Ahead of the Curve:
The Role of CTEM in Cyber Risk Management

A Guide to Continuous Threat Exposure Management

CRITICALSTART®

Executive Summary

Adopting Continuous Threat Exposure Management (CTEM) is a strategic imperative for organizations aiming to enhance their cybersecurity posture. CTEM offers a comprehensive approach to continuously identifying, assessing, and mitigating risks posed by cyber threats.

By leveraging CTEM, organizations can expect to see a significant reduction in breaches. According to the "Top Trends in Cybersecurity for 2024" report from Gartner: "By 2026, organizations prioritizing their security investments based on a continuous threat exposure management program will realize a two-thirds reduction in breaches."

Critical business drivers for CTEM adoption include the need to manage expansive attack surfaces resulting from increased digitalization, such as SaaS, digital supply chains, and remote work. CTEM addresses the rapid evolution of threats and the weaponization of vulnerabilities, providing a way to measure, assess, and identify vulnerabilities and other threats for prioritized mitigation, leading to real risk reduction.

Over the next three years, organizations will realize strategic gains from CTEM adoption through improved alignment of security operations with dynamic attack surfaces and modern IT architectures. This alignment will enable organizations to focus on the most pressing security issues, ensuring a more effective and measurable impact on the business's risk profile.

In this whitepaper, we will:

- Delve into the specifics of CTEM, highlighting how it drives greater risk reduction by prioritizing business context and cross-functional ownership.
- Demonstrate how CTEM helps organizational leadership make data-informed decisions.
- Explore the five-step CTEM approach—scoping, discovery, prioritization, mobilization, and validation—and how each contributes to a robust security management process.
- Discuss the challenges organizations face in creating a CTEM program and how to overcome them.

By the conclusion, you will see how your organization can leverage Critical Start to move purposefully toward the implementation of a successful CTEM strategy and lower the risk of a breach.

Continuous Threat Exposure Management (CTEM) is as a cyclical set of processes and capabilities that enable enterprises to evaluate the accessibility, exposure, and exploitability of their digital and physical assets continually and consistently.

This programmatic approach that encompasses scoping, discovery, prioritization, validation, and mobilization. These steps provide actionable outcomes and to align closely with what is important to the business, ensuring that security efforts lead to tangible risk reduction.

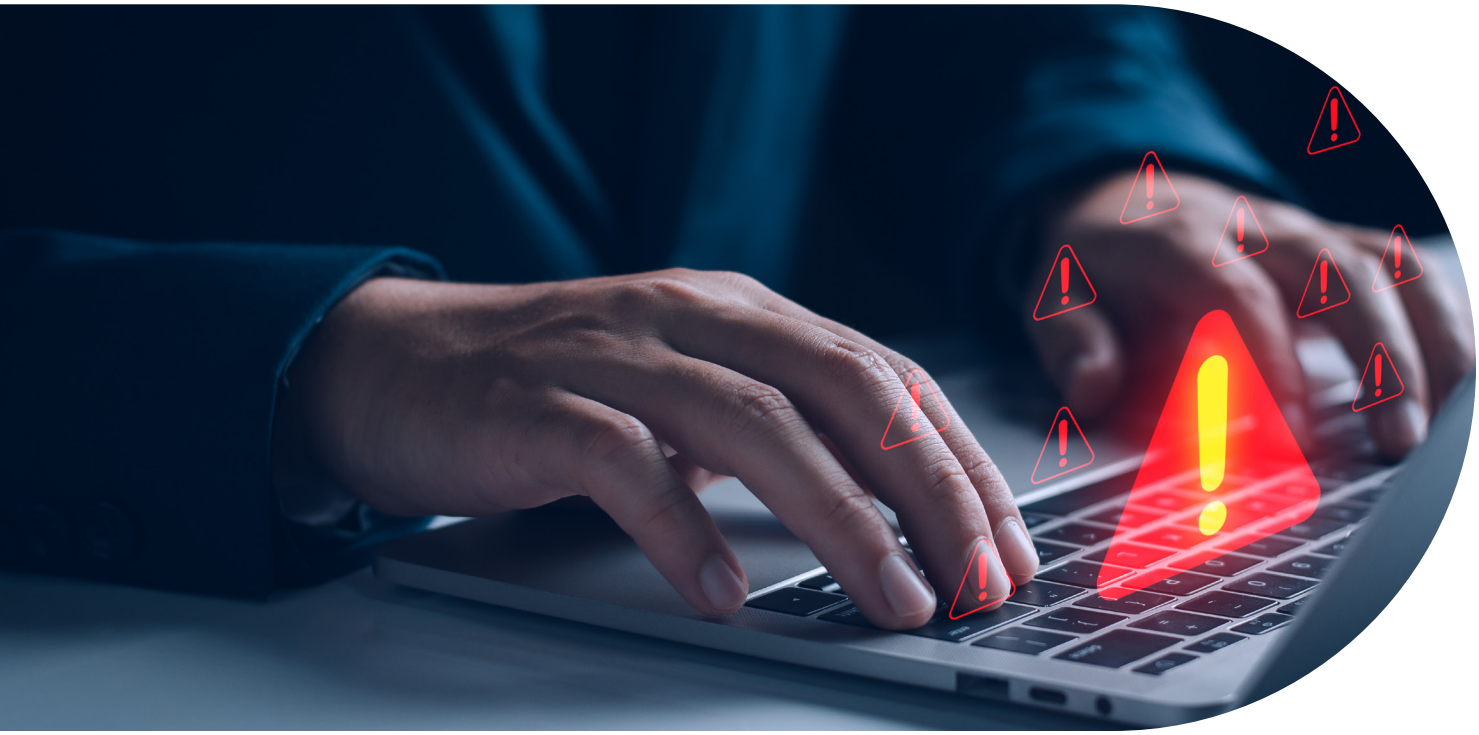
[1]*Addiscott, Richard, et. al. (2024, January 4). Top Trends in Cybersecurity for 2024. Gartner.*

Introduction to Continuous Threat Exposure Management

Continuous Threat Exposure Management (CTEM) has caught the attention of analysts and industry leaders alike, and for good reason. As organizations grow and evolve, so does the complexity of their digital environments. Meanwhile, threat actors have become increasingly more sophisticated and adept at breaching systems through vulnerability exploitation. Traditional vulnerability management tools buckle under the load of alerts. That is where CTEM steps in.

CTEM is not just a set of tools; it is a whole strategy. Think of it as a five-step dance that keeps your business in rhythm with your security initiatives. When implementing CTEM, you start by scoping out your digital terrain, discovering what is at risk, and where your systems offer potential entry points to would-be attackers. Next, you prioritize—because not all risks are created equal. First, you secure the most critical assets by aligning potential risks to your business needs and goals. After that, you validate your defenses, then finally mobilize to patch up weaknesses, starting with the highest priority items first. Then, you start the process over so that exposure management becomes a continuous cycle that adapts to new assets and emerging threats.

A critical difference between CTEM and its predecessors is its focus on people. Automated security tools are great—but only if all stakeholders understand the value they are providing and why they are important. The CTEM approach provides continuous, measurable data, focused through a lens of business context, that organizational leadership can use to quantify cyber risk management investments. Additionally, CTEM cuts through the noise and volume of vulnerability data to offer clear prioritization and implementation steps for operational teams. This continuous feedback loop between analysis, action, and proof delivers tangible, ongoing evidence that your security practices are actively protecting your business.



Introduction to Continuous Threat Exposure Management (continued)

Benefits of Adopting a CTEM Strategy

CTEM offers a strategic approach to cybersecurity that reduces the risk of breaches, aligns security efforts with business priorities, enhances resilience, and fosters a collaborative environment for managing cyber risks. With careful CTEM alignment and the right tools in place, organizations realize significant benefits that help navigate the complex and dynamic threat landscape.

The business benefits of CTEM are multifaceted and can significantly enhance an organization's cybersecurity posture. Here are some key advantages:

Proactive Risk Management

CTEM enables organizations to stay ahead of threats by continuously identifying and assessing vulnerabilities. This proactive stance helps prevent breaches before they occur, reducing the potential for damage and the costs associated with incident response.

Prioritized Risk Reduction

With CTEM, organizations can focus on the most critical risks first, ensuring that resources are allocated effectively. This prioritization is crucial in managing the vast number of vulnerabilities and active exposures organizations face today.

Enhanced Cyber Resilience

By adopting CTEM, organizations can build a more resilient security infrastructure that can more quickly adapt to and recover from cyber incidents. This resilience is key to maintaining business continuity in the face of evolving threats.

Actionable Insights

CTEM provides the data that security teams need to make informed decisions about how to protect their assets. These insights derive from continuous analysis and assessment of changing business assets and the evolving threat landscape.

Better Business Alignment

One of the main benefits of CTEM is its focus on alignment between security measures and business objectives. By understanding the business context of cyber risks, CTEM ensures that security efforts tie directly into protecting the organization's most critical assets and processes.

Adaptability

CTEM's flexible framework allows organizations to adapt their security strategies as new threats emerge and the business evolves. This adaptability is essential for staying relevant in a rapidly changing cyber environment.

Strategic Decision Making

CTEM empowers executives to make strategic decisions regarding risk management. With a clear understanding of the impact of cyber risks on business operations, leaders can choose to remediate, mitigate, or accept risks based on informed assessments.

Cross-Team Collaboration

Implementing CTEM requires collaboration across various teams, fostering a culture of shared responsibility for cybersecurity. This collaboration gives voice to all key stakeholders to ensure effective threat exposure management.

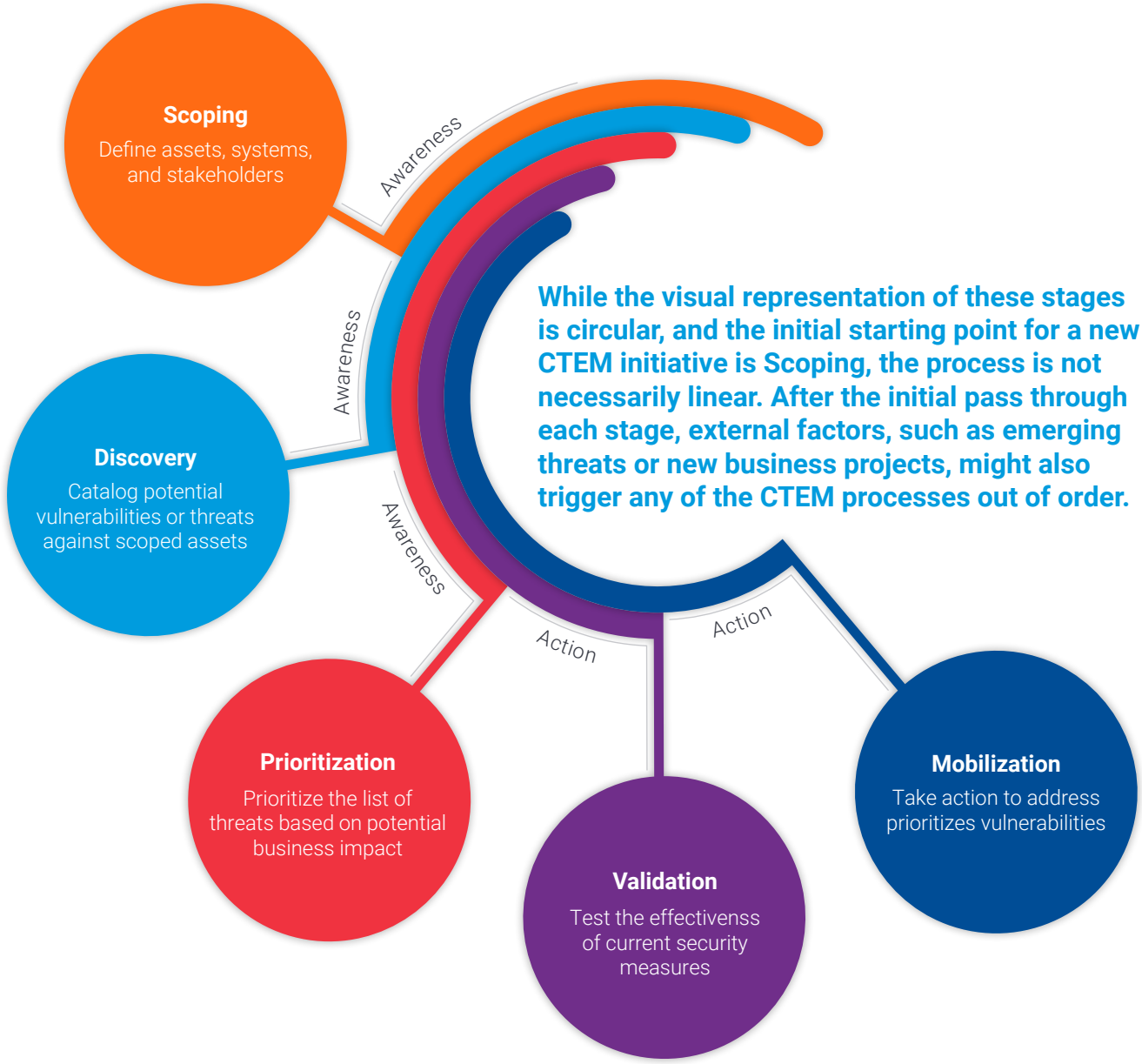
Security Maturity Optimization

CTEM goes beyond traditional patching and signature-based defenses. It enables organizations to optimize their security posture in ways that mature independently from the CTEM program itself, providing long-term benefits.

Introduction to Continuous Threat Exposure Management (continued)

How CTEM Works

Breaking down CTEM into its five stages—scoping, discovery, prioritization, validation, and mobilization—helps organizations manage and navigate the complex process of threat exposure management in a structured and systematic way. Each stage has a specific goal, expected outputs, and triggers that indicate when to begin each stage, ensuring a comprehensive approach. This helps teams raise awareness of risks through diagnosis and then act based on evidence. The five process stages of CTEM provide a cyclical and comprehensive approach to managing cybersecurity risks.



While the visual representation of these stages is circular, and the initial starting point for a new CTEM initiative is Scoping, the process is not necessarily linear. After the initial pass through each stage, external factors, such as emerging threats or new business projects, might also trigger any of the CTEM processes out of order.

Introduction to Continuous Threat Exposure Management (continued)

Here is a brief description of the goal, output, and triggers of each of the five stages of CTEM:

	Goal	Outputs	Triggers
Scoping	Define the boundaries of the CTEM program, including which systems, assets, and stakeholders are involved.	A clearly scoped outline that includes all assets and areas covered by the CTEM program.	New business initiatives, acquisitions, mergers, or other organizational changes.
Discovery	Identify and catalog potential weaknesses and risks relating to assets within the CTEM scope.	A contextualized inventory of assets that outlines potential vulnerabilities, threats, and risks.	Identification of new assets or changes to existing assets.
Prioritization	Address the identified vulnerabilities to determine which pose the greatest risk to the organization.	A prioritized list of outstanding risks and exposures.	Discovery of new vulnerabilities, active exploitations, threat actor group movements, threat intelligence, zero-day events, and critical patch alerts.
Validation	Evaluate the effectiveness of current security measures and determine the likelihood of attack success and analyze and predict attack paths that could lead to high-priority assets.	A report that confirms the findings of the prioritization stage and validates the efficacy or deficiency of existing controls.	Completion of prioritization or the introduction of new security controls or measures.
Mobilization	Act against prioritized vulnerabilities. This can include patching, implementing new security controls, implementing remediation recommendations, and/or documenting accepted risks.	Dashboards and reports that demonstrate the changes made to security, along with measurable impact of each of those changes.	The findings of the validation stage or an active security incident.

CTEM and Your Security Stack—Getting the Most from Your Investments

As you put together your CTEM program, keep in mind its inherent adaptability. The power of CTEM is its ability to help you achieve the greatest risk reduction possible within the capacity of your existing investments and resources. Chances are, you already have much of what you need in-house. Once your CTEM program becomes integral to your overall security strategy, the evidence it produces will help you make informed decisions for new tools and staffing to fill gaps based on quantifiable metrics.

The integrated security stack in CTEM is central to the strategy. It is a sophisticated blend of technologies that work together seamlessly to automate and enhance the CTEM process. Here is how it works:

Automation and Enhancement

Design your security stack to do the heavy lifting of security operations, automating the scoping, discovery, prioritization, validation, and mobilization stages as much as possible. This means that instead of manually sifting through data, security teams can rely on dashboards and reports that flag potential issues, prioritize alerts, and offer ranked recommendations that streamline the remediation process.

Actionable Remediation Guidance

It is not enough to identify threats; you need a clear path to deal with them. With the right data points derived from your existing vulnerability scanners, inventory management, and configuration management database (CMDB) solutions, you can derive actionable remediation guidance. These contextualized, business-aware data points provide options and strategies to tackle vulnerabilities effectively.

Integration with Threat Detection and Response

Your security operations center (**SOC**) relies on your security stack and related intelligence feeds to provide a real-time view into threats against your systems. A CTEM program standardizes how these teams receive exposure data and exploit intelligence, which allows them to respond quickly and with greater confidence. The result in an enhanced security posture built on top of prescriptive, trusted processes.

Supporting Human Involvement

While automation is a key feature, the security stack enhances and supports human expertise. Your security professionals use your tools and the information they provide to make informed decisions and take decisive action. It is a partnership where technology and human expertise work hand in hand to protect the organization.

Continuous Improvement

One of the biggest benefits of CTEM across an integrated security stack is that it represents a designed focused on continuous improvement. As new threats emerge and technologies advance, you will have evolving data points that will inform strategic decision-making so that you stay ahead of the curve. CTEM and its foundational technologies form a living system that grows and adapts to the organization it protects.

The integrated security stack in CTEM is a powerful ally in the ongoing battle against cyber threats. It is smart, responsive, and an essential component of any robust CTEM strategy.

CTEM and Your Security Stack—Getting the Most from Your Investments (continued)

Reactive or Proactive Measures? How About Both.

Cybersecurity strategies have shifted from reactive to proactive and back again. Is it better to shrink your Time to Detect (**TTD**) and Median Time to Respond (**MTTR**)? Or is it better to close the gaps so that there is nothing to respond to in the first place? The truth is that an effective security strategy contains a healthy blend of both reactive and proactive measures. You cannot plan for every threat, but you can make informed decisions that reduce risk while also improving your response to attackers who find their way around your defenses.

CTEM is about assembling the right team and using the right tools to optimize both active threat exposure management and proactive cyber defense.

CTEM as Active Threat Exposure Management

Exposure Management is a programmatic approach focusing on risk, threat identification, and ongoing remediation. But it goes beyond traditional vulnerability patching—it is not just about closing the gaps. It is about making sure they do not open back up in the future. Your automated vulnerability scanners, asset discovery tools, and risk-based prioritization technologies all enhance human efforts for the identification of potential exposures and response to real-time incidents and zero-day events.

Certain security tools in your tech stack may even be able to take over the repetitive tasks of scoping, discovery, prioritization, validation, and mobilization. Additionally, because the CTEM process hinges on built-in validation, you can trust the credibility of active alerts. This means response teams act faster, cutting down the TTD and MTTR so they can stop attacks before they cause any real damage.

CTEM as Proactive Cybersecurity Defense

With automated, risk-based, contextualized analysis, teams following a CTEM program become adept at finding and remediating risks before they become opportunities for adversaries. This proactive strategy gives you a significant advantage over unknown threats simply by approaching defense through that lens of business context.

When you mitigate and remediate potential risks to your highest-value assets first, you ensure that those assets remain protected, no matter how or when an adversary strikes.

CTEM and Your Security Stack—Getting the Most from Your Investments (continued)

What's in Your Stack?

When it comes to cyber security, there is a tool for everything. CTEM is not a tool in and of itself but rather a strategy that integrates tools and processes to produce the data you need. The following tools and services offer CTEM coverage across the continuous discovery, assessment, prioritization, validation, and mobilization stages so you can reduce exposure across digital estates. It is important to integrate these tools into a cohesive security stack that aligns with your organization's specific needs and threat landscape.

Asset Inventory and Categorization: A comprehensive asset inventory and assessment gives you contextualized analysis and risk profiling of assets so you can determine the potential business impact of a breach. Your asset inventory should provide a continuous view into the risk profile of each of your assets based on business context, multi-vector threat analysis, and vulnerability scan data.

Coverage Gap Analysis: Continuous discovery of endpoint, vulnerability, and asset coverage gaps ensures you do not miss potential security holes. You cannot secure what you do not know is there. Tools that provide this gap analysis allow you to deploy agents, install the latest patches, upgrade, or remove unpatchable systems, and prioritize fixes based on potential impact to the organization. Also, be sure to account for coverage of external assets or those exposed to or impacted by third-party vendors.

Vulnerability Prioritization and Management: To stay ahead of exposures, you need timely analysis of vulnerability scans, effective patch management, and rapid response to zero-day and weaponized attacks. Furthermore, with asset criticality ratings as a primary data point driving vulnerability prioritization, you can make informed decisions on where to patch first to reduce the most risk.

Risk Assessments: Regular risk assessments compared against industry frameworks, target maturity measures, and peer benchmarks can help you make purposeful, data-driven decisions for tool and process improvements.

Cyber Risk Register: A Cyber Risk Register is a centralized, customized risk visibility and reporting dashboard that demonstrates security maturity and posture through a lens of business context. Having a Cyber Risk Register in place helps you understand and manage unique business risks specific to their impact on the organization, qualify existing tool efficacy, and quantify risk reduction over time.

The Challenges of Standing Up a CTEM Program

Like any new program or strategy, organizations face challenges and barriers when starting down the path toward CTEM. In many organizations—especially those that are large or disbursed—security, operations, and leadership operate on different assumptions or in departmental or geographic silos. As seen above, alignment with a CTEM strategy provides significant risk reduction benefits. Organizational leadership might be asking some pointed questions regarding the achievability of a new CTEM program. When faced with these questions, here is some guidance on how to answer them to get started on a solid footing.

How can we align our security and non-security teams?

One of the primary challenges you will face in standing up a CTEM program is achieving alignment between non-security and security teams. Communication gaps often exist between IT infrastructure, DevOps, security, and business units, leading to confusion about ownership, lack of alignment on expectations, and other issues. To overcome this challenge, organizations can foster a culture of collaboration and ensure the establishment of clear communication channels. Regular cross-functional meetings and unified security frameworks can help bridge these gaps. Additionally, clearly defined and communicated roles and accountability check-ins can help teams accept ownership over their new responsibilities.

Before we make changes, do we have a decent understanding of our current security posture?

Creating a comprehensive view of an organization's security posture requires both a breadth and depth of knowledge across multiple teams. A CTEM program encompasses any area of the business that could potentially lead to asset exposure. Therefore, it is imperative to know what tools, controls, and processes you have in place across assets, networks, endpoints, clouds, and devices. You also need to understand the pros and cons of your current solution. Addressing this challenge requires two separate initiatives. You can use integrated tools that provide visibility across all assets and vulnerabilities, ensuring a unified approach to threat management. Additionally, you can conduct a framework-aligned risk assessment to identify your security maturity, strengths, and weaknesses.

We are already drowning in diagnostics. Will CTEM add more dashboards and metrics that we need to manage?

Managing diagnostic overload is also a significant challenge. The volume of data and alerts generated by various security tools can be overwhelming. Organizations can implement smarter—not full—automation to manage this overload. By designing a program that operates a broader set of exposures and establishing regular, repeatable cycles without contributing to alert fatigue, organizations can ensure consistent threat exposure management outcomes.

How do we delegate responsibilities when these teams have never had to deal with exposure management?

Prioritized lists alone are rarely enough to mobilize and motivate non-security teams. Yet delegating the remediation of risks to asset and application owners is an effective way to increase security awareness and improve overall business processes. Organizations should include non-security stakeholders in discussions and decisions related to risk management and assign accountability to those stakeholders over their areas of control. This ensures that exposure management outputs are visible across cross-functional teams and that risk reduction efforts become a shared goal and metric. By aligning the scopes of exposure assessment cycles with specific business projects, security becomes an integral part of each stakeholder's job and set of responsibilities.

The Challenges of Standing Up a CTEM Program (continued)

Everything changes so fast—our environment, threats, vulnerabilities, and exposures—will CTEM really maintain and improve our security posture, or is it just another buzzword?

Maintaining a dynamic and current security posture over time is key to risk reduction. But you cannot get there with antiquated processes and tools. The secret to a mature program that keeps pace with change is the creation of strong workflows that rely on the automation of both analysis and remediation. Organizations should establish regular, repeatable cycles as part of their CTEM program and adhere to the five-step process—scoping, discovery, prioritization, validation, and mobilization—to guarantee consistent outcomes. They should clearly define trigger events that require action, along with key stakeholders, expected outcomes, and timelines.

We can barely keep up now. How are we supposed to implement CTEM with the current level of expertise and resources we have?

In an industry plagued by an ongoing resource shortage, most organization need better strategies to improve outcomes with limited staff, budgets, or both. While a lack of expertise and shortage of resources can hamper efforts to provide effective cyber risk management, the inherent flexibility of CTEM provides a foundation for using what you have and growing your maturity over time. Your organization can start with only a portion of your assets or teams—those that inherently pose the most risk if breached.

Some examples would be payment processing systems, data processing systems that manage personally identifiable information (**PII**), or those systems that house corporate intelligence or proprietary information. By working with a smaller but more valuable subset of your overall asset landscape, you can prove value and make the case for a more extensive, wider implementation of CTEM.

By addressing these challenges with strategic planning, clear communication, and the right tools, organizations can successfully implement a CTEM program and enhance their cybersecurity defenses.

Getting Started with CTEM

Initiating a CTEM program begins with understanding the strategies for starting and maintaining ongoing exposure management. This involves a programmatic approach encompassing scoping, discovery, prioritization, validation, and mobilization. These steps provide actionable outcomes that closely align with what is important to the business, ensuring that security efforts lead to tangible risk reduction.

Not many organizations can implement wholesale process change, nor is it necessarily wise to try to convert your entire vulnerability and risk management strategy to CTEM all at once. You might end up widening gaps or creating new risks in the process. Here are a few best practices to keep in mind when moving forward with CTEM:

- ✓ **Set Clear Objectives:** Define what you want to achieve with your CTEM program. Your goals could include improved visibility into assets, better prioritization of vulnerabilities, cyber risk reduction, enhanced response to threats, improved cross-team ownership of cybersecurity, and more. Make your objectives measurable and assign clear ownership and timelines.
- ✓ **Develop a Workflow:** Establish a structured workflow that includes the five steps of a CTEM cycle: scoping, discovery, prioritization, validation, and mobilization. Use the tools you have in place to conduct activities throughout each stage of your workflow. This will help you identify coverage gaps while improving the ROI of your existing investments.
- ✓ **Inventory and Categorize Assets:** Use tools to inventory and categorize your assets and vulnerabilities. Focus on risk awareness—you want to determine which assets and systems pose the most risk to your organization. This analysis requires a combination of knowledge, including business context, vulnerability exploitation and attack tactics, potential attack vectors, likelihood of an attack, and more. Understanding what is at risk will offer insights into where to start and how to best prioritize your efforts.
- ✓ **Simulate and Test Attack Scenarios:** Regularly simulate or test attack scenarios to evaluate your defenses. This will help you identify additional weaknesses and areas for improvement.
- ✓ **Create an Actionable Path:** Ensure there is an effective and actionable path for infrastructure teams, systems, and project owners to act on findings. When you are first starting with CTEM, clear, documented communications standards and approval workflows are necessary. A well-defined communication path informs and empowers stakeholders to do their part successfully.
- ✓ **Start Small:** Conduct an asset inventory and visibility scan and determine which assets pose the greatest risk. Focus initially on the most critical assets and systems in your organization. Gradual implementation allows for smoother integration, proof of value, and better results.
- ✓ **Align with Business Objectives:** Include the five steps of CTEM—scoping, discovery, prioritization, validation, and mobilization—as part of a project or business initiative. This allows you to involve key stakeholders from the beginning of the project and tie CTEM responsibilities and outcomes to the project objectives.
- ✓ **Adapt to Changes:**
    1. Be prepared to adapt your CTEM processes to external factors such as new business initiatives, organizational changes, or emerging attack techniques.
    2. If you start small, create a plan for expanded CTEM coverage and involvement across your organization.
    3. Remember, CTEM is cyclical by nature. By keeping adaptation in mind, you will continually refine, improve, and expand your processes to naturally encompass new assets and defend your organization against emerging threats.

Conclusion

Continuous Threat Exposure Management (CTEM) has emerged as a powerful strategy that helps organizations overcome the mounting challenges of cybersecurity. The strategic adoption of CTEM is not just a trend but a transformative process leading to a more secure future. As we have explored in this whitepaper, the benefits of CTEM are clear and measurable, offering a path to significantly reduce cyber threats and align security operations with dynamic attack surfaces and continuously emerging vulnerabilities and threats.

The five-step CTEM approach provides a structured and effective methodology for organizations to proactively manage their cybersecurity risks. By scoping, discovering, prioritizing, validating, and mobilizing, organizations can ensure that their security measures are both comprehensive and tailored to their specific needs.

While challenges may arise implementing a CTEM strategy, they are not insurmountable. With cross-functional ownership and data-informed decision-making, organizations can overcome these hurdles and emerge stronger and more resilient.

As we look to the future, the promise of CTEM is not just the reduction of breaches but also the empowerment it offers organizations. CTEM equips cross-functional teams with the tools and knowledge to take control of their cybersecurity, making informed decisions that protect their assets and stakeholders.

We encourage you to apply these insights within your organization. The journey towards a successful CTEM strategy is well within reach, and the rewards are significant. With the right approach and commitment, your organization can achieve a level of cybersecurity that protects your assets and enhances business operations. By following the process outlined above, CTEM can become your key strategy for creating a safer, more secure organization.

Gain Rapid CTEM Alignment with Key Critical Start Capabilities

For security leaders seeking proactive exposure identification and optimized security operations, Critical Start MDR offers human-driven 24x7x365 investigation and true response mitigation across IT and OT environments. Our flexible deployments, backed by contractual SLAs, integrate proactive security intelligence through a transparent platform and mobile app. This comprehensive approach ensures threats and risks are identified, minimizing breach likelihood and impact, preventing business disruption, and driving improved SOC outcomes to enhance the productivity of your security operations.

- Endpoint and vulnerability coverage gap detection and SIEM log health monitoring to ensure the SOC is receiving all threat signals.
- Comprehensive, continuous asset inventories with criticality ratings that categorize risk impact based on business function.
- The most flexible deployment models that support all IT and OT threat types & log sources to consolidate security monitoring, detection, and response regardless of tools integration.
- Human-driven investigation and true response mitigations with contractual SLAs.
- A turn-key Vulnerability Management Service with Vulnerability Prioritization that streamlines and simplifies patching.
- A trust-oriented approach to resolving false positives and identifying benign true positives.

Conclusion (continued)

Learn more about how Critical Start can serve as a foundational element for your CTEM program. Contact us for a customized demonstration.

Further Reading:

- Asset Visibility in Cybersecurity | Myths, Dos and Don'ts, and Strategic Insights
- Simplify Vulnerability Management with Critical Start
- Risk Assessments: The Hidden Key to Continuous Security Improvement
- The Hidden Risks: Unmonitored Assets and Their Impact on MDR Effectiveness
- Threat-aware Vulnerability Prioritization

For more information, contact us at:
https://www.criticalstart.com/contact/