CTEM Operationalization with Armis Centrix™

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

More Complexity, More Risk

Organizations face an increasingly daunting challenge to identify and fix cyber exposure risk. Amplifying this challenge is the growing breadth and complexity of the attack surface, incorporating IT, cloud, operational technologies, cyber-physical systems, and IoT assets, in tandem with a more sophisticated threat landscape—targeting not just traditional CVE vulnerabilities, but also exposures including cloud misconfigurations, runtime, code, and application issues.

To guide organizations with a structured and systematic approach to this challenge, the leading industry analyst firm Gartner developed the Continuous Threat Exposure Management (CTEM) framework. The CTEM framework "is a pragmatic and systemic approach organizations can use to continually evaluate the accessibility, exposure and exploitability of digital and physical assets."

Making CTEM a practical reality with the Armis Centrix™ Platform

By providing unmatched visibility, security, and control, Armis enables organizations to effectively manage their attack surface, prioritize and reduce their exposure risks, and maintain a sustainable and repeatable remediation lifecycle. Armis Centrix™ is a unified, cohesive platform to identify critical exposures and operationalize risk reduction.

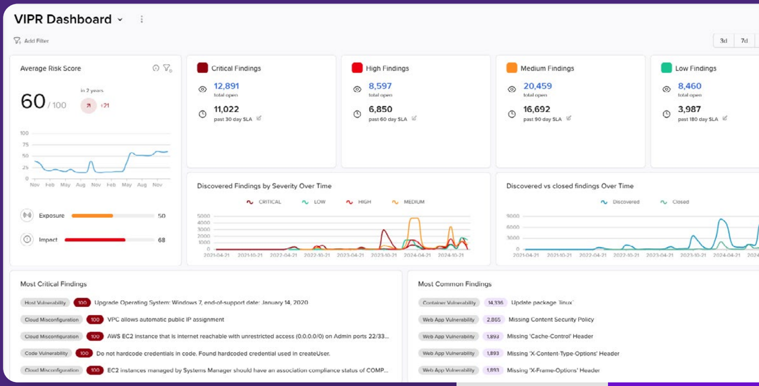
Armis is recognized as a Sample Vendor in the newly defined technology category of Exposure Assessment Platforms introduced in the Gartner® Hype Cycle™ for Security Operations (published July 2024). Armis supports CTEM programs by providing a consolidated view of priorities across security domains. Amis Centrix™ for VIPR - Prioritization and Remediation (VIPR Pro) consolidates security tool findings, adapts prioritization based on asset profile, business risk weighting, and threat intelligence, then automates ownership assignment for remediation responsibility, and helps monitor and manage the remediation lifecycle.

VIPR Pro supplements and extends the comprehensive visibility provided by Armis Centrix™ for Asset Management and Security. By integrating Armis Centrix™ for Early Warning, security teams can preemptively reduce risks by focusing on the critical vulnerabilities that threat actors are exploiting in the wild or about to weaponize with the most impact on their environment.

Armis' Centrix™ believes it is uniquely positioned to help organizations operationalize the CTEM framework, providing a platform that integrates:

- Comprehensive asset discovery and visibility for IT and non-IT assets.
- Enriching and extending asset visibility with consolidated exposure assessment and prioritization, adapted to organizational risk and business impact.
- Early Warning to minimize the exposure window for actual risks based on validated evidence of active exploits and weaponization of exploits for N day and zero days.
- Operationalization of the remediation lifecycle through AI-enabled and asset-centric ownership assignment, remediation workflow integration, and remediation activity reporting.

The Armis Centrix™ platform enables organizations to collaboratively transform and improve the security and organizational processes needed to scale and automate CTEM frameworks.



Host Vulnerability	100	Upgrade Operating System: Windows 7, end-of-support date: January 14, 2020
Cloud Misconfiguration	100	VPC allows automatic public IP assignment
Cloud Misconfiguration	100	AWS EC2 instance that is internet reachable with unrestricted access (0.0.0.0/0) on Admin ports 22/33...
Code Vulnerability	100	Do not hardcode credentials in code. Found hardcoded credential used in createUser.
Cloud Misconfiguration	100	EC2 instances managed by Systems Manager should have an association compliance status of COMP...

Container Vulnerability	14,336	Update package `linux`
Web App Vulnerability	2,865	Missing Content Security Policy
Web App Vulnerability	1,893	Missing 'Cache-Control' Header
Web App Vulnerability	1,893	Missing 'X-Content-Type-Options' Header
Web App Vulnerability	1,893	Missing 'X-Frame-Options' Header

See, protect and manage your entire attack surface with Armis Centrix™

Visit **Armis.com** to find out more

Mapping the CTEM Framework to Armis Centrix™ Capabilities

CTEM Framework Steps (Gartner)	Description	Armis Centrix™ Alignment
Discovery	Identify visible and hidden assets, vulnerabilities, misconfiguration, and other risks.	Armis Centrix™ provides both the ability to discover assets as well as capabilities to ingest, consolidate, and contextualize asset, risk and security exposure findings from an extensive breadth of data sources.
Prioritize	Prioritization should factor in urgency, security, availability of compensating controls, tolerance for residual attack surface, and level of risk posed to the organization.	Armis Centrix™ automates contextual and adaptable exposure assessment and prioritization based on finding severity, asset priority, environmental context, and threat intel - integrating with an Early Warning list - across security domains and asset categories. Integration with Armis Centrix™ for Asset Management and Security for asset profiles and enrichment.
Validation	Confirm attackers could actually exploit a vulnerability, analyze all potential attack pathways to the asset, and identify if the current response plan is fast and substantial enough to protect the business.	Armis Centrix™ adaptable prioritization enables security teams to align risk scoring with business impact and compliance objectives, helping to justify the fix with the business. Integrated with Armis Centrix™ for Early Warning, security teams can justify urgent remediation requests based on protecting exposed critical assets from actual threats from active exploits.
Mobilization	Ensure teams operationalize the CTEM findings through collaboration.	Armis Centrix™ automates ownership assignment, supports bidirectional integration with ticketing systems, and centrally monitors remediation activity. Centralized exception management.

Key features that we believe make Armis Centrix™ the go-to platform for CTEM Operationalization:

- Translates millions of alerts to thousands of grouped findings.
- Streamline time spent on manual assessment of alerts and prioritization **by 80%** through consolidation, deduplication, and contextualization.
- 75% improved MTTR for the right findings to reduce risk.
- Accurate and evidence-based early warning intelligence that uses AI to track the vulnerabilities being exploited in the wild or about to be weaponized.
- Has the broadest cloud-native platform that sees, protects, and manages the entire attack surface (IoMT/IoT/IT/OT/Cloud) with four market-leading products.
- 50 AI Engines to proactively see, protect and manage exposures and unacceptable risk.
- Utilizes the largest asset intelligence engine, tracking billions of items across the world to identify, classify, aggregate, normalize, and enrich them with context.
- Has an AI-driven Asset Intelligence Engine that understands ‘known good’ behavior baselines.

See
Discover, contextualise, enrich and profile every asset

Protect
Take measures and prioritise efforts against all exposures

Manage
Establish workflows and track risk reduction

Gartner Press Release, Gartner Identifies the Top Cybersecurity Trends for 2024, February 22, 2024, https://www.gartner.com/en/newsroom/press-releases/2024-02-22-gartner-identifies-top-cybersecurity-trends-for-2024 | Gartner, Hype Cycle for Security Operations, 2024, Jonathan Nunez, Andrew Davies, 29 July 2024 | GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and HYPE CYCLE is a registered trademark of Gartner, Inc. and/or its affiliates and are used herein with permission. All rights reserved. | 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, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

See, protect and manage your entire
attack surface with Armis Centrix™

Visit **Armis.com** to find out more