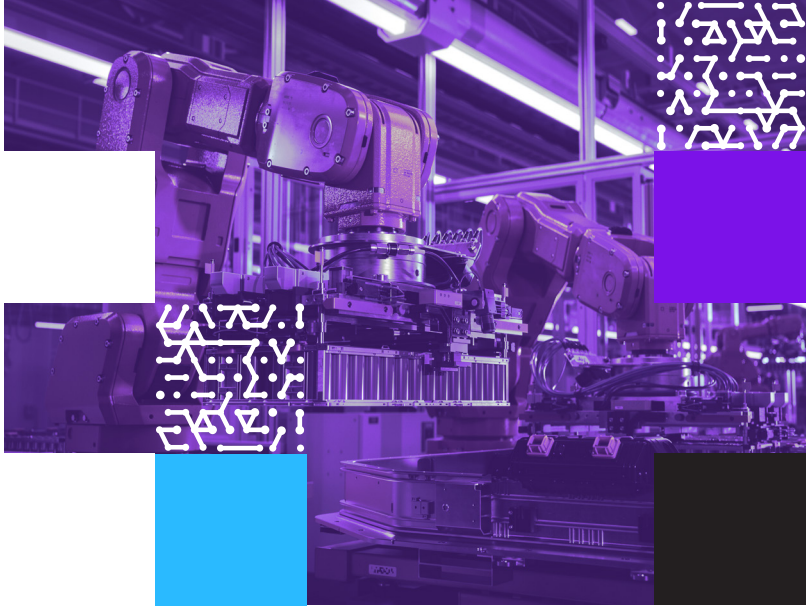
ARMIS

Armis Centrix™ for VIPR - Prioritization and Remediation



for OT/IoT Security.

Go Beyond CVEs

The volume of accumulated vulnerabilities that organizations need to deal with is measured in the millions. Unfortunately, many organizations continue to put more money into revamped versions of stale technologies, or continue to leverage inadequate scoring systems based on the characteristics of vulnerabilities rather than the risk to their business.

Built for OT

Industrial environments and the critical assets within them possess a unique fragility, unable to withstand the traffic generated by typical vulnerability scanners.

Armis Centrix™ goes beyond basic asset discovery, collecting extensive and accurate information about each asset, including its characteristics, configurations, behavior, relationships, and vulnerabilities.

This level of visibility is essential for maintaining a strong cybersecurity posture and operational efficiency within complex OT environments.

Critical VIPR – Prioritization and Remediation Use Cases:

Consolidate

Manually aggregating vulnerabilities from many different sources is a difficult and time consuming task. But with Armis, the consolidation is performed automatically for every asset in the environment.

Contextualize

Assign context to findings including threat intelligence, likelihood of exploit, and asset attributes like environmental information and business impact.

Prioritize

Automate prioritization based on business impact, the severity and likelihood of the exploit. Focus on high-impact fixes that will resolve the largest number of security issues.

Assign and Remediate

Leverage predictive capabilities to determine who is most likely responsible for the asset and the remediation.

Monitor and Report

Track, monitor and demonstrate progress for both individuals tasks, as for overall risk activity and trends in the organization.

Consolidate, Prioritize and Respond to the Vulnerabilities that Matter Most.

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

Key features that make Armis the go to product for Vulnerability Prioritization and Remediation.

Consolidate and Organize Security Findings

Bring order to the chaos, sort findings and group findings based on context and relationships.

Automate Prioritization

Clearly determine remediation priorities based on evaluation of environmental factors, ingested and custom asset labels, and configurable risk severity.

Manage Exceptions Lifecycle

Maintain visibility into remediation progress and automate follow ups for exception requests through one tool.

Centralize Visibility into Risk

Understand how your teams and the tools they are using are performing through a consolidated dashboard, and measure the effectiveness of the remediation process.

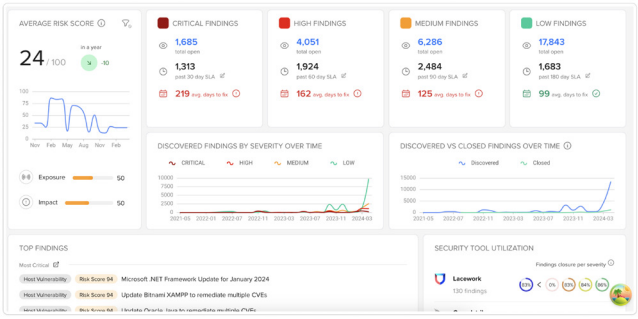
Agentless Solution

which works with all devices, managed and unmanaged, IT or OT/ICS.

Why more businesses are trusting Armis to deliver better outcomes

1. **Focus**
   Reduce security findings volume by 50-1 with ML deduplication.
2. **Efficiency**
   Improve mean time to resolution (MTTR) by as much as 90%.
3. **Future-Proofed Cybersecurity**
   Ready for future digitalisation.
4. **Operational Resilience**
   With Armis organisations are reducing ransomware attacks on their critical infrastructure.
5. **Compliance and Safety**
   Across the entire production process in manufacturing and other OT/ICS industries.
6. **Impactful Actions**
   Assign limited resources to the findings with the highest impact, and measurably reduce risk.

Product Overview



Consolidate, Prioritize and Respond to the Vulnerabilities that Matter Most.

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