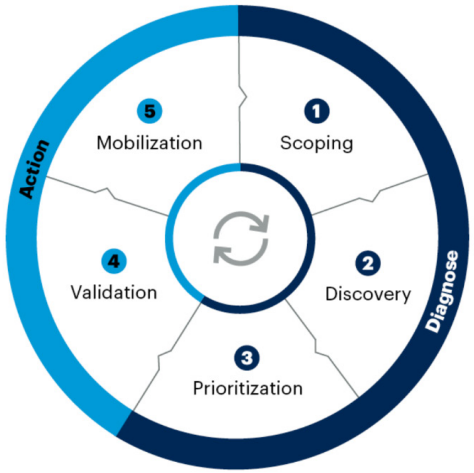
ARMIS® Gartner®

Aligning With Gartner® Guidance For An Effective CTEM Program

Cybersecurity professionals face immense challenges due to the constantly evolving threat landscape, sophisticated adversaries, and expanding attack surfaces. CIOs and CISOs struggle with an overwhelming number of weaknesses and hidden exposures, making it difficult to prioritize and effectively remediate risks. This lack of visibility provides ample opportunities for malicious actors to infiltrate networks. To combat these issues, Gartner recommends implementing Continuous Threat Exposure Management (CTEM).

Continuous Threat Exposure Management Process Phases



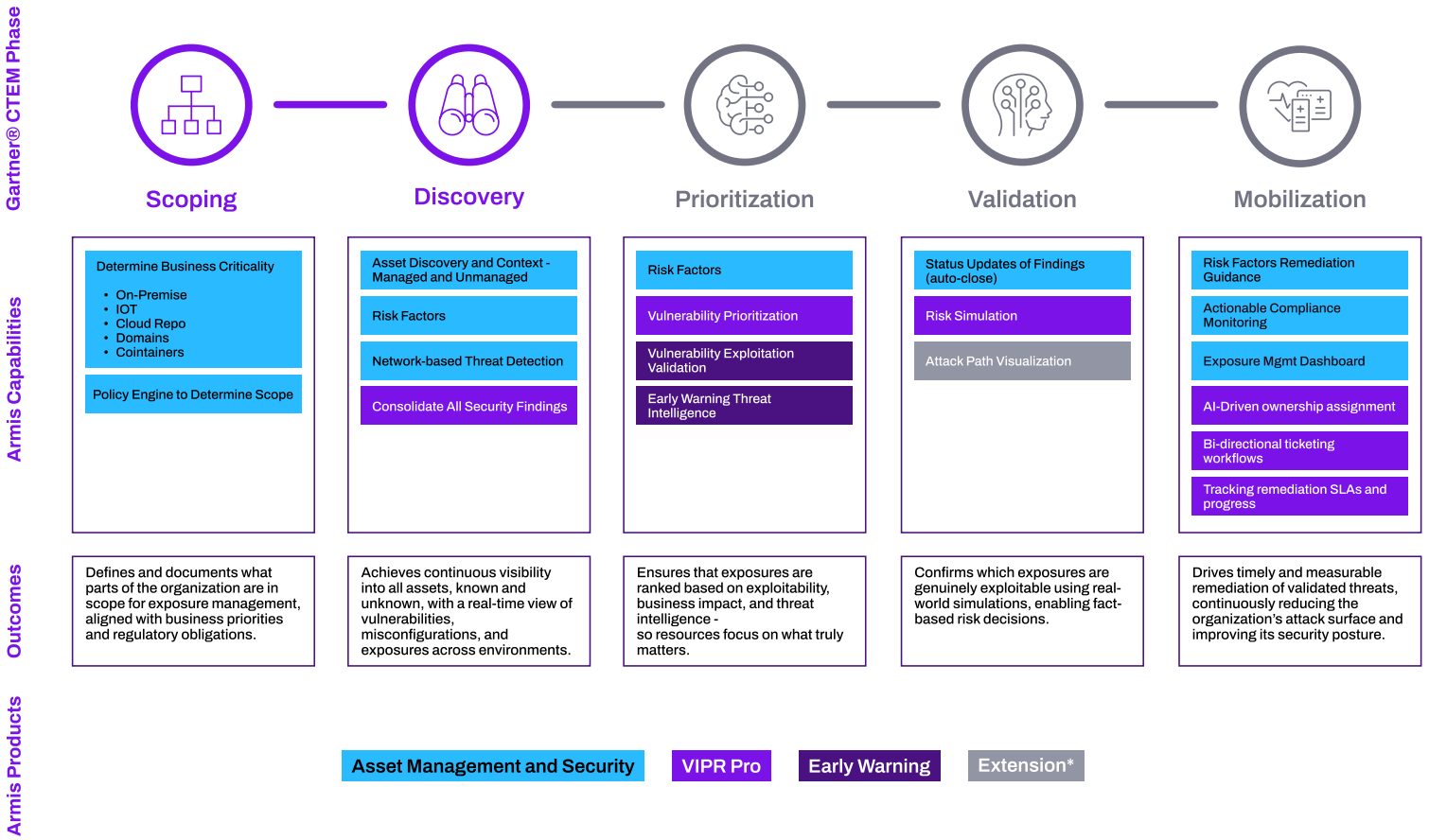
Source: Gartner
831705_C

Gartner

1. **Scoping:** During the scoping phase of CTEM, the initial identification and definition of assets are strategically aligned with business relevance from the outset.
2. **Discovery:** Using the information collected during scoping, target discovery at the relevant assets and risk profiles for that scope, strategically aligned with business relevance from the outset.
3. **Prioritization:** Prioritizing the treatment of exposures needs to be based on a combination of the urgency, severity, availability of compensating controls, risk appetite and level of risk posed to the organization.
4. **Validation:** The part of the process by which an organization can validate how potential attackers can exploit an identified exposure and how monitoring and control systems might react.
5. **Mobilization:** The objective of the mobilization effort is to ensure teams operationalize the CTEM findings by reducing friction in approval, implementation processes and mitigation deployments.

How Does Armis Contribute To a CTEM Program?

Organizations building a CTEM program leverage various tools to inventory assets, categorize vulnerabilities, and simulate attack scenarios. Armis Centrix™ enables an effective implementation of a comprehensive CTEM program, supporting the following core elements:



*please contact your Armis customer success or sales representative for more information on pricing and availability

Conclusion

We believe CTEM is set to revolutionize existing technology by converging cybersecurity validation and exposure assessment platforms. Platforms like Armis Centrix™ offer robust capabilities to facilitate the implementation of an effective CTEM program, empowering organizations to proactively manage and reduce their cyber exposure.

External Source: Use Continuous Threat Exposure Management to Reduce Cyberattacks

Ready To Learn More?

White Paper: Operationalizing a Risk-driven Continuous Threat Exposure Management (CTEM) Program

Playbook: Mastering Cyber Exposure Management & Security

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Visit Armis.com to find out more