Hive Pro®

Whitepaper

A Comprehensive CTEM Guide for CISOs

Table of Content

Introduction

Traditional approaches to vulnerability management are proving insufficient. CISOs cannot rely on current trends in vulnerability management to yield success moving forward. The Continuous Threat Exposure Management (CTEM) framework from Gartner provides a timely solution, enabling organizations to take a broader and more comprehensive view of their security posture. CTEM is a dynamic, holistic process designed to address the full scope of potential threats and vulnerabilities, ensuring a proactive and agile security strategy. By shifting focus from mere vulnerabilities to a complete understanding of exposure, CTEM offers a structured, continuous, and actionable framework for enterprises. This whitepaper explores the concept of CTEM with the purpose of educating CISOs and offering valuable insights on implementation.

Defining CTEM

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

Where RBVM Falls Short

Risk-based vulnerability management (RBVM), a longstanding approach to conquering vulnerability reduction, misses a key point: exposure extends beyond vulnerabilities. Exposure is any weakness that enhances the feasibility with which an attacker can infiltrate your organization. The weaknesses that must be addressed beyond vulnerabilities are security findings, misconfigurations, inadvertently exposed digital assets, obsolete technology, and the human element. In fact, 45% of surveyed professionals agree that their lack of a common view of applications and assets across security and IT teams causes a major delay in the vulnerability patching process.

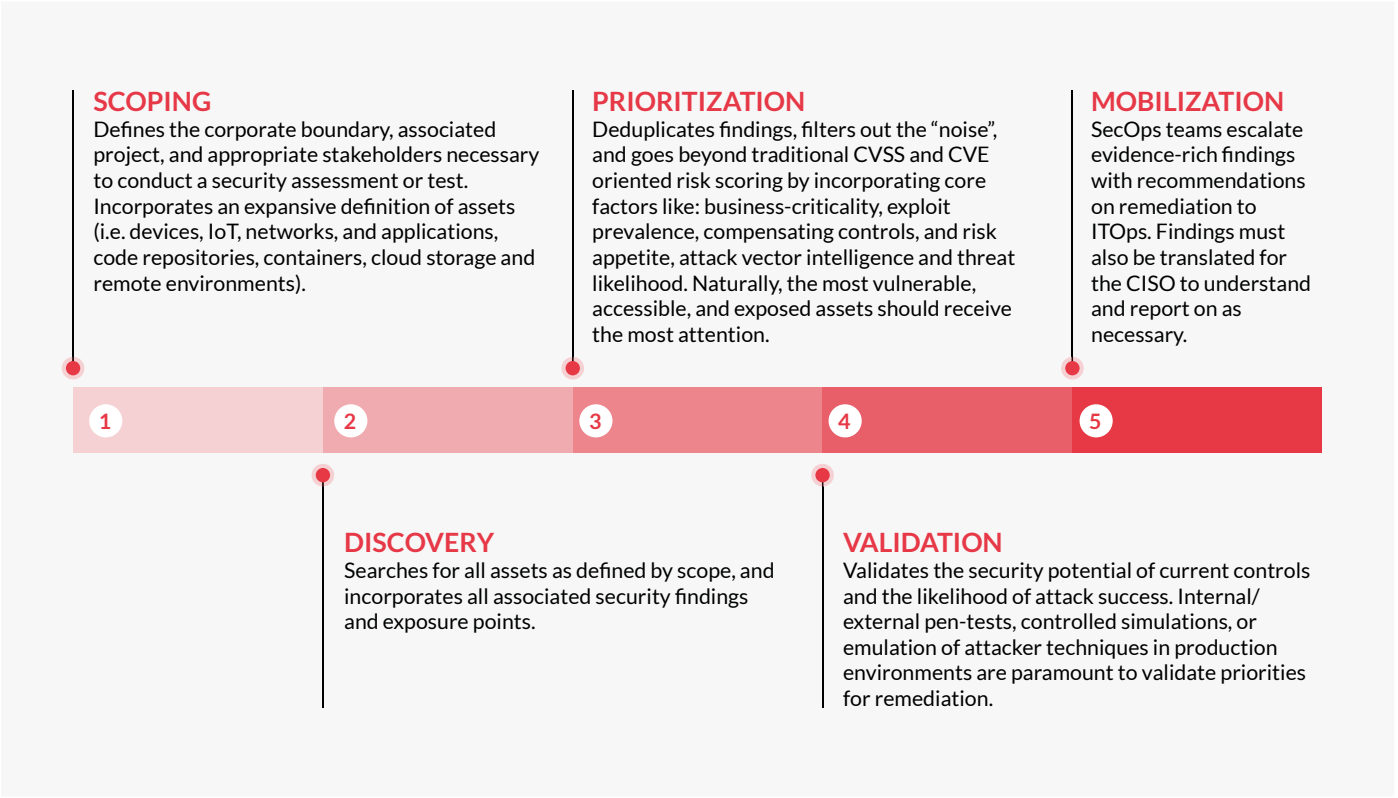
In sum, the aforementioned weaknesses comprise an organization's attack surface. To limit the exposure of their attack surface and to further reduce it, Security teams must have adequate visibility of the terrain, a means to protect it, and a strategic outlook on enemy action, or the "attacker's perspective". Unfortunately, most Security teams face challenges with all three requirements, leaving CISOs at the helm of a tenuous future.

How CTEM Helps Security Functions

Even with following RBVM alone, Security teams struggle with compounding open vulnerabilities, long lists of generic remediations, a limited workforce, siloed security tools and as a result, security findings sprawl. On average, it takes 20+ minutes to manually detect, prioritize and remediate each exploitable vulnerability. Additionally, 45% of surveyed professionals claim that siloed tools cause delays in remediation. These numbers say that even with the limited visibility they have of their exposed attack surface, Security teams are in urgent need of change and improvement.

The Continuous Threat Exposure Management (CTEM) framework was created to remedy the issues described above through a 5-step process emphasizing a path towards complete attack surface visibility and management, purpose-built for all stakeholders involved in vulnerability management, including the CISO whose responsibility it is to report on such findings with confidence and assurance in cyber resiliency.

Here's a very brief summary of the 5-Step Process:



What makes CTEM different from RBVM according to the process above? The incorporation of threat intelligence, exploitation likelihood, and security validation to preempt attacks and remediate the security findings that matter. It's typical for a Security organization to keep their Red and Blue teams, or their general security analysts and threat analysts apart. CTEM is asking for CISOs to incorporate findings from these normally siloed functions to build for true resiliency. Simple enough. Though how do CISOs benefit in the short and long term?

CISOs – Why Should You Care?

Below is how CTEM enables the the top 5 priorities of CISOs:

- **Build A Security Strategy and a Defensible Security Architecture:** Any good Security Strategy meets the business' objectives and risk outlook with an amenable security strategy and architecture–one that protects the enterprise while still enabling growth.

  By offering a holistic view of both internal and external attack vectors, CTEM addresses visibility gaps, ensuring comprehensive insights into potential threats. This data-driven approach permits proper resource allocation, focusing on high-risk zones, thus remedying necessary gaps and optimizing costs. Siloed operations, a common challenge, are eliminated as CTEM integrates diverse security measures for a unified front. It not only enhances collaboration among tools and teams but also counteracts the skills shortage by automating tasks and leveraging existing assets. CTEM's adaptable framework meets any Security strategy by ensuring preparedness for future challenges and reinforcing a proactive stance in the changing threat landscape.

- **Manage Cyber Risks:** CISOs must routinely and confidently evaluate, mitigate, and communicate security risks (exposure, vulnerabilities, potential impact, compensating controls, Security function needs, etc.) to both technical and non-technical stakeholders. Lagging indicators in risk are never helpful for reporting.

  CTEM empowers CISOs to adeptly manage cyber risks by fostering a proactive security stance. Instead of a traditional reactive approach, which addresses threats post-exploitation, CTEM identifies and counters high-risk security findings in advance. By shifting to continuous evaluations of Security posture through means of automation and better collaboration, CISOs are afforded the closest to a real-time reflection of the threat environment they can get. This continuous vigilance not only combats current threats but also builds resilience against forthcoming challenges. By detecting threats early, CTEM curtails response times, ensures swift mitigation, arms CISOs with leading indicators in risk tha they can feel confident to report on, and ultimately minimizes the potential impact of breaches if they are to occur.

- **Ensure Governance and Security Compliance:** CISOs must maintain continuous organizational compliance with relevant industry regulations, standards, and laws related to information security. Every compliance measure requires the creation of a sound vulnerability management program and measures to combat threats.

  CTEM provides a structured approach to meet this need with greater efficiency than any program before it has, as demonstrated in earlier portions of this paper.

- **Collaborate with Other Executives & Reporting on Security Metrics:** CISOs must build for Security while preventing friction across their C-level peers. To build for cross-functional harmony and to provide assurance, constant communication and justification for action is necessary.

CTEM enables CISOs to report on top-line remediation priorities that may cause downtime for functions but all for good reasons, enough to inspire their peers to adjust to Security needs to benefit the enterprise. CTEM also inspires collaboration across every step, while keeping top of mind that combating and/or preventing threats is a shared pursuit in the enterprise. Additionally, the continuous monitoring and metrics provided by CTEM allow for clearer demonstration of the value derived from security investments.

By integrating the CTEM framework into their Security programs, CISOs not only enhance their security posture but also align their cyber strategies with evolving business needs. As the threat landscape continues to grow in complexity, CTEM offers a proactive and agile solution, ensuring that CISOs remain at the forefront of enterprise security, safeguarding their organization's assets, reputation, and future.

What Tools Are Best Fit for CTEM

The tools best fit for organizations building a CTEM program will accomplish each step sufficiently: from inventorying and categorizing assets, to surfacing exposure points, correlating threat, and vulnerability intelligence with asset intelligence, to simulating or testing attack scenarios, fostering collaboration across relevant teams, and driving vulnerability remediation.

The following tools have been instrumental meeting parts of CTEM:

EASM (External Attack Surface Management):
Gives CISOs a clear view of all digital assets exposed to the internet.

CAASM (Cyber Asset Attack Surface Management):
Offers insights into the internal threat landscape, ensuring that all assets, including IoT, OT, and shadow IT, are covered.

CNAPP (Cloud Native Application Protection Platform):
Platform encompassing Cloud Security Posture Management, Cloud Service Network Security, and Cloud Workload Protection Platforms to provide a complete security visibility, control and protection to cloud-native workloads across public and private clouds.

VA (Vulnerability Assessment):
Helps identify weaknesses in the system, ensuring that the CISO is always aware of potential vulnerabilities.

VPT (Vulnerability Prioritization Technology):
Ensures that resources are directed towards the most critical vulnerabilities that could have the biggest impact on the organization, rather than wasting time on low-risk vulnerabilities.

BAS (Breach and Attack Simulation):
Allows CISOs to simulate cyberattacks in a controlled environment, helping to understand attack effects and to identify areas for improvement.

PTaaS (Penetration and Testing as a Service):
Offers on-demand testing services that can be scaled based on organizational needs, making it cost-effective.

Patch Management:
Automates the acquiring, installing, and verifying patches (or updates) for software applications and systems.

ITSM and Ticketing Tool:
Facilitates the management and delivery of IT services. A ticketing tool tracks, manages, and organizes tasks, issues, and projects through a centralized platform.

Additionally, sources for threat intelligence, vulnerability intelligence, and patch & IOC intelligence are necessary feeders to keep a continuous pulse on exposure management. All tools must have some level of automation that helps to accomplish work in a smart and efficient manner. Reducing manual labor is one benefit; however a reliable, consistent, repeatable automation process with verifiable results is what matters most.

Where to From Here?

We recommend a general, step-by-step adoption of CTEM below.

- **Step 1:** Educate your Security organization in constructive discussions about CTEM and engage with peers on continuing the discussion. Additionally, if you have a Gartner subscription, please explore their research.

- **Step 2:** In the event that you and your team feel prepared to explore CTEM, review your current RBVM or VM program for rooms for improvement so that you can define clear objectives for what the CTEM program should achieve in alignment with your organization's risk appetite and business goals.

- **Step 3(a):** Begin a project-based review of your asset and vulnerability inventory and document associated stakeholders. Review assessment/scan cycles for process gaps/stalls in escalation and/or remediation. Document your sources for threat intelligence, method of prioritizing vulnerabilities, method to test security tools, and tools to escalate issues. All gaps should be noted. All tools in use should be documented and surveyed regarding efficiency and aptitude to meet CTEM requirements.

- **Step 4:** Host discussions with your ITOps team and relevant asset owners to discuss their suggested room for improvement. Explore tooling gaps and approach vendors who can fulfill a good majority of your needs from one platform, as tool sprawl is a trying problem for every organization.

- **Step 5:** Implement CTEM.

The Continuous Threat Exposure Management (CTEM) framework provides a timely solution for CISOs enabling their organizations to take a broader and more comprehensive view of their security posture, and to proactively combat threats. Now more than ever, CISOs need to build for proactive security to enable true cyber resilience.

About Hive Pro Uni5 Xposure

Hive Pro is recognized as a trusted vendor by leading analyst firms Gartner, Inc. and Forrester, affirming their industry expertise and reliability. Their flagship product HivePro Uni5 is now complemented by the Uni5 Xposure platform. Uni5 Xposure enables total asset exposure visibility and management by combining the strength of the HivePro Uni5 platform (asset discovery, AI-driven VPT, BAS, threat intelligence, patch intelligence and multiple integrations) with additional core capabilities like out-of-the-box total infrastructure scanning (code, web, mobile app, network, cloud, container), security assessment orchestration and workflow management, and actionable recommendations for remediation. Uni5 Xposure presents a unified and actionable view of threat exposure and risk across various evaluations to enable continuous cybersecurity assurance and resilience.

Hive Pro's corporate headquarters are located in Herndon, Virginia, with presence across the US, EMEA, and APAC.

Read more about Uni5 Xposure here .

To learn more about Hive Pro, visit www.hivepro.com.

Hive Pro®

Get in Touch

Hive Pro Inc. | info@hivepro.com | www.hivepro.com

Book a Demo

Read our Blog