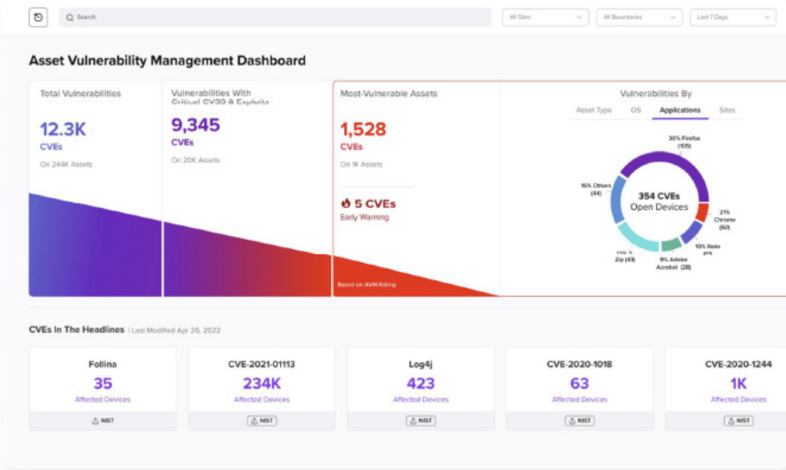
Armis Centrix™ for Early Warning for OT

Take a proactive approach to the threat before it impacts your organization. Revolutionary AI technology and machine learning algorithms that leverages dark web, intelligent honeypots and HUMINT to stop attacks before they impact your organization and protect critical assets with confidence.

Redefining OT Security by Preempting the Attack

Protect your critical infrastructure with enhanced attack surface awareness and prevention. Armis Centrix™ for Early Warning empowers you with an early warning system designed to anticipate threats, understand their potential impact, and take preemptive action to neutralize them, effectively moving the security posture from defense to offense.



Asset Vulnerability Management Dashboard

Total Vulnerabilities: 12.3K CVEs — On 244K Assets

Vulnerabilities With Critical CVSS & Exploits: 9,345 CVEs — On 20K Assets

Most-Vulnerable Assets: 1,528 CVEs — On 1K Assets

5 CVEs Early Warning

Based on AVM Rating

Vulnerabilities By: Asset Type | OS | Applications | Sites

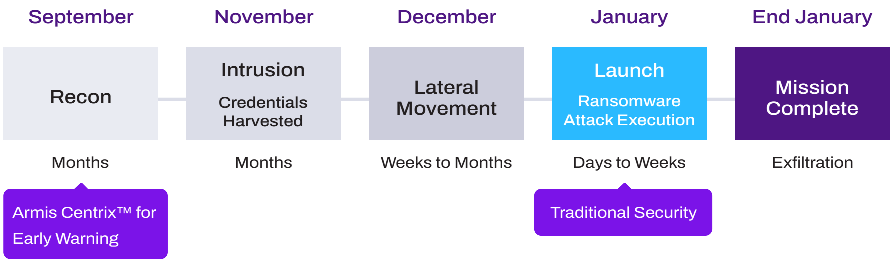
354 CVEs Open Devices

CVEs In The Headlines | Last Modified Apr 26, 2022

Follina	CVE-2021-01113	Log4j	CVE-2020-1018	CVE-2020-1244
35 Affected Devices	234K Affected Devices	423 Affected Devices	63 Affected Devices	1K Affected Devices
NIST	NIST	NIST	NIST	NIST

Address the Vulnerabilities That Matter Most with Proactive Vulnerability Intelligence

With Armis Centrix™ for Early Warning, you can ensure your OT organization is always leveraging the most up-to-date protection to mitigate the risk associated with high stakes vulnerabilities. Transcend traditional security measures and proactively identify preparatory indicators of attacks and exploits.



September	November	December	January	End January
Recon	Intrusion Credentials Harvested	Lateral Movement	Launch Ransomware Attack Execution	Mission Complete
Months	Months	Weeks to Months	Days to Weeks	Exfiltration

Protect Against and Prevent OT Cyberattacks with Armis Centrix™ for Early Warning Use Cases:

Leverage AI-powered Early Warning Intelligence

to anticipate threats, understand their potential impact, and take preemptive action to neutralize them, effectively moving the security posture from defense to offense.

Protect Against Weaponized Threats

by understanding global attack surface and real-time hacker behaviors and techniques.

Preempt Threat Actors

and stop them before they impact your organization, thanks to HUMINT and AI intelligence, scouring dark web chatter.

Detailed Analysis of Ransomware Attacks

including intelligence on what credentials and hacking tools are being sold and leveraged.

Address Ongoing Vulnerabilities

that are actually being exploited by threat actors with Armis Labs intelligence, listening posts, trends, and expertise.

Preventive Security Guidelines

to notify of potentially exploitable vulnerabilities or faults and begin remediation workflows before an attack happens.

Stop the attack before it happens with Armis Centrix™ for Early Warning

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

Key features that make Armis the ultimate proactive security solution for OT

Early Warning included with Armis Centrix™ allows you to leverage our dark web insights, AI-powered pre-attack threat hunting, and create an early warning system.

AI Capabilities that can predict attack behavior, tactics, and likely targets; with proactive adjustment to each customer's needs and current threat environment.

Notifications of impending threats via the channels you use within your organization.

Smart Honeypots and other deception technologies to learn hacker behaviors and techniques.

Human Intelligence Integration leveraging advanced listening posts to scour Telegram channels, the dark web, and attacker forums for actionable intelligence and reverse engineering attacks.

Machine Learning of current methods and tactics being discussed to understand the context of the conversation and identify the threat for contextual risk determination.

Integration with existing tech stacks, enabling a comprehensive and cooperative view across the security stack.

Dashboards give your teams the information most important to their work, reducing the overall clutter.

351 Cases - Where Armis Centrix™ for Early Warning flagged CVEs up to 2 years before NIST.

On average, **80% of exploits** are published before the CVEs are released.

Early Warnings have identified an additional **1,200 CVEs** that have no benchmark as NIST is yet to recognize them yet.

98% reduction in the number of vulnerabilities you need to worry about.

Why Healthcare Organizations **Trust Armis to Deliver Better Outcomes**

1. **Superior Threat Detection.** 98% reduction in the number of threats organizations need to worry about with early warning detection.

2. **Reduced Risk to your Critical Operations** with significantly improved security posture and preventive security maintenance.

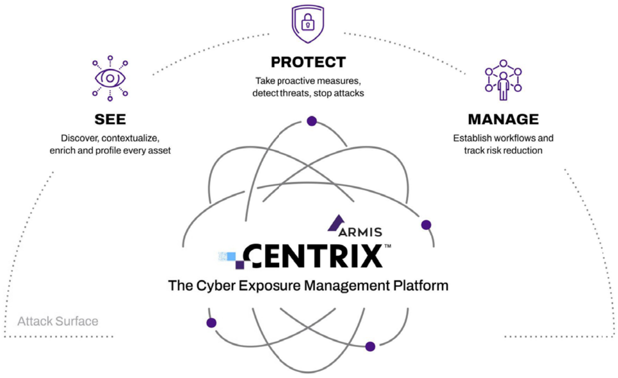
3. **Reduce Attack Likelihood** and minimize uptime disruptions and danger to operators.

4. **Accurate Reconciliation** allows for faster time-to-remediation and instantly identify affected assets, for 20-40x fewer patches and outages.

5. **Reputation and Trust.** OT organizations using Armis are industry leaders upholding best cybersecurity practices.

6. **Speed of Deployment** is critical in OT environments where identifying imminent threats to critical infrastructure is a top priority.

7. **Optimized OT asset Utilization.** Time and usage statistics help determine best maintenance windows, avoiding downtime and production outages.


PROTECT
Take proactive measures, detect threats, stop attacks
SEE
Discover, contextualize, enrich and profile every asset
MANAGE
Establish workflows and track risk reduction
ARMIS CENTRIX™
The Cyber Exposure Management Platform
Attack Surface

Intelligence Centre

Dynamic Honeypots

Dark Web

HumINT

Stop the attack before it happens with Armis Centrix™ for Early Warning

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