ARMIS®

WHITE PAPER

The Top 5 Ways to Advance Threat Hunting in Your Organization with Early Warning Detection

At its core, threat hunting is a cybersecurity approach where analysts actively and iteratively search through assets in their environment to detect threats that evade existing defense, detection, and response capabilities. Unlike traditional security measures that react to alerts, threat hunting involves proactively seeking out the adversary before they signal their presence.

But like skilled detectives, a threat hunting analyst's effectiveness is contingent on the quality of intelligence they can access and the evidence they can compile. To achieve a more sophisticated and bullet-proof approach to threat hunting, analysts must pursue timely, accurate, and evidence-based intelligence. This should leverage early warning detection to prioritize the actions of threat actors.

For organizations looking to fortify their defenses and adopt a smarter approach to threat hunting with timely, accurate, and evidence-based intelligence, Armis has prepared The Top 5 Ways to Advance Threat Hunting in Your Organization with Early Warning Detection.

1. Build a Solid Foundation for Early Warning Detection

Traditionally, being proactive has meant staying well-informed about your system, defense posture, and security status on the ground. This approach, while comprehensive, often leads to a reactive cycle of hit-or-miss mitigation techniques due to its labor-intensive nature.

Organizations must adopt early warning detection systems to effectively prepare for and mitigate security incidents before they cause significant harm or disruption. Like a lightning detector at a sporting event, Tsunami detectors in the Pacific Ocean, or Missile Detection Systems during the Cold War, cybersecurity early warning detection systems have been pivotal in enabling teams to brace for impact long before calamity strikes for decades. What you may find though is not every early warning detection system provides timely, accurate and evidence-based intelligence.

To establish a foundational early warning detection system that is timely, accurate, and evidence-based, ensure your cybersecurity practices encompass the following:

> **Understand Organizational Assets and Risks:**
>
> Recognize that defending the unknown is impossible. Identify and prioritize critical assets, data, and systems within your organization. Understand the potential impact of security threats on these assets and the specific risks your organization faces

> **Empower with timely and accurate asset intelligence:**
>
> AI-powered asset intelligence engines can monitor billions of assets world-wide in order to identify cyber risk patterns and behaviors and enrich existing assets.

Follow the Threat Actors with Early Warning Detection:

Employ indicators such as honeypots, intelligence and research to predict potential threats and make real-time assessments. This type of detection can add CVEs to your organization's early warning list before they're published by globally accessible knowledge agencies and corporations.

Demand Evidence-based Threat Intelligence:

Rely on evidence-based threat intelligence feeds and sources to stay informed of emerging threats and the tactics employed by attackers.

Blend Manual, Artificial Intelligence (AI) and Automated Techniques:

Employ a combination of manual investigation techniques, AI, and automated tools to search for and identify potential threats efficiently.

2. Emphasize AI with machine learning for multi-faceted intelligence.

Leverage sophisticated data analysis techniques, including machine learning algorithms and statistical modeling, to predict anomalous or suspicious behavior within your environment before it happens. Threat hunters use AI to automatically and dynamically process and analyze large volumes of intelligence, saving a significant amount of time and resources. Machine learning algorithms can automatically identify patterns or anomalies indicative of potential malicious activity, enabling threat hunters to detect and investigate security threats, at times, months before they occur.

The most intuitive, proactive defense solutions are multifaceted, building early warning lists by drawing insights from actual threat actors behaviors. Ways to proactively track threat actor activity before a threat is even launched include:

Smart Honeypots Deployment:

Purpose-configured, smart honeypots, situated outside of client environments, create potential "hotspots" that allow for the observation of malicious behaviors and techniques.

Dark Web Intelligence:

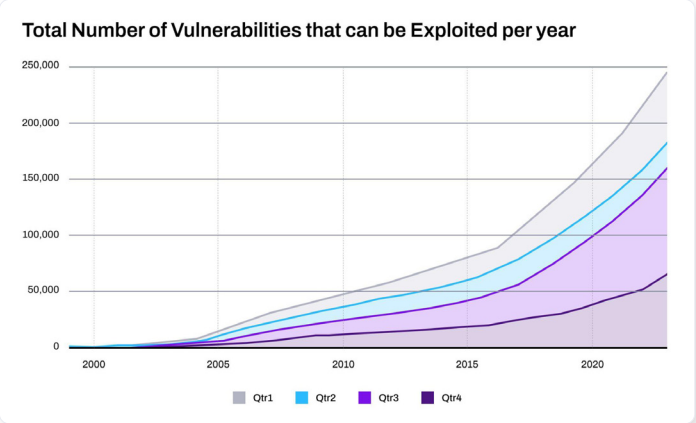
By scouring the deep and dark web for pertinent "chatter," organizations can gain valuable intelligence into nascent cyber threats, enabling preemptive action.

Human Intelligence Integration:

Leveraging human intelligence through strategic feeds, reverse engineering, and "listen posts," ensures unparalleled coverage and accuracy in threat detection.

3. Seek solutions that prove evidence-based, timely and accurate "before the attack" capabilities

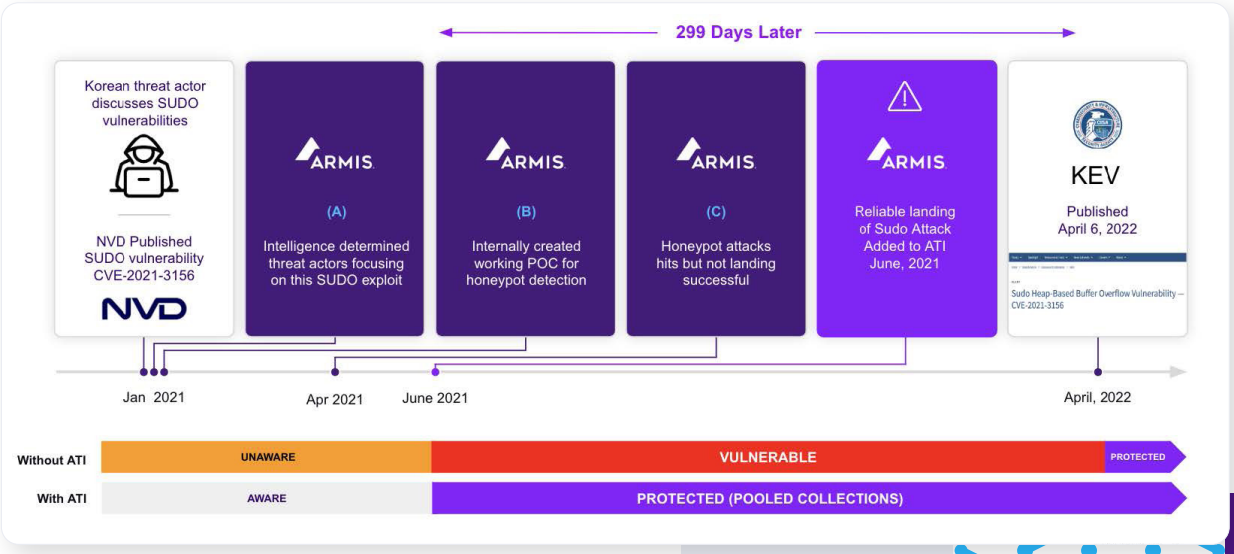
During a recent discussion with a CISO from a Fortune 100 company, he exclaimed, "There's millions of vulnerabilities in our organization but only a small percentage matter."



The ever-expanding attack surface significantly burdens vulnerability management teams and the SOC. Currently, most teams mitigate risk by using Common Vulnerability Scoring System (CVSS) scores for vulnerabilities or Common Vulnerabilities and Exposures (CVEs). But if teams are drowning in CVEs to prioritize and remediate, they can easily miss a critical vulnerability. Afterall, according to Ponemon, "60% of compromises are from known vulnerabilities."

Trying to manage vulnerabilities without understanding risk is impossible. Organizations instead need to utilize exploitability. Exploitability allows you to enrich CVSS scores with what threat actors and attackers are actually doing. This can reduce CVEs to manage by 98%.

The best way to utilize exploitability is to leverage early warning detection that combine AI and machine-learning so you can leverage evidence-based, timely and accurate intelligence as demonstrated below:



In the above timeline, a vulnerability was announced in January 2021.

Utilizing early warning detection allowed intelligence to determine that threat actors were focusing on a SUDO exploit in April 2021. To counteract this, a smart honeypot was crafted to lure the attackers, proving successful in June 2021.

Within a mere two months, sufficient information was collected and subsequently leveraged alongside human intelligence to reverse engineer the exploit. Following this, a Sysmon rule was established with the objective of detecting any exploitation of this vulnerability in the wild, which it successfully accomplished.

Ultimately, the National Vulnerability Database issued a CVE for this particular exploit in April 2022—10 months after the initial detection through early warning systems.

4. Customize with purpose and seek ROI.

Threat hunting, utilizing early warning detection derived from AI and evidence-based intelligence, represents an optimal state of cyber defense. But imagine the further advantages if you could deploy honeypots tailored to a specific industry. Such honeypots would not only mimic the systems and services prevalent within that sector but also the tactics, techniques, and procedures (TTPs) attackers commonly use against organizations in that field. This capability is within reach through AI, enabling the research of industry-specific threats, selection of honeypot types, and design of custom honeypot environments. It also allows for the analysis of asset intelligence from that vertical and leverage of dark web chatter. While pooled honeypots serve as a fundamental defense mechanism, custom honeypots offer a level of personalization that significantly enhances security, streamlines productivity, and boosts ROI.

Improvements in ROI stem from:

> **Targeted Insight Generation:**
>
> By tailoring solutions to replicate particular systems, applications, or vulnerabilities of interest to your organization or industry, you attract attackers with specific targets in mind. The resulting intelligence on their TTPs enriches your security strategy, enabling more effective allocation of resources against genuine threats.

> **Reduced False Positives:**
>
> Custom honeypots designed to closely resemble your actual systems and configurations reduce the incidence of irrelevant automated scanning or low-level attacks. This specificity helps your security team focus on real threats by minimizing the noise from false positives.

Early Threat Detection:

Custom honeypots facilitate the early detection of threats in the attack lifecycle. Monitoring interactions within the honeypot allows for the identification of potential threats before they evolve into substantial attacks on your live environments, considerably mitigating possible damage and related costs.

5. Empower integrations.

Integrations are pivotal in augmenting threat hunting capabilities, as they enhance visibility across different platforms, automate key security workflows, and facilitate a more effective detection and response mechanism to security threats. Through the seamless synchronization of security tools and systems, organizations can consolidate and analyze data more efficiently, enabling quicker identification of suspicious activities. Automation brought about by integrations reduces manual workload, allowing security teams to focus on strategic threat analysis and response. Additionally, the capability of integrating with threat intelligence platforms means that organizations can leverage the latest information about vulnerabilities and attacks, ensuring a proactive defense posture. In essence, the power of integrations lies in their ability to bring together disparate pieces of information into a coherent, actionable insight, significantly improving the effectiveness of threat hunting operations.

Here's how threat hunting is improved when organizations are empowered by integrations:

Centralized Data Collection:

Integrating threat hunting tools with data sources such as security logs, network traffic, endpoint telemetry, and asset intelligence feeds allows for centralized collection and aggregation of diverse data sources. This provides threat hunters with comprehensive visibility into the organization's security posture and enables them to identify anomalies and patterns more effectively.

Vulnerability Prioritization and Remediation:

Discovering vulnerabilities is a great first step, but effectively addressing them makes the difference between eliminating risk and remaining exposed. An AI approach, with real-time alerts, offers a unified platform for technology risk prioritization and resolution lifecycle management across code, infrastructure, cloud, and application findings.

Correlation and Contextual Analysis:

Integrating threat hunting tools with security information and event management (SIEM) systems enables correlation of security events and contextual analysis of security data across disparate sources. This helps threat hunters identify complex attack patterns and tactics used by adversaries that may span multiple stages of the kill chain.

Workflow Integration:

Integrating threat hunting tools with incident response platforms and ticketing systems streamlines the workflow for threat investigation, response, and remediation. This allows threat hunters to seamlessly escalate and track incidents, collaborate with other security teams, and document findings for future reference and analysis.

Armis Centrix™ for Early Warning: A Revolutionary Approach to Cybersecurity

In today's rapidly evolving cyber threat landscape, Armis Centrix™ for Early Warning stands at the forefront, offering a groundbreaking AI technology that harnesses the power of dark web analysis, smart honeypots, and human intelligence (HUMINT) to thwart attacks before they impact organizations. Armis Centrix™ for Early Warning is designed as an early warning system, equipped to arm organizations and agencies with actionable intelligence even before vulnerabilities become public, attacks are initiated, and potential damages occur. Here's what Armis Centrix™ for Early Warning brings to the security table:

Early-warning Intelligence System:

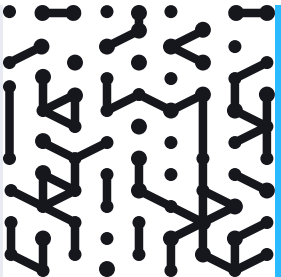
Gain a critical head start of 3-6 months, spotting threats during their incipient stages, and prepare your defenses ahead of time.

Actionable Insights:

Facilitates a contextual risk assessment enabling targeted countermeasure strategies, thus elevating the precision of your security posture.

Proactive Defense:

Bolsters your environment's resilience against cyber threats by implementing preemptive safeguards, effectively mitigating risks before they crystallize into actual attacks.



Outcomes with Armis Centrix™ for Early Warning:

> Achieve a **98% reduction** in the number of vulnerabilities that need immediate attention, streamlining your security efforts towards genuine threats.

> On average, **80%** of exploits are known and documented before corresponding CVEs are officially released, highlighting the critical time advantage Armis Centrix™ provides.

> A significant **23-day average gap** exists between the disclosure of an exploit and the issuance of its corresponding CVE, emphasizing the importance of early detection.

> Experience a **10X expansion** in your oversight and understanding of the cyber threat ecosystem, facilitated by the depth and breadth of intelligence sourced by Armis Centrix™.

Armis Centrix™ for Early Warning redefines proactive cybersecurity, offering organizations an advanced, insightful, and pre-emptive approach to combating digital threats.

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