XM Cyber

Guide

5 Stages of CTEM

Your Guide to Making Them a Reality

Introduction

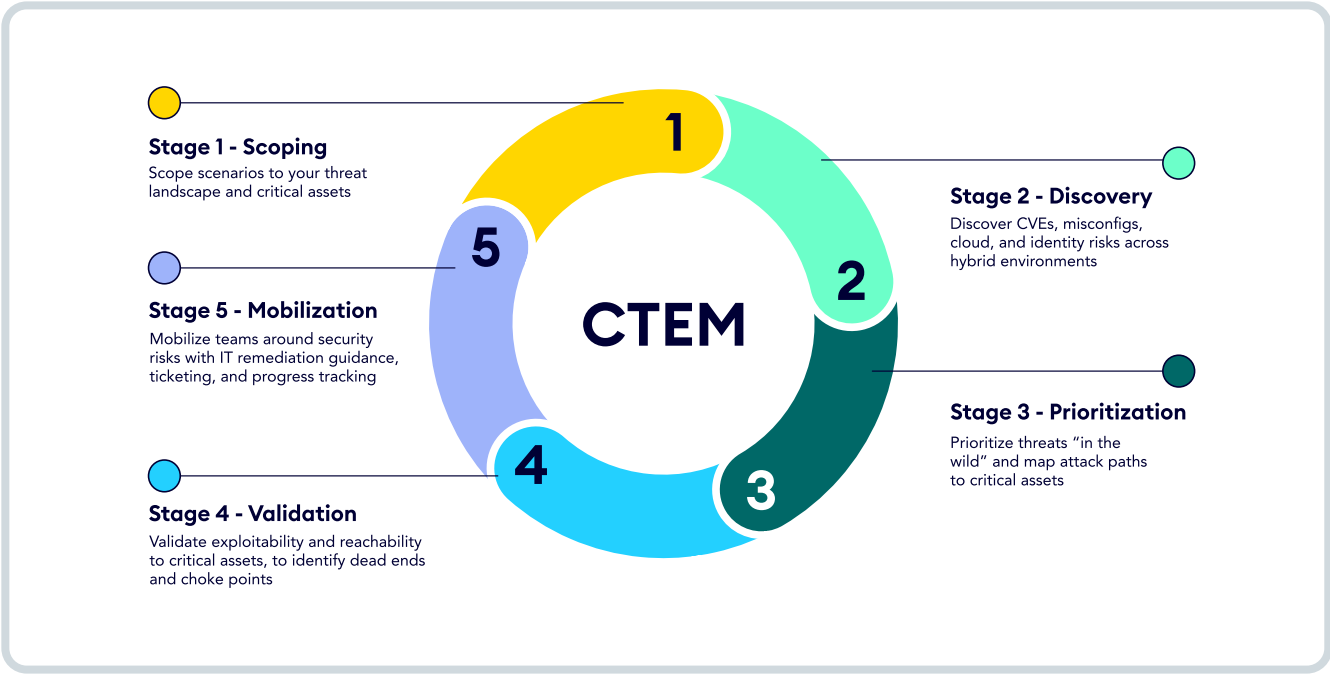
As organizations grow and change, so too do the risks and threats they face.

The complexity of today's environments mean that yesterday's approaches and best practices no longer cut it today. Expanding IT infrastructure, new vulnerabilities and exposures, and advancing attack vectors introduce novel threats. Complicating the situation, organizations have an overwhelming volume of exposures – far more than they can actually fix, and some of which can't be fixed. Exposures are typically separated into different lists based on the tools available for different types of exposures, and for different environments – on-premise, cloud, containers, traditional vulnerabilities, configuration issues, identity exposures, Active Directory issues, and more. And often, there's no way to aggregate these exposures or place them into context according to actual risk.

The result? A lot of time is wasted on fixing exposures that don't matter. And even when progress is made, it's hard to correlate it to overall organizational risk, or to illustrate how their efforts are making a difference.

Increasingly, The Continuous Threat Exposure Management (CTEM) Framework by Gartner is being seen as an impactful way to address the full range of challenges that put organizations at risk. A strategic framework that helps organizations continuously assess and manage cyber risk, a holistic CTEM program goes far beyond assessing CVEs and other vulnerabilities. It breaks down the complex task of managing security threats into five distinct stages: Scoping, Discovery, Prioritization, Validation, and Mobilization. Each stage plays a key role in identifying, addressing, and mitigating vulnerabilities before they can be exploited by attackers.

In this guide, we cover the 5 stages of CTEM, explore how they help organizations finally reduce risk and improve security posture in an impactful way, and understand how XM Cyber helps organizations stage by stage.



Scoping

Scoping is the initial phase in which security teams identify the infrastructure segments that should be included in the program and determine the critical assets. As part of this step, organizations decide what matters most to their business – the threat landscape, their crown jewels, and/or their use cases – and then adapt the CTEM program accordingly.

Large organizations have complex attack surfaces that extend far beyond traditional devices and applications. To effectively protect this ecosystem, most organizations start by establishing an initial scope. This initial CTEM scope should demonstrate rapid value to stakeholders, and thus, it generally takes a narrow focus. Organizations then add use cases that encompass digital risk protection, and provide different focus for reporting on the attack surface.

Defining and refining scope requires understanding of business priorities and identifying the potential impact of threats. Unlike traditional vulnerability management projects, CTEM programs adopt an "attacker's point of view", looking beyond CVEs. Scoping for a CTEM program pilot involves considering external attack surfaces and evaluating SaaS security postures – especially given the increasing reliance on remote work and critical business data hosted in the cloud.

The scoping process encompasses multiple steps, starting with a detection phase that:

Leverages open-source intelligence methods to detect assets.

Employs network scanning tools to identify network-level services.

Uses attack surface management techniques to monitor changes in the attack surface map.

Uses crawlers to discover URLs and user inputs.

A well-defined and evolving scope is vital for the success of CTEM programs in large organizations, considering the diverse and expanding nature of the modern attack surface.

An effective CTEM Scoping process is built on two pillars: continuous monitoring and automation. Continuous monitoring is a must-have, owing to the dynamic nature of cyber threats. Automation is indispensable because manual scoping processes are time-consuming, prone to human error, and simply impractical when dealing with a multitude of digital assets.

The next step is to determine which are critical assets for which risk and the impact that would be amplified in the case of cyberattack. While continuous automated detection can increase efficiency, you'll need to verify that critical systems that hold sensitive data, essential for business transactions or that hold intellectual property, aren't overlooked.

-> How XM Cyber Helps With Scoping

XM Cyber discovers the entities with the highest combination of compromise effect over your environment and likelihood of being breached themselves according to the choke point score. That is true across the multi-cloud environment or in the internal network. It also automatically discovers critical technical assets by categorizing assets in the multi-cloud or in the internal network.

XM Cyber offers an integration with your CMDB or asset management system to automatically label your assets based on the business processes they are supporting.

As part of the CTEM Scoping phase, XM Cyber has developed a unique methodology for helping organizations to secure their most critical and exposed enterprise technology assets, in relation to their main business focus. It also provides a configurable engine to define use cases that are critical for your enterprise. It then maps critical business processes to underlying IT assets to prioritize exposures based on risk to the business.

Discovery

Discovery plays a key role in comprehensively assessing and understanding an organization's digital landscape. The main objective of this phase is to unearth and evaluate entities along with associated risk levels. Discovery goes beyond identification of assets and vulnerabilities. It includes the detection of misconfigurations in assets and security controls, as well as identity and access exposures, such as exposed credentials and over-permissions.

If the Discovery step is limited in scope, then your security program will have inherent blind spots and all the following steps will leave your IT environment exposed to cyber threats.

-> How XM Cyber Helps With Discovery

Discovery Across Your Hybrid Environment

Many security solutions focus on finding issues either on-prem or in a cloud environment. These tools may provide good coverage for a specific segment of your environment, but will miss out on exposures that enable attacker lateral movement from your on-prem breach point into sensitive data and resources in your cloud environment. XM Cyber helps discover exposures across your hybrid environment, to block attack paths that compromise critical assets on-prem and in the cloud.

Discovery from External Attack Surface to Internal Critical Assets

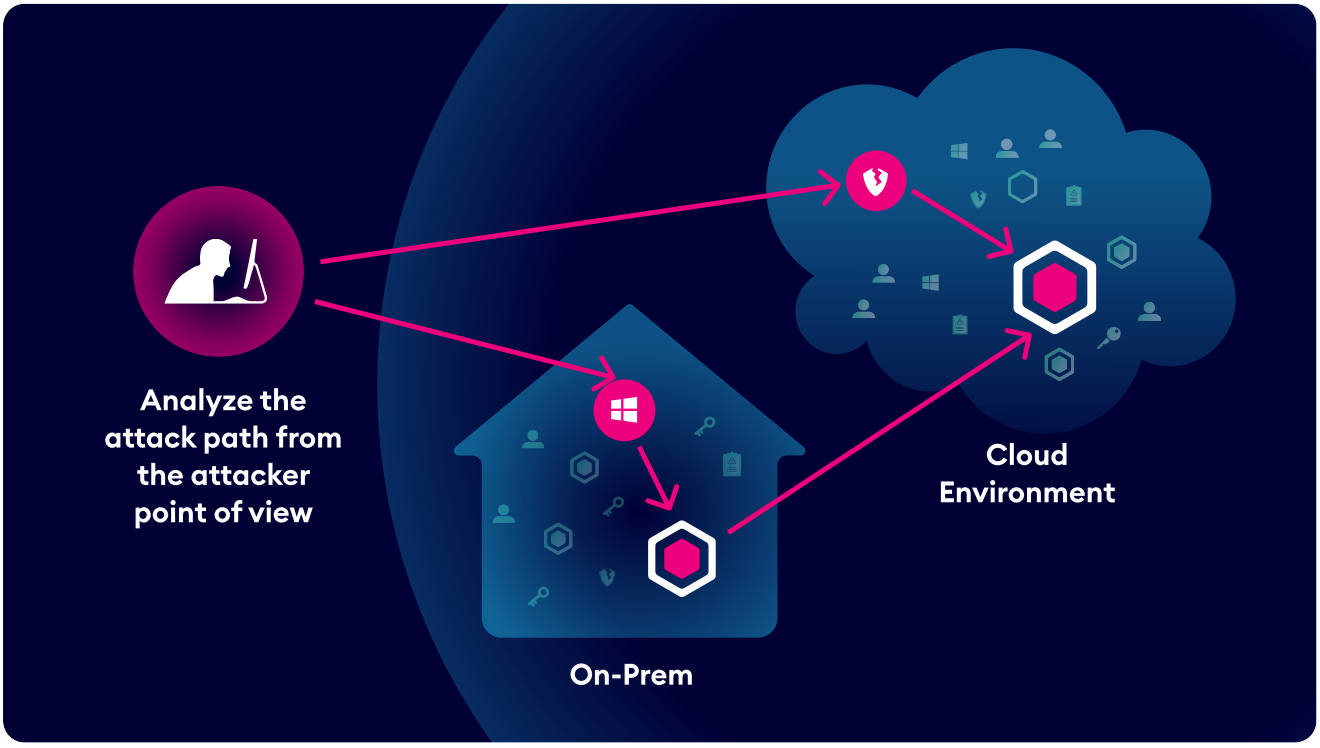
Attackers see the full picture. They identify the potential breach point, either by finding a public-facing vulnerable asset, or by leveraging leaked and stolen credentials, and then research how to move across your environment to accomplish their goal. To stop them, you need to be able to discover the potential breach points before they do, and to discover exposures that can be used to compromise your critical assets. XM Cyber's discovery runs from your external attack surface to internal critical assets.

Continuous Discovery

Discovery at a point-in-time could be misleading. Your environment and the threat landscape keep changing and today could pose threats that were undiscoverable yesterday. Therefore, continuous discovery is the most comprehensive approach, and provides better protection from attackers.

In-depth Discovery Using Sensors

With XM Cyber, you can discover assets and exposures where you don't have sensors installed by connecting to your Active Directory domains, multi-cloud environment, legacy systems, and OT systems.



Prioritization

The goal of exposure management is not to remediate every identified issue or focus solely on zero-day threats, but to prioritize and address the threats that could most likely be exploited in YOUR environment and have the most critical consequences on your business.

Prioritization involves assessing potential vulnerabilities identified in the Discovery stage and addressing them based on priority, considering their likelihood of exploitation and potential impact. Factors like potential damage to assets or reputation, the probability of successful exploitation, and the difficulty in dealing with the vulnerability are considered in this stage.

Once prioritized, CTEM offers a guiding framework for organizations to develop a plan to validate and address vulnerabilities - implementing security controls or processes, conducting regular testing to ensure effectiveness.

Prioritization is an ongoing process, requiring security stakeholders and teams to continually assess, rank, and select which assets require immediate attention based on the potential risk.

-> How XM Cyber Helps With Prioritization

By incorporating XM Cyber into your CTEM program, you can more efficiently manage threats and exposures, ensuring accurate and cost-effective prioritization and remediation that rapidly improves security posture. XM Cyber manages prioritization by:

Highlighting Choke Points

XM Cyber leverages its proprietary Attack Graph Analysis™ to highlight assets and exposures that, when remediated, block multiple attack paths – the Choke Points that offer more bang for your remediation buck. By fixing these Choke Points first, you gain remediation efficiency and save time and money on analysis and remediation efforts. Recent research found that 2% of exposures are Choke Points, meaning that 2% of your current remediation efforts can block most of your critical attack paths.

Deprioritizing Dead Ends

XM Cyber also leverages attack paths to identify exposures on attack paths that don't compromise critical assets, so an attacker who exploits these for lateral movement won't endanger business critical systems and applications – Dead Ends that can be deprioritized – as opposed to exposures that directly impact critical assets. Recent research found that 75% of exposures are "Dead Ends" and can be deprioritized.

Prioritizing Across CVEs, Misconfigurations & Identity Issues

In a single dashboard view, teams can discover, prioritize, remediate, and validate all exposure types from the external attack surface, to on-prem and cloud environments, offering a more holistic and contextual view into risk.

Generating Attack Paths from the Attacker's Perspective

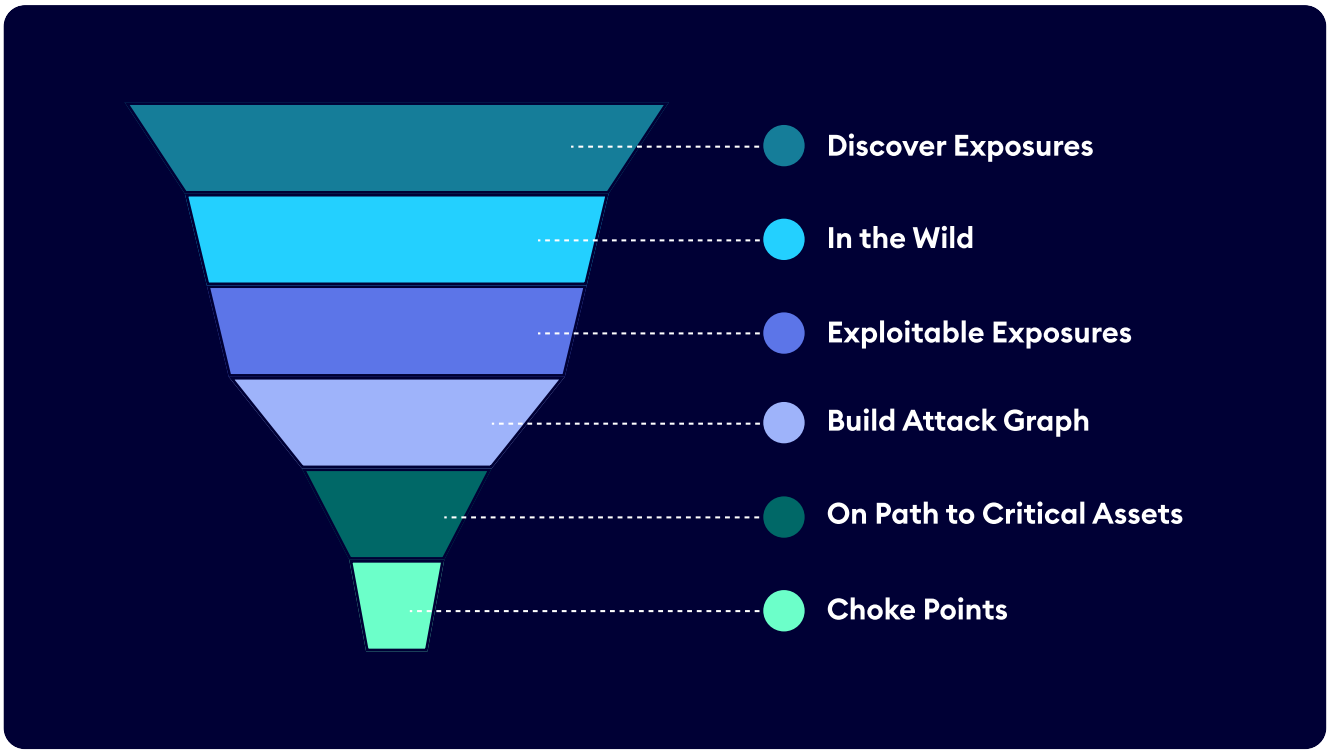
XM Cyber leverages attack paths to check the exploitability and the potential impact on critical assets in YOUR environment. Attack paths provide the business context of each asset and each exposure to not only calculate the priority, but even to identify remediation alternatives to block the attack path in case an exposure can't be fixed.

Monitoring Security Controls

XM Cyber's Security Control Monitoring (SCM) module provides insights into the activation and configuration of security solutions along the attack path that could block it from compromising critical assets.

Continuously Evaluating Security Posture Score

XM Cyber helps you share continuously updated metrics of security posture and trending that shows the impact of remediation efforts, and thus the success of prioritization.



Validation

Validation looks at how attacks can occur and the likelihood of their occurrence. This step assesses if the assertions of the previous steps are accurate and validated. Validation puts the findings of CTEM Discovery to the test, confirming which discovered exposures are truly dangerous.

Validation aims to achieve three key goals:

Confirming Exploitability

Verifies if attackers can truly exploit identified weaknesses, separating critical issues from false positives.

Identifying Attack Paths

Maps out all potential routes hackers might use to exploit the exposure, giving a complete picture of the attack landscape.

Testing Response Effectiveness

Assesses if the organization's current security controls and incident response procedures are sufficient to stop real attacks targeting these weaknesses.

By validating exposures, CTEM helps ensure resources are directed at fixing issues attackers can truly exploit. A robust validation process strengthens security posture by focusing on real threats and proactively addressing exploitable exposures.

It's crucial to first clearly define the scope and goals of your CTEM validation process, including identifying critical assets and systems to better focus validation on the most critical assets and systems within your organization – those with the most significant impact if compromised. Also, establish clear objectives: Do you want to prioritize high-risk exposures, test specific attack scenarios, or both?

Next, choose the validation techniques right for your organization's unique security posture and ecosystem. Traditional approaches include automated tools, manual testing, and attack path modeling.

While CTEM defines validation as the fourth step, between prioritization and mobilization, one could argue that validation should actually run alongside these steps. Prioritizing exposures that may not be valid within your environment based on architecture and security controls is a futile effort. Spending cycles on analyzing the potential impact of an exposure that's not exploitable is frustrating and inefficient. That's why XM Cyber runs validation alongside prioritization. As we generate the attack graph analysis, we analyze exploitability and impact to critical assets.

-> How XM Cyber Helps With Validation

The XM Cyber platform validates whether issues are exploitable in a specific environment and if security controls are configured to block them. It does this by:

Leveraging the XM Attack Graph for Exposure Validation

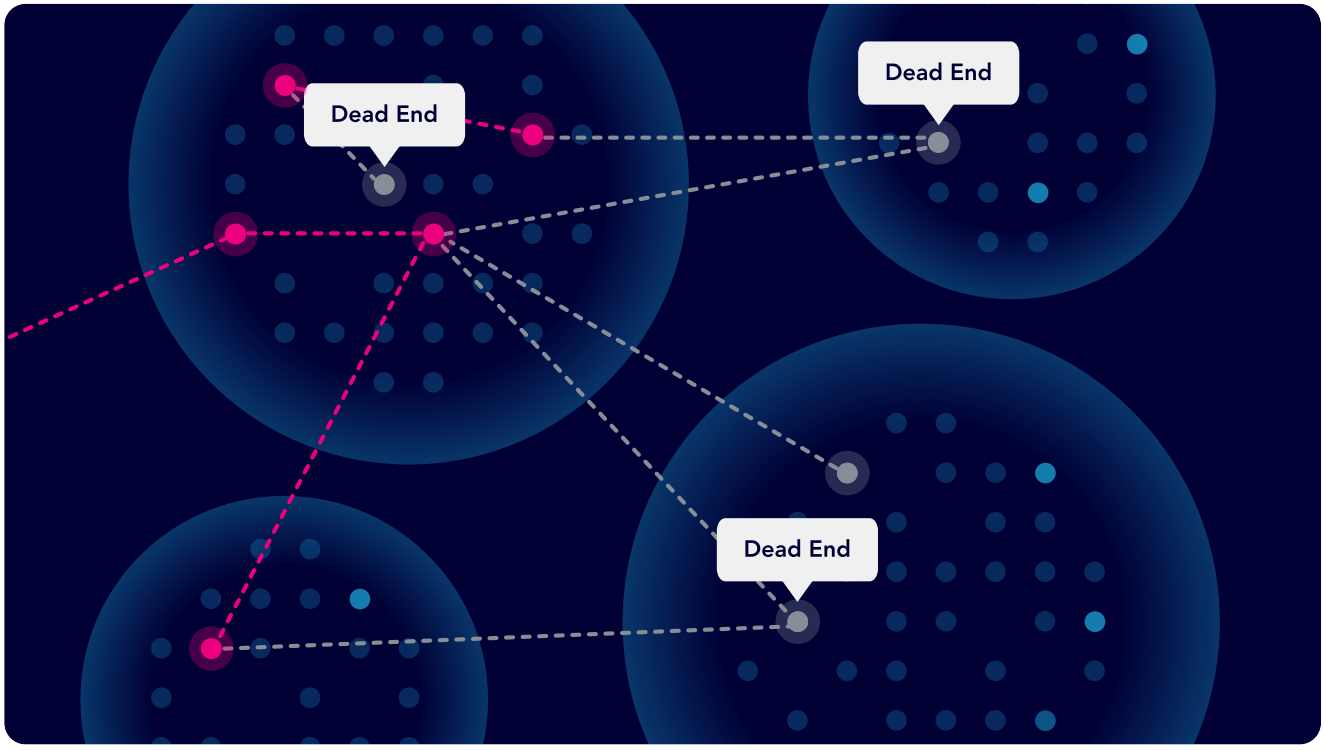
XM Cyber identifies the exposures that are exploitable in your environment based on XM Attack Graph Analysis™ and focuses on fixing them first to increase security and efficiency.

Verifying the Effectiveness of Security Controls

The platform monitors security controls for misconfigurations to reduce risk, ensuring compliance with policies and regulations, and integrating results into the attack path.

Confirming that Remediation Reduces Risk

Lastly, it validates that applied fixes block attack scenarios and improve security posture in order to gain confidence and improve reporting to management.



Mobilization

Mobilization isn't just about advising on what needs to be fixed, but also advising on what doesn't need to be fixed. Security teams need to realize who should be responsible for remediating risks, whether it's patching a vulnerability, blocking users, adjusting configurations, and in certain cases, risk acceptance.

Mobilization is where resources, tools, and personnel are prepared and organized to proactively remediate threat exposures.

-> How XM Cyber Helps With Mobilization

To increase the effectiveness of remediation, it's essential to engage with the relevant team who will fix the problem and communicate the prioritization and categorization of any required fix. And while this can certainly help, it may not be enough. Beyond transparency and empowerment, there are several ways that XM Cyber helps resolve friction and boost efficiency and effectiveness across teams:

Focus on Exposures with the Highest Impact

To increase confidence and ensure the operations team has bandwidth to establish the most effective fixes, make sure to only send those exposures that are, in fact, exploitable in your environment AND compromise critical assets (business or IT infrastructure). You need a reliable way to narrow down the endless lists of vulnerabilities and other exposures into a shortlist of what really matters, and identify the fixes that block multiple attack vectors. XM Cyber helps you generate this list.

Provide Full Context and Justification

Lack of transparency increases frustration on both sides of mobilization. Collect the context of the exposure and the entity it was found on, including the justification of why they are on the shortlist. This can be based on how easy or difficult they are to exploit in your IT environment, and on the number of critical assets compromised by this exposure and the impact it would have on your business. Just like in any relationship, communication cannot be overrated.

Provide Complete Guidance on What and How to Fix

Don't assume the operations team will know exactly what to fix and how to do it. Although in most cases they make the final decision, remediation guidance can increase effectiveness and level-set expectations. Make sure to provide full context of the required fix, whether it's applying a patch, blocking access, restricting permissions, or adjusting configurations of systems and controls.

Leverage Integrations to Streamline and Automate the Process

Whether you're using a ticketing system, a SIEM, and/or a SOAR system, remediation requests should be streamlined to ensure consistency and efficiency. To facilitate remediation, you'll have to adhere to the existing process flow and package justification, guidance, and alternatives for the fix into an ITSM ticket, or an incident.

Provide Remediation Alternatives

In some cases, the exposure with the highest severity or impact can't be fixed. This can be due to a versioning issue, system-defined group permissions, or other limitations. In most cases, the operations team will notify you of the limitation, but in some cases, the risk will remain without your knowledge – and this could be the exposure that jeopardizes your business in the next cyber attack. You need to provide alternatives that would still reduce risk and block a potential attack. This can be done by visualizing and analyzing the attack paths that leverage this exposure and remediating an adjacent step in the path.

Close the Loop and Verify Remediation was Effective

To ensure risk reduction and regain confidence, you'll need to verify that the applied fix resolved the high impact exposure and that potential attacks will be blocked. Not verifying remediation leads to a disconnect between teams and could create a false sense of resilience. The way to achieve remediation verification is by running continuous discovery across your holistic environment. If the exposure is no longer discovered on the entity AND the attack paths that cross these entities are blocked, then remediation was effective at reducing risk.

Wrapping It All Up

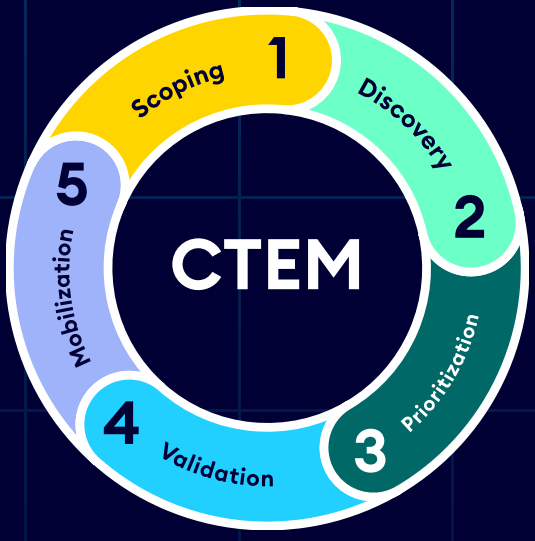
Building a comprehensive CTEM program is a nuanced and challenging process – but one that is well worth it when done properly. Use the tips and best practices in this guide to help ensure your CTEM undertaking is a success.

There are multiple technologies that map into each stage, but integrating all of them into a holistic framework is very challenging. XM Cyber's unified approach to CTEM simplifies implementation by integrating multiple stages into one cohesive platform. This minimizes the complexity associated with deploying disparate tools and processes. With XM Cyber, you get real-time visibility into your exposures, enabling you to prioritize remediation efforts based on actual risk rather than theoretical assessments.

The platform facilitates seamless communication between SecOps and IT Ops, ensuring that everyone is on the same page regarding vulnerabilities and remediation. This collaboration fosters a more efficient and responsive security posture, allowing your organization to address potential threats quickly and effectively. Moreover, the XM Cyber Continuous Exposure Management Platform enables you to report risk to your C-suite and Board with accuracy and confidence that the correct issues are being addressed most optimally. With XM Cyber making the 5 stages of CTEM an achievable reality, you can finally reduce risk and improve security posture in a truly impactful way.

Want to learn more about how XM Cyber enables the 5 stages of CTEM?

Reach out to us today!



XM Cyber

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.