ARMIS®

WHITE PAPER

The Age of Generative AI in Cyber Exposure Management

Introduction

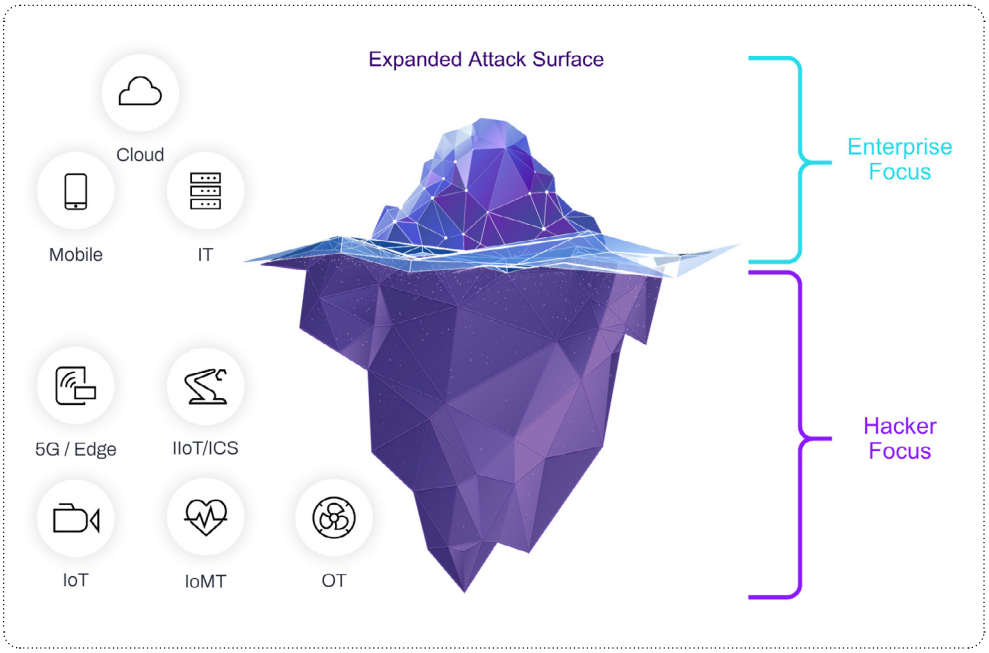
The conversation around the use of artificial intelligence (AI) has become ubiquitous. When it comes to cyber exposure management platforms, what does AI truly bring to the table? This white paper aims to demystify AI's role in enhancing cybersecurity measures by leveraging advanced technologies to address age-old problems in innovative ways.

Defining Generative AI

Generative AI refers to algorithms that can generate new content, predictions, and insights based on existing data. In the context of cyber exposure management, generative AI is not just a buzzword. It serves as the backbone for developing smarter, more efficient systems capable of handling complex cybersecurity challenges.

The Role of AI in Cyber Exposure Management

According to Armis Labs, the number of connected assets will grow to 50 billion in 2025. The vast majority of these connected assets remain unseen, unmanaged, and not secured. This is mostly because organizations are not aware of them and they are missed by traditional security solutions. This gap in visibility creates significant vulnerabilities that can be exploited by cyber attacks, which increasingly target government agencies, critical infrastructures, and healthcare organizations.



3x
more non-IT/Mobile assets in 2025

2x
the volume of cyber attacks

80%
of assets are unseen or unmanaged

In addition to the visibility gap, human error further exacerbates security risks, as employees may unknowingly introduce vulnerabilities through misconfigurations or unsafe practices. The need for rapid response is crucial to minimize damage; swift action can significantly reduce the time to containment, preventing downtime and halting the spread of threats. Organizations must prioritize agility in their incident response strategies to outpace potential lateral movement by attackers and safeguard their critical assets.

With the rising tide of cyber threats, leveraging AI technology is imperative, as it can provide the enhanced visibility and proactive management necessary to safeguard these essential systems. The integration of AI into cyber exposure management is not just beneficial; it is essential for creating a resilient defense against an evolving threat landscape.

By harnessing the power of artificial intelligence, platforms can analyze vast amounts of data with unprecedented speed and accuracy. This enables organizations to proactively identify vulnerabilities, anticipate potential risk, and fortify their security infrastructures more effectively. AI not only enhances threat detection capabilities but also automates operational tasks, allowing cybersecurity professionals to focus on more complex, strategic initiatives. Operational tasks are wide-ranging and can include asset consolidation and contextualization, deduplication engines, prioritization ticketing and predictive ownership rules. As cyber threats continue to evolve, the integration of AI into exposure management is becoming essential for robust and resilient defenses.

Fighting Fire with Fire: Leveraging AI in Cybersecurity to Outsmart Adversaries

Armis Labs uncovered the AI-powered tactics of nation-state actors, identifying several threat actors actively using AI for advanced cyber capabilities, including:

- Russian-affiliated Forest Blizzard (APT28)
- North Korean hackers Emerald Sleet (Kimusky)
- Iranian threat actors Crimson Sandstorm (Imperial Kitten)
- Chinese state-affiliated groups, Charcoal Typhoon (Aquatic Panda) and Salmon Typhoon (Maverick Panda)

As generative AI continues to evolve, cyber threats are similarly becoming more sophisticated through the use of AI technologies. Attackers are increasingly employing machine learning algorithms to automate their methods, allowing for quicker and more effective exploitation of vulnerabilities in systems. AI-powered malware can adapt and learn from its environment, enabling it to evade traditional security measures by altering its behavior in real time. Moreover, adversarial AI can be used to create deepfakes, phishing schemes, and other deceptive tactics that are alarmingly convincing. This arms race between defenders and attackers underscores the necessity of implementing advanced AI-driven cyber exposure management solutions that not only detect and mitigate these emerging threats but also anticipate future vulnerabilities in a landscape that is continually reshaped by technology.

Key Benefits of AI in Cyber Exposure Management

Enhanced Visibility

Traditional cybersecurity tools often focus on visible, managed assets, leaving a substantial portion of the attack surface — unmanaged and under-managed assets —unmonitored. AI enhances visibility by:

> **Unified Asset Inventory:** Integrate with your existing IT and security tools, aggregating, deduplicating, and normalizing data for every asset in your environment.

> **Profile and Classification:** Establishing detailed profiles and classifications for assets, including unseen ones, to provide a comprehensive view of the attack surface.

> **Asset Intelligence, Context and Behavior:** Turn data into informed decisions. Asset Intelligence Engines add contextual intelligence to every asset actionable and based on their behavior and roles within the organization, allowing your IT and Security teams to prioritize remediation efforts based on threats, risks and criticality.

Improved Threat Detection

AI engines focus on real-time threat detection (including early warning), scoring risks, and prioritizing responses. Specific benefits include:

> **Tracking Exploitation with Early Warning Intelligence:** AI engines deploy honeypots and large language models (LLMs) to create decoy environments that attract and analyze attacker behavior. Reverse engineering LLMs play a vital role in dissecting malware and understanding the tactics, techniques, and processes (TTPs) used by adversaries. Language conversation analysis assists in interpreting threat actor communications, aiding in threat determination and ranking. Utilizing proof-of-concept (POC) validators, organizations can verify potential vulnerabilities and exploits. Simultaneously, SMT/SAT solvers are used to solve logical formulas that may uncover latent threats. Trend anomaly detection monitors patterns for unusual activities that could signal an attack, while deception technology focuses on identifying known CVE (Common Vulnerabilities and Exposures) exploits. Moreover, these AI-driven methods excel at detecting “0-day attacks” and provide an advanced framework for finding, ranking, and analyzing threat actor exploitation.

> **Threat Detection:** Using AI-driven algorithms, organizations can swiftly and accurately identify anomalies within their environments, allowing for the detection of potential threats at their inception.

Prioritization

Normalization and Deduplication: Ingests and reorganizes data from security and IT tools to transform large sets of asset and risk information into digestible fix items.

Prioritization and Risk Scoring: Assigning risk scores to vulnerabilities and other findings; then to prioritize mitigation efforts effectively.

Remediation

Effective remediation is crucial in addressing the vulnerabilities identified through AI-driven insights. With the ability to discover, analyze and prioritize risks, generative AI facilitates targeted responses by suggesting practical remediation strategies. Key aspects of this process include:

Assign Ownership: Predictive ownership rules through AI assign fix responsibilities, and enable ongoing communication for distributed teams through bidirectional integration with their preferred workflow or ticketing system.

Continuous Monitoring: Establishing systems for ongoing assessment and validation of the remediation process to ensure vulnerabilities remain resolved over time.

Connect The Finding To The Fix: By providing actionable guidance to speed accurate mitigation efforts based on the specific finding.

Efficient Management

AI optimizes the management of cyber exposure by consolidating and prioritizing vulnerabilities, ensuring that resources are focused on the most critical issues:

Consolidation: Aggregating data from various sources to provide a unified view.

Prioritization: Leveraging AI to prioritize vulnerabilities based on their potential impact.

Policies and Reporting: Report on the efficacy of your vulnerability management approach from beginning to end.

By properly leveraging AI as a key ingredient in cyber exposure management and security efforts, organizations can substantially reduce unnecessary noise and focus on the risk that actually matters.

Practical Applications and Case Studies

Asset Lifecycle Management

From the moment a new device is detected on the network, AI starts its lifecycle management:

Early Warning

Detecting and monitoring vulnerabilities that are being exploited in the wild or are about to be weaponized.

Day 0

Detection of a new device (e.g., a camera) through passive traffic inspection.

Ongoing

Continuous profiling and enrichment of device information using AI-driven rules.

Anomaly Detection

Identifying irregular behavior based on historical data and established baselines.

Actionable Insights

Providing recommendations and enforcement actions to mitigate identified risks.

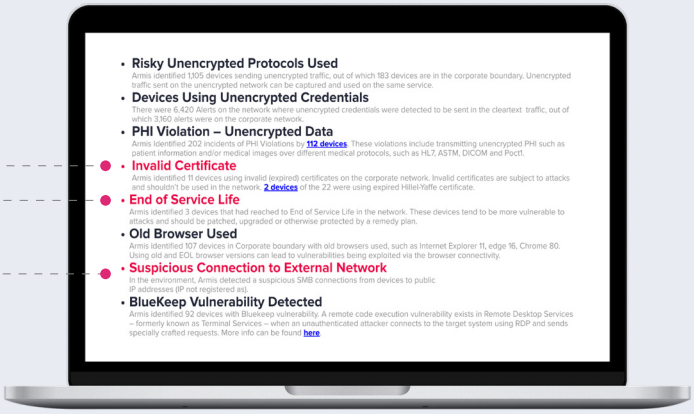
Real World example | Asset Management

Armis was installed for a successful POV

Prospect was trying to procure budget, and wasn't monitoring for alerts…

Multiple critical findings during POV

- Invalid Certificates
- 3 Network Devices End of Service
- Suspicious SMB connections to external network



Outdated edge hardware was the entry point for a ransomware attack. All active security measures and agents were disabled.

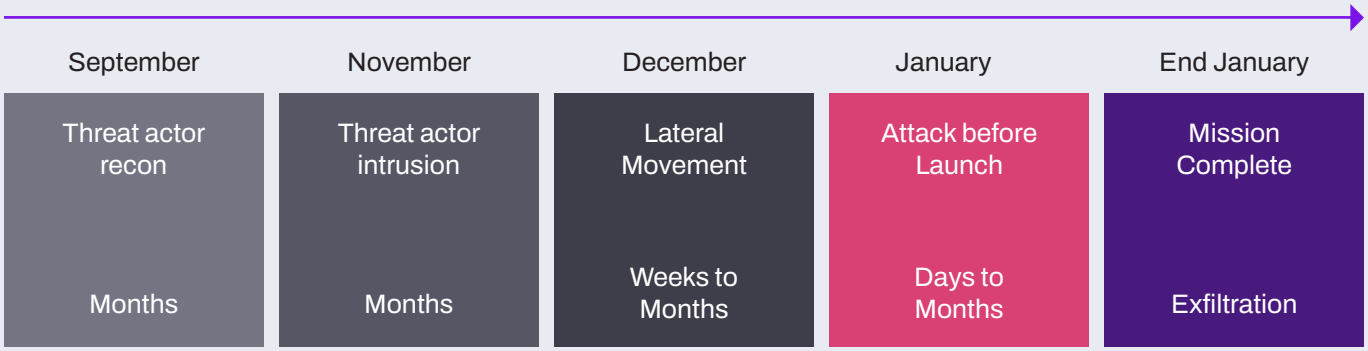
Hospital was out of commission for several months, reverting to pen & paper.

Threat Detection

AI engines continuously monitor network traffic to detect anomalies. For instance, an unexpected surge in traffic to a camera within the network could indicate a security breach. By recognizing this irregularity, the system can promptly alert administrators and take protective actions. Additionally, proactive tools like honeypots and deception technology leverage AI to track threat actors' behaviors, allowing for the preemption of attacks during the formulation stage.

Real World example - Threat Detection

Proactive vs. Reactive Vulnerability Management

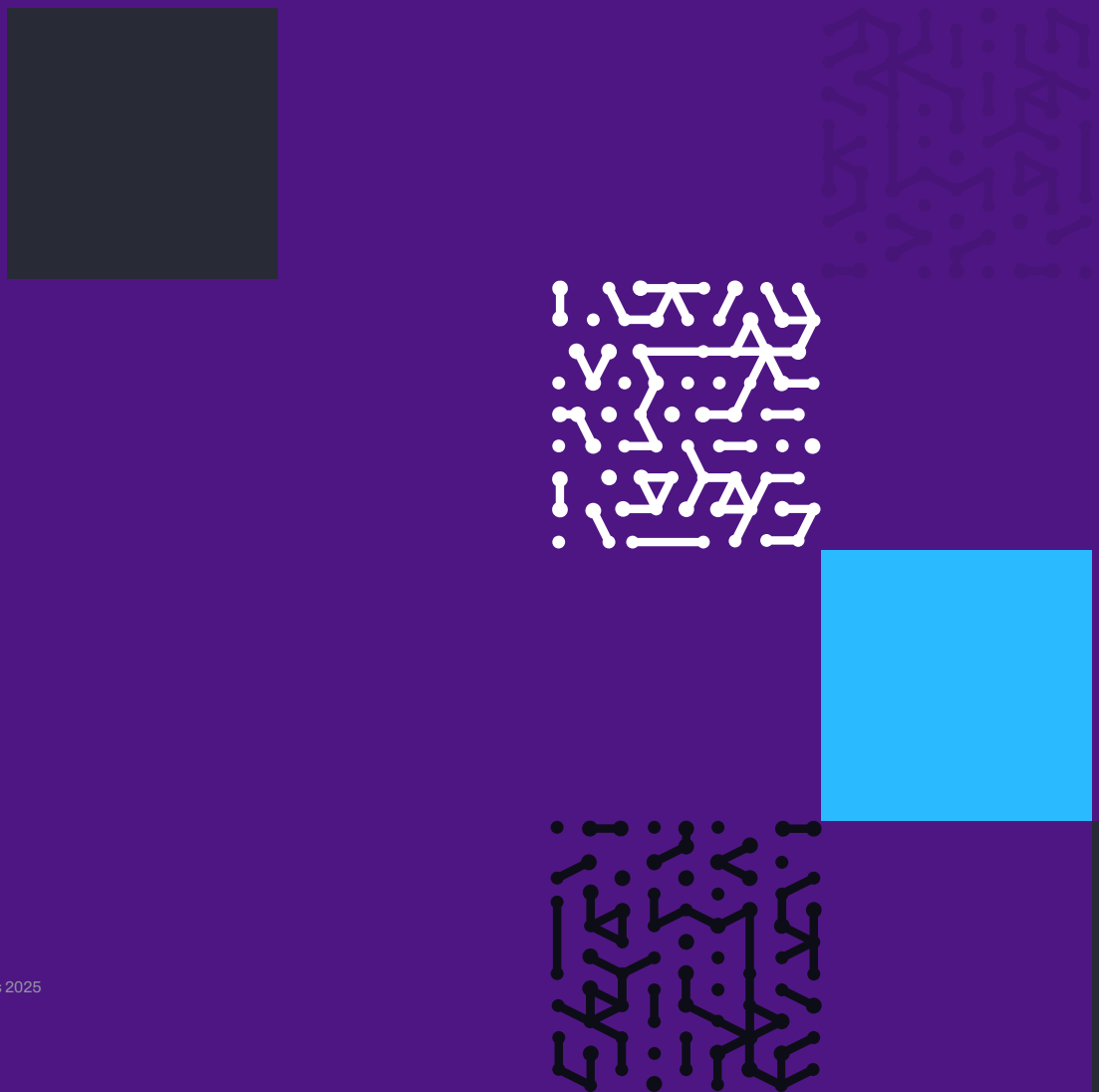


AI engines empower early warning systems that employ honeypots and dark web intelligence to track threat actor behaviors and monitor vulnerability exploitation.

Traditional security focused on a manual, reactive approach that includes remediating vulnerabilities after an attack is already in progress.

Conclusion

Generative AI marks a groundbreaking leap in operationalizing cyber exposure management, transforming the way organizations tackle cybersecurity challenges. By enhancing visibility into network activities, boosting threat detection capabilities, and streamlining management processes, AI empowers organizations to proactively counter cyber threats. When harnessed effectively, AI-driven cyber exposure management platforms become unstoppable forces, offering unparalleled protection and adaptability, ensuring that businesses remain fortified against evolving threats. These platforms not only predict and mitigate risks but also continuously learn and adapt, providing a robust defense mechanism that keeps organizations one step ahead of potential cyber adversaries.



Introducing Armis, The Cyber Exposure Management & Security Company

Armis Centrix™, the Armis cyber exposure management platform, is powered by the Armis AI-driven Asset Intelligence Engine, which sees, secures, protects and manages billions of assets around the world in real time.

Asset Management and Security
Complete asset inventory of all asset types allowing any organization to see and secure their attack surface

OT/IoT Security
See and secure OT/IOT networks and physical assets, ensure uptime and build an effective & comprehensive security strategy

Medical Device Security
Complete visibility and security for all medical devices, clinical assets and the entire healthcare ecosystem - with zero disruption to patient care

VIPR - Prioritization and Remediation
Consolidate, prioritize and remediate all vulnerabilities and security findings; improve MTTR with automatic remediation and ticketing workflows

Early Warning
Early warning AI based system that leverages intelligence from the Dark Web, Dynamic Honeypots and HUMINT to stop attacks before they impact your organization

Armis Centrix™ utilizes 50 AI engines to handle billions of security events daily across hundreds of countries. The AI engines are categorized into three main areas:

5B+ assets monitored 24/7/365

Asset Discovery: New assets real time detection, deduplication and consolidation;

Profile Classification: deep learning of asset behavior and protocol attributes for profile classification;

Asset Context: aggregating and clustering additional asset-related context.

6.5M+ daily security decisions

Early Warning Threat Detection: deception technology; anomalous behavior detection; reverse engineering; dark web language tracking;

Risk Score: Asset criticality, threat ranking; graph-centrality and data exposure engines;

Investigation: alert investigative context and workflow suggestions; threat determination.

Consolidating and prioritizing **1B+** potential exposures daily

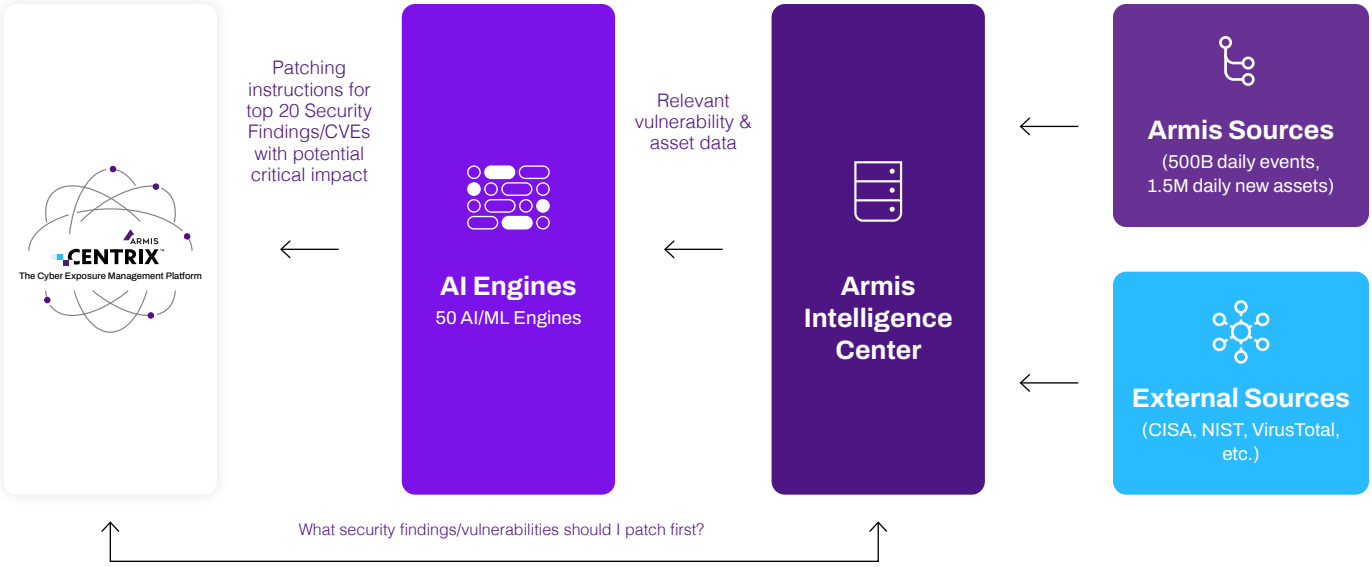
Security Findings: deduplication alerts, ChatGPT integration, Natural Language Processing;

Vulnerability Management: vulnerability criticality classifiers and unified prioritization;

Suggested Actions: Fix recommendations, ACL rules suggestions; ownership discovery, risk appetite;

Personalized Policies and Reports.

The Armis Asset Intelligence Engine is a collective AI-powered knowledge base, monitoring billions of assets world-wide in order to identify cyber risk patterns and behaviors. It feeds the Armis Centrix ™ platform with unique, actionable cyber intelligence to detect, prioritize and remediate real-time threats across the entire attack surface.



AI-driven Business Outcomes That Deliver

50-1 Reduce findings volume in complex environments by 50-1 with ML deduplication

90% Cut time spent on identifying owners and assigning tickets by 90%, with custom ticketing rules

90% Improve MTTR by as much as 90%

1/2 Half the time for resolution of critical findings, with ongoing improvements in reduction of response times anticipated

7x Increase the number of closed findings by 7x over three months, reducing overall threat debt

98% reduction in vulnerabilities to prioritize based on tracking threat actor exploitation

Detect vulnerabilities months/years earlier than CISA KEV

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