ARMIS FEDERAL

Armis + MOSAICS:
Enhanced Situational Awareness for the Warfighter

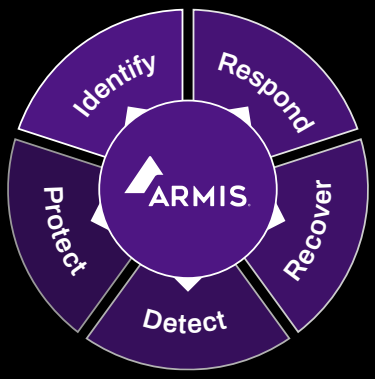
To quickly gain More Situational Awareness for Industrial Control Systems (MOSAICS) you must have the right set of capabilities. These should be integrated into a platform which provides focus and visibility to detect, mitigate, and recover quickly and effectively against all threat levels, from low-risk low impact threats to high risk severe impact threats.

An effective situational awareness platform provides an operational advantage to secure, operate, and defend critical industrial control systems (ICS) assets across the five functions of NIST Cyber Security Framework. Combining these cyber security elements into a unified dashboard enables organizations to understand their security posture in real time; ensuring mission reliability, operational advantage, and protection from non-kinetic attacks.

More Situational Awareness for Industrial Controls Systems

Identify at Scale Simply with Asset Intelligence

Create a unified asset inventory that identifies physical systems as well as software components across IT, OT, IoT, cloud, and legacy systems to identify and understand where critical assets, data, and systems are located. This inventory is a tool for improving the security and resilience of critical ICS. It helps to identify and classify system components based on their criticality and vulnerability. It also helps to evaluate the governance and risk management practices of the system, as well as supply chain risks.



Respond Quickly to Reduce Impact

Quicker response to the identified cyber security incident reduces the impact to the system. The prescribed course of action (COA) includes both manual and automated actions. The responses are determined through assessing the impact of the threat, prioritizing identified vulnerabilities, containing and eradicating the threats, and applying mitigations while maintaining communication across systems.

Protect Thoroughly with IT & OT Optimized Collectors

Protect ICS assets through the implementation of IT and OT optimized collectors. This technology helps protect against a myriad of threats by managing facilities and ICS assets and providing real-time monitoring. Organizations can use this data to measure and prioritize efforts against cyber threats as well as develop and maintain baselines.

Detect Effectively with Anomaly Based Intrusion Detection

Detect potential cyber security events and identify anomalies by collecting, analyzing, and correlating data from sources in real time. Real time continuous monitoring allows for quick identification of changes from baseline configurations, detection of policy violation and anomalous behavior. Input from sources such as network traffic, logs, sensors, and threat intelligence help to visualize affected networks, devices, and the impact of the event.

Recover Efficiently with Focused Action Plan

Recover from incidents efficiently to restore operations and minimize downtime within mission relevant timeframes. Additionally, recovery should include a thorough review of lessons learned that will enhance future decision making and strengthen the overall resilience of the ICS cyber security posture.

Situational awareness of ICS can be accomplished quickly and easily with Armis Centrix™, the Armis Cyber Exposure Management Platform.

ARMIS FEDERAL

Armis: Committed to Securing the Federal Mission with FedRAMP Compliance

Armis understands the unique security challenges faced by federal agencies. That's why we're dedicated to providing the highest level of assurance and compliance with FedRAMP Moderate and IL4 certifications, along with a DoD ATO. This commitment extends beyond just obtaining certifications; it's embedded in our DNA.

Key Benefits of Armis Centrix™

Detect

> Discovers, contextualizes, enriches, and profiles every asset and improves visibility into the ICS network and devices, including legacy and unmanaged assets.

Mitigate

> Provides a faster and more effective response to cyber incidents by contextualizing and understanding ICS devices within the overall network.

Recover

> Integrates and coordinates with existing security and orchestration tools to deliver automated responses to detected vulnerabilities, minimizing downtime.

Asset Intelligence Engine

The Armis Asset Intelligence Engine is our AI-powered knowledge base, monitoring billions of assets worldwide 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. Mapping your entire attack surface is a priority to maintain operational resilience. It enhances the existing configuration management database (CMDB) tool with comprehensive contextual information and ensures the data is always correct and current.

Continuous Monitoring with OT Optimized Sensor

Armis Centrix™ secures and manages OT/IoT networks and assets, ensuring uptime. It thoroughly analyzes every device, assesses risks and behavior, and alerts or blocks suspicious or abnormal devices with NAC and firewall integrations. The Armis platform analyzes device behavior to identify risks and detect cyber attack techniques. The platform is cloud-based, flexible, and integrates easily with your existing network and security products with minimal disruption.

Anomaly Based Intrusion Detection

Armis Centrix™ empowers organizations to efficiently gain deep situational awareness and track and manage their assets across diverse environments, ensuring optimal utilization and cost-effectiveness. It then monitors for vulnerabilities and compliance issues in real time to make detection and anomalies easier to prioritize and manage. Armis Centrix™ does not utilize any kind of active scanning or probing because such methods are potentially dangerous to ICS devices. Instead it passively monitors wired and wireless traffic to identify each device to understand its behavior without disruption. Each asset is assigned a risk score based on severity and impact of vulnerabilities. Vulnerabilities can be prioritized by risk, assets, and business context.

Quick Response, Quicker Mean Time to Recovery

Armis Centrix™ tracks behavior against "known good" baselines to provide quick responses to anomalous behavior. It analyzes this data by using device profiles and characteristics stored in the Armis Asset Intelligence Engine to assess each device's risk, detect threats, and block threats automatically. It can automatically block, quarantine, or disconnect devices that pose a risk or show malicious activity, based on network policies.

Recovery-focused Action Plan

Armis Centrix™ delivers and implements a security strategy that covers all assets to restore operations efficiently and quickly. Vulnerabilities can be quickly detected and remediated with automated tools and workflows that improve recovery time. Risk reduction and process efficiency can be tracked with the platform, improving COA decisions.