noetic

How to Implement Continuous Threat Exposure Management (CTEM)

CTEM at a glance, Gartner® recommendations, and an overview of the Noetic solution

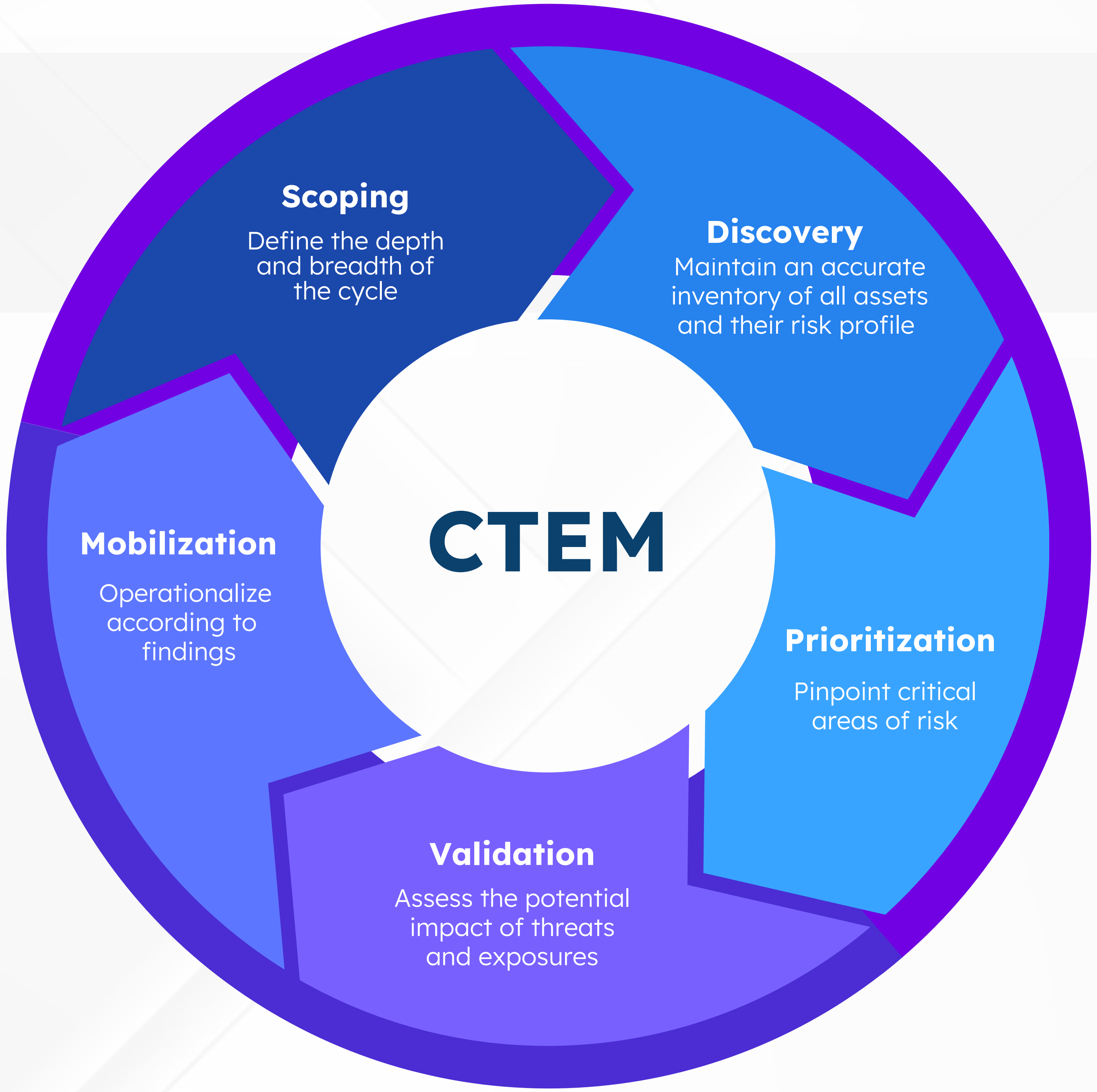
As the attack surface continues to evolve and expand, it's essential that organizations respond accordingly. Progressive cybersecurity programs consider attack surface management (ASM) a core component of a wider set of processes and capabilities known as continuous threat exposure management (CTEM).

> By 2026, organizations prioritizing their security investments based on a continuous exposure management program will be 3x less likely to experience a breach.

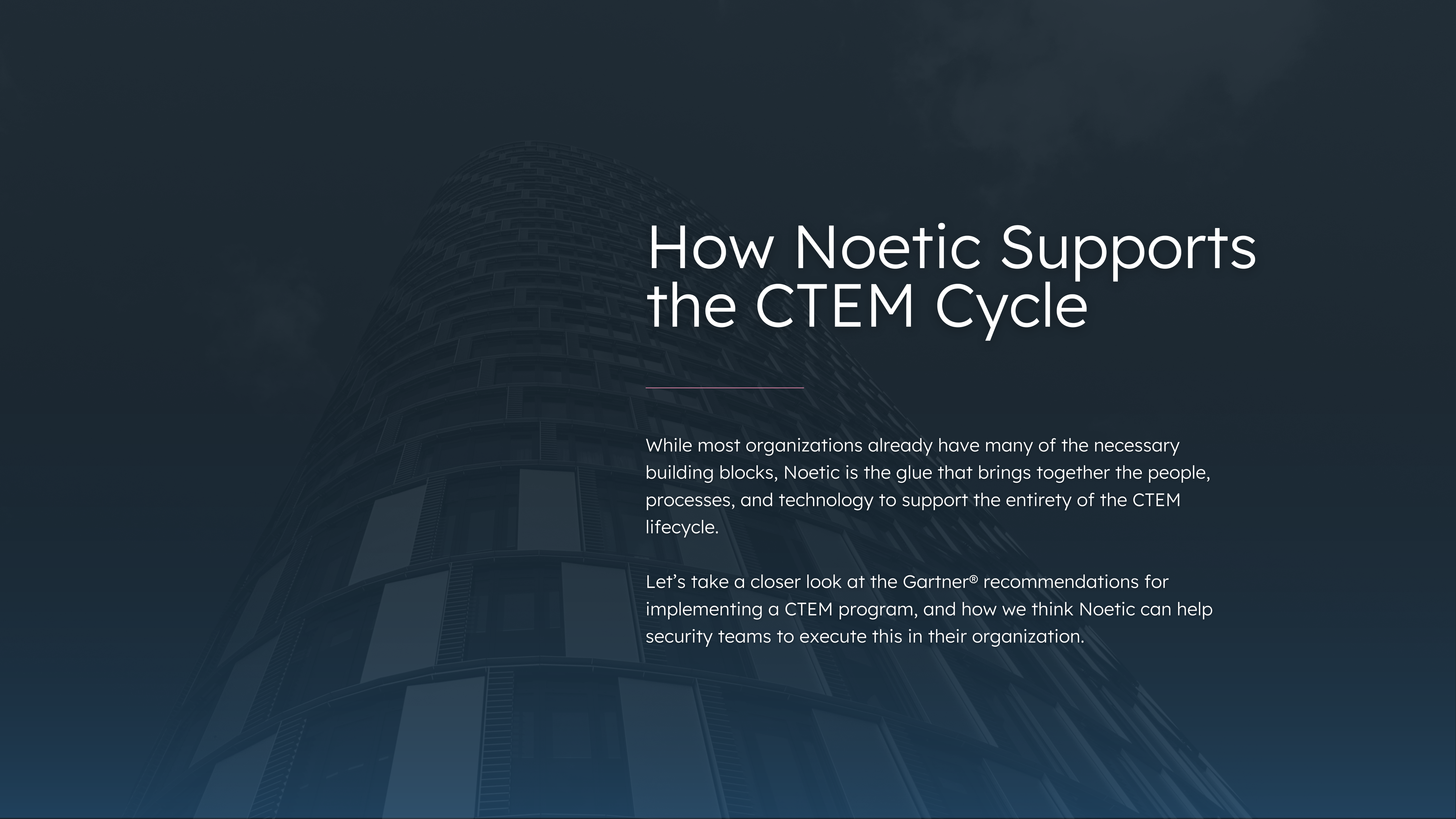
– Gartner®, Implement a Continuous Threat Exposure Management (CTEM) Program, July 2022

According to Gartner®, "A CTEM program is an integrated, iterative approach to prioritizing potential treatments and continually refining security posture improvements." When implemented correctly, CTEM programs produce the actionable insights security and risk leaders need to truly understand, reduce, and communicate risk as it pertains to the business—rather than just the traditional IT ecosystem.

Inherently, this empowers organizations to shift from a siloed, tool-centric vulnerability management practice into an integrated, scalable exposure management program that keeps up with the pace of the ever-expanding attack surface.



CTEM
Scoping
Define the depth and breadth of the cycle
Discovery
Maintain an accurate inventory of all assets and their risk profile
Prioritization
Pinpoint critical areas of risk
Validation
Assess the potential impact of threats and exposures
Mobilization
Operationalize according to findings



How Noetic Supports the CTEM Cycle

While most organizations already have many of the necessary building blocks, Noetic is the glue that brings together the people, processes, and technology to support the entirety of the CTEM lifecycle.

Let’s take a closer look at the Gartner® recommendations for implementing a CTEM program, and how we think Noetic can help security teams to execute this in their organization.

	Scoping	Discovery	Prioritization	Validation	Mobilization
Gartner® Recommendations	A CTEM program goes beyond self-inflicted vulnerabilities and also takes the “attacker’s view,” beyond the traditional common vulnerabilities and exposures.	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.	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.	While not limited to attackers’ techniques, the “validation step” often relies on manual assessment activities, such as red team exercises, to extend its reach.	At higher maturity, “mobilization” also requires an evolution of the tools to better integrate together so that they can deliver context to other parts of the organizations, such as the incident response team.
The Noetic Solution	Noetic helps teams effectively scope projects with a holistic understanding of both the business criticality and relationships associated with each individual asset. The intuitive graph interface maps business context together with technical data from existing security and IT management tools. Noetic also provides added flexibility to gain visibility into unique asset types critical to your security and risk posture by adding ad-hoc data from spreadsheets, legacy applications, and more.	Noetic enables teams to quickly discover and maintain an accurate registry of the environment by: • Automatically extracting data from any tool using agent-less API connectors, providing coverage for both cloud and on-premises assets • Continuously aggregates, correlates and deduplicates data within a single source • Enriches existing datasets with reference lists, providing added layers of business context	Noetic guides teams to prioritize critical threats and exposures according to multiple dimensions of insights, including: • Technical asset data from existing vulnerability scanners, ITAM tools, and more • Intra-asset relationships and interconnectivity • Third-party vulnerability intelligence on severity & exploitability from trusted sources such as MITRE, FIRST, NIST and CISA. • Relevant business context such as impacted users, sensitive data or business-critical applications. • Compensating security controls deployed	With Noetic, teams are better positioned to validate acceptable risk tolerance levels through attack path maps that identify potential lateral movement—or blast radius—of an event. Users can integrate external validation and breach attack simulation (BAS) tooling with Noetic to build these insights and processes into the Noetic graph database.	Noetic empowers teams to mobilize without friction. Users leverage Noetic’s bidirectional connectors and automation & workflow engine to: • Provide clean, validated metadata back into different systems of record • Create and resolve tickets in ITSM tools such as ServiceNow and Jira, • Trigger repeatable end-to-end automated actions such as initiating vulnerability scans or deploying endpoint agents.

Gartner® does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

GARTNER® is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Get started today with Noetic

🌐 noeticcyber.com/demo

✉ info@noeticcyber.com