WHITE PAPER

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

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.

A trustworthy industry analyst firm Gartner® developed the Continuous Threat Exposure Management (CTEM) framework. As per Gartner®, CTEM is a program helping organizations to improve their maturity when they govern and operationalize the five recommended phases of exposure management: scoping, discovery, prioritization, validation and mobilization.

43%

of organizations lack full visibility into their IoT, OT, and unmanaged devices, leaving significant gaps in asset inventory management—a critical element in Gartner's CTEM exposure discovery.

Armis Labs

Security operations always start with protecting what is in your organization's IT, digital, and operational footprint. Likewise, remediating risks starts with understanding what risks you have in your environment, the relative urgency and impact of those risks being exploited, and the likelihood those risks will be exploited. To fix those prioritized risks, security teams need to be able to collaborate effectively with remediation teams, or maintain 'mobilization' as defined within the CTEM framework.

While the CTEM framework has been in existence for some time, Gartner® has recently defined a set of technology profiles that support CTEM programs, including Exposure Assessment Platforms. Complementing Attack Surface Management (ASM), EAPs support CTEM programs "by providing a better, more consolidated view of high-risk exposures, which in turn allows organizations to take key actions to prevent breaches." (Gartner® Hype Cycle™ for Security Operations, 2024)

This white paper explores our findings from the Gartner® CTEM framework and discusses how we think Armis technologies can play a key role in enabling CTEM programs to ensure organizations maintain operational resilience while proactively minimizing their attack surface:

- Discovery and profiling of all asset types for comprehensive visibility
- Exposure assessment across host, cloud, code, and application security findings sources
- Adaptable risk contextualization and prioritization, with early warnings on active exploits and weaponization
- Operationalization of the remediation lifecycle, with ongoing transparency into remediation status

Gartner® Definition of the CTEM Framework

Gartner® defines Continuous Threat Exposure Management (CTEM) as a program helping organizations to improve their maturity when they govern and operationalize the five recommended phases of exposure management: scoping, discovery, prioritization, validation and mobilization.

Threat exposure management encompasses a set of processes and technologies that allows enterprises to continually and consistently assess the visibility and validate the accessibility and exploitability of an enterprise's digital assets.

CTEM comprises five stages

01 Scoping

Primarily organizational in nature, involving security teams and business leaders defining the scope of CTEM programs, based on both business risk and potential impact.

02 Discovery

Technical process of identifying assets, vulnerabilities, and exposures. Ideally should extend across the organization's attack surface.

03 Prioritize

Identifying and addressing the threats most likely to be exploited against the organization. Because organizations need to understand actual, contextualized risk, traditional ways of prioritizing exposures via predefined base severity scores are no longer sufficient.

04 Validation

Process of verifying that risks are real, and a fix is viable. A good validation process requires a mix of technical assessments and organizational acceptance.

05 Mobilization

Ensure teams operationalize the CTEM findings by reducing friction in approval, implementation processes and mitigation deployments.

Definition of Exposure Assessment Platforms

According to the Gartner® Hype Cycle for Security Operations, 2024, Exposure Assessment Platforms "continuously identify and prioritize exposures, such as vulnerabilities and misconfigurations, across a broad range of asset classes. They natively deliver or integrate with discovery capabilities, such as assessment tools that enumerate exposures like vulnerabilities and configuration issues, to increase visibility."

In practical terms, EAPs cover the discovery, prioritization, and mobilization phases of CTEM programs. Armis is recognized as a Sample Vendor for CAASM, Exposure Assessment Platforms and CPS Security.

Making CTEM a practical reality with the Armis Centrix™ Platform

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

- Comprehensive asset discovery 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 for preemptive action based on validated 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.

These capabilities enable organizations to collaboratively transform and improve the security and organizational processes needed to scale and automate CTEM frameworks.

The following sections outline how Armis delivers on these CTEM imperatives through:

Comprehensive Asset Discovery and Visibility

Visibility is the foundation of an effective CTEM program. 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.

Armis Centrix™ finds in real-time all connected assets, including IT, IoT, OT, IoMT, IIOT, cloud, and applications, and for each asset, provides a granular contextualized intelligence record. In addition, the platform analyzes the network traffic and provides a complete network map that covers connections to and from assets, virtual and physical segments, and the external internet.

Armis Centrix™ can aggregate, correlate, and normalize all the data from these sources to get a complete picture of everything in your environment and apply appropriate business and security policies.

Armis Centrix™ supports coverage of the internal, external, cloud, and end-user attack surface by providing a holistic view of an organization's cyber assets. This helps users identify, monitor, and manage assets beyond their internal network, improving visibility and control over potential risks. Full visibility ensures that organizations can identify every asset connected to their networks and in their environment, eliminating blind spots that could harbor potential vulnerabilities or other security issues.

Furthermore, Armis Centrix™discovers potential exposures and security findings on managed and un-managed devices such as outdated operating systems and applications, CVE matches, default credentials, malfunctioning protection agents, insecure protocols usage, bad segmentation, security controls coverage issues, and external-facing assets.

Consolidated Risk Contextualization and Prioritization

According to Gartner®, scoping includes "traditional devices, apps and applications but also less tangible elements such as corporate social media accounts, online code repositories and integrated supply chain system." Armis Centrix™ automatically ingests asset data, vulnerabilities, and exposure findings from native discovery and third-party integrations for cloud, code, containers, application security, and host vulnerabilities and misconfigurations - providing the consolidated view of priorities across security domains outlined in the EAP definition.

The Armis Centrix™ platform incorporates standard scoring such as CVSS and EPSS as well as source tool severity ranking as inputs for prioritization. With the base score as the starting point, Armis Centrix™ further enriches the prioritization with asset exposure assessment, exploitability and ingested asset information and applied custom metadata labels for contextualization - in addition to incorporating threat intelligence.

The Armis Centrix™ platform allows security teams to adapt prioritization through custom labels that enable finer-grained control over how exposures are prioritized. For example, users can use labels with configurable risk scoring to prioritize or suppress findings based on compensating controls, such as whether an endpoint protection platform (EPP) is in place or whether the asset is part of a production environment or is public-facing. By incorporating such factors, organizations can ensure their severity scoring reflects real-world risk more accurately, taking into account business context, security measures, compliance concerns, and asset exposure.

The combination of composite vulnerability severity and asset priority is then further enriched with threat and exploit feeds - including native integration with Armis Centrix™ for Early Warning.

Armis Centrix™ supplements third-party findings with native Risk Factors assigned to assets, such as asset behavior, configuration issues, end-of-life hardware or software, operating system, or default credentials in use.

Armis Centrix™ supports coverage of the internal, external, cloud, and end-user attack surface by

providing a holistic view of an organization's cyber assets. This helps users identify, monitor, and manage assets beyond their internal network, improving visibility and control over potential risks. Full visibility ensures that organizations can identify every asset connected to their networks and in their environment, eliminating blind spots that could harbor potential vulnerabilities or other security issues.

Furthermore, Armis Centrix™discovers potential exposures and security findings on managed and un-managed devices such as outdated operating systems and applications, CVE matches, default credentials, malfunctioning protection agents, insecure protocols usage, bad segmentation, security controls coverage issues, and external-facing assets.

Preemptive Prioritization and Validation: Early Warning Threat Intelligence

By integrating Armis Centrix™ for Early Warning alerts, security teams can preemptively reduce risks by focusing on the critical vulnerabilities in the early stages of exploit with the most impact on their environment. Early Warning provides evidence-based intelligence on active exploits and those about to be weaponized, often discovering threats well before they are added to the CISA KEV catalog.

In combination with consolidated visibility across the organization's environment of asset profiles and exposure prioritization, Early Warning enables teams to operationalize a preemptive posture on emerging threats, and focus remediation activities on exposures with the most urgent level of risk. Teams can align their resources on immediate and actual risk, not a theoretical severity risk, shifting from fire drills to a systematic and preemptive strategy to close the exposure window.

According to a Ponemon Institute study, **54% of organizations** report not being able to respond effectively to security incidents due to poor integration between asset visibility and threat detection tools. Armis Centrix™, with its integration into ITSM platforms, bridges this gap for more efficient response.

The automated response mechanisms in Armis Centrix™ allow for rapid isolation or remediation of compromised devices without manual intervention. This speeds up containment and ensures organizations can quickly neutralize security findings before they spread.

Mobilization: Operationalization of the Remediation Lifecycle

Armis Centrix™ supports the operationalization of the remediation lifecycle through automated ownership assignment, bidirectional integration with ticketing systems for collaboration, monitoring and tracking, and centralized reporting by individual tasks, business or organizational unit remediation activity performance, overall risk trends, and exception requests.

Ownership assignment for assets and remediation tasks can be enabled both through predictive assignment using AI inference, as well as predefined rules based on asset properties, sites, boundaries, ingested CMDB and cloud resource tags and labels, and custom asset attributes.

Armis Centrix™ can use findings properties such as file path to perform assignment to a remediation owner based on responsibility for application code or container operating system. Armis Centrix™ integrates with user identity stores as well as CI/CD users to build a comprehensive view of remediation ownership in terms of organizational hierarchy and team or business unit members.

Security teams can centrally track and monitor remediation task status, by criticality, finding category and asset class across ticketing systems. In addition to organization-wide tracking of SLAs by finding severity (critical, high, medium and low) over configurable time intervals, analysts can build custom reporting dashboards based on filters and properties that are relevant for compliance mandates and security policies.

Armis Centrix™ also provides a remediation campaign capability that allows vulnerability management teams to create and scope targeted campaigns for specific assets, vulnerabilities targeted by a new active exploit, new CISA KEV exploits, or exposure categories, with a defined end date. Campaigns can serve the function of addressing critical risks in a scoped process, as well as identifying areas of weaknesses or issues in the remediation lifecycle.

> On average, it takes organizations **80 days to patch** critical vulnerabilities, significantly increasing their exposure to threats. Armis Centrix™ enables faster identification and patch prioritization.
>
> **Armis Labs**

In Summary

Continuous Threat Exposure Management (CTEM) framework offers a proactive and adaptive approach to systematically addressing cyber exposure risk. By offering unmatched visibility, security, and control, Armis enables organizations to effectively manage their attack surface, address risks, and respond to threats in real time.

With its ongoing investments in external attack surface management, compliance, and industry-specific capabilities, Armis continues to provide the most comprehensive platform for enabling and operationalizing CTEM programs, ensuring organizations can stay ahead of their dynamic attack surface.

Appendix

CTEM Framework Steps	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 Early Warning capabilities - 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 at actual threat 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.

CTEM Functionality (Gartner®)	Description	Armis Centrix™ Alignment
Exposure Assessment	Continuously identify and prioritize exposures, such as vulnerabilities and misconfigurations, across a broad range of asset classes. Natively deliver or integrate with discovery capabilities, such as assessment tools that enumerate exposures like vulnerabilities and configuration issues, to increase visibility (Gartner® Hype Cycle for Security Operations, 2024)	Armis Centrix™ consolidates and deduplicates security tool alerts, asset data, and incorporates threat intel in assessment. Automates finding contextualization and prioritization across security domains, and enables the remediation lifecycle process.
Attack Surface Management	Continuously identifying, monitoring, and managing all of an organization’s internal and external internet-connected assets to discover potential attack vectors and exposures.	Armis Centrix™ aggregates, deduplicates, and normalizes asset data from your existing solutions and CMDB to provide an always accurate inventory, uncover security gaps, and automate responses — streamlining your operations.
Continuous Monitoring and Detection	Ongoing surveillance of network activities to detect and respond to evolving threats in real-time.	Armis Centrix™ continuously monitors for suspicious behavior, anomalies, and attack patterns, providing instant threat detection across IT, OT, and IoT environments.

GARTNER® is a registered trademark and service mark of Gartner® and Hype Cycle is a registered trademark of Gartner®, Inc. and/or its affiliates in the U.S. and internationally 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.

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

Website

Platform

Industries

Solutions

Resources

Blog

Try Armis

Demo

Free Trial