exposure Management platform is the most comprehensive solution for delivering the value of exposure management – the core capability required for a CTEM program. XM Cyber uniquely discovers exposures that go beyond traditional vulnerabilities, encompassing a wide range of configuration and identity issues that real-world attackers rely on to succeed.

XM Cyber analyzes exposures, connectivity, and the value of various assets – across remote devices, on-premise, and cloud. Unlike some of the aforementioned approaches, XM Cyber's approach to validating exposures is safe to run comprehensively across large environments without risk of creating operational issues or false positive alerts.

XM Cyber goes beyond one-time detection, continuously providing valuable prioritization and guided remediation, as well executive-level reporting and security posture trending. All the above help you avoid busy work, implement improvements that protect your assets from real-world attackers, and clearly communicate status and trending to busy executives.

Want To Learn More About Getting Started With XM Cyber's Continuous Exposure Management Platform?

Reach Out To Us Today!

XM Cyber

XM Cyber is a leading Continuous Exposure Management company that transforms the way organizations approach cyber risk, enabling security teams to prevent more attacks with 75% less remediation effort. Its XM Attack Graph Analysis™ capability discovers CVEs, misconfigurations, and identity issues across on-premise and all major cloud environments. It analyzes how attackers can chain exposures together to reach critical assets, identifies key "choke points", and provides remediation guidance. Founded by top executives from the Israeli cyber intelligence community, XM Cyber has offices in North America, Europe, Asia, and Israel.