ARMIS®

WHITEPAPER

How Armis supports the MITRE ATT&CK® for ICS

Overview

Industrial Control Systems (ICS) are the backbone of critical infrastructure, including energy, manufacturing, and utilities. These systems, which were once isolated, are now interconnected with IT networks and the broader internet, increasing their exposure to sophisticated cyber threats. Recognizing the growing complexity and criticality of securing ICS/OT environments, MITRE ATT&CK® for ICS provides a comprehensive framework for understanding adversarial behavior specific to these systems.

This guide is designed for cybersecurity professionals, OT engineers, and executives seeking to strengthen their ICS security posture by operationalizing the MITRE ATT&CK® framework with the support of Armis technology—enabling better preparedness and faster incident response for securing operational technology (OT) environments.

Table of Contents

Introduction

Industrial Control Systems (ICS) are increasingly vulnerable to cyberattacks. Recent attacks on ICS systems have highlighted the evolving threat landscape. In 2023, a ransomware attack targeted an Eastern European energy provider, causing operational disruptions in power distribution. In 2024, a major steel manufacturer experienced downtime due to malware infiltrating their ICS network, demonstrating the increasing sophistication of attacks against manufacturing sectors. These incidents underline the urgent need for proactive measures to secure critical infrastructure.

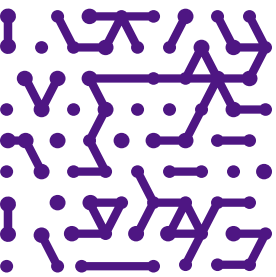
66%

of manufacturers have experienced a security incident related to IoT or ICS devices over the past two years.

The attacks are not limited to large enterprises. According to a commissioned study conducted by Forrester Consulting on behalf of Armis, 66% of manufacturers have experienced a security incident related to IoT or ICS devices over the past two years.

To help combat this increasingly concerning issue, The MITRE Corporation has developed version 20 of their highly popular MITRE ATT&CK® for ICS framework, released in October 2023. This updated version enhances its focus on Industrial Control Systems.

Unlike previous ATT&CK® frameworks that were oriented towards traditional and mobile computing environments, the ATT&CK® for ICS is designed to help enterprise security practitioners understand adversary behavior and plan appropriate security systems tailored to the unique challenges of operational technology (OT) and ICS environments. This latest version includes new techniques, sub-techniques, and mitigations specific to modern ICS threats, enabling better alignment between security strategies and the evolving threat landscape.



In this guide, you'll learn how to align with MITRE ATT&CK® for ICS to:

1. Deliver Holistic Visibility Across All Assets
2. Provide Contextualized Threat Insights
3. Support Proactive Defense Strategies
4. Enable Efficient Incident Response

The security challenge for industrial control systems

The United States National Institute of Standards and Technology (NIST) defines ICS as:

> "An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes."

There are a wide range of ICS devices, some of which include:

- Process Control Systems (PCS)
- Distributed Control Systems (DCS)
- Supervisory Control and Data Acquisition (SCADA) Servers/Clients
- Programmable Logic Controllers (PLC)
- Human Machine Interface (HMI)
- Manufacturing Execution Systems (MES)
- Field Devices
- IT/ICS Boundary interfaces

Many people refer to these environments as "operational technology" or OT environments. In this white paper, we shall use the term ICS simply to remain consistent with the term used by MITRE, but we view the terms as largely interchangeable. Historically, ICS environments were relatively safe from cyberattacks because ICS devices were installed in isolated or "air-gapped" networks, and because many of the devices were obscure and therefore unknown and untargeted by most attackers.

All of this is changing. Control system architectures are being connected to traditional enterprise IT networks (Ethernet, Wi-Fi, etc.), and device manufacturers are building ICS devices on top of common operating systems such as Windows, Linux, Android, and VxWorks. These changes increase the risk that ICS can be compromised by the same kind of attacks used to compromise devices on corporate IT networks.

The following are some of the reasons why maintaining security for ICS environments is increasingly challenging.

The Increasing Challenges of Maintaining Security for ICS Environments

Unpatchable

ICS devices typically do not allow for root access or the installation of agents required to monitor and protect them. These devices often run proprietary or highly specialized operating systems that are incompatible with traditional endpoint protection tools used in IT environments. This lack of agent compatibility prevents the deployment of standard cybersecurity solutions, leaving ICS devices vulnerable to threats that are commonly addressed in IT settings.

Disruptable

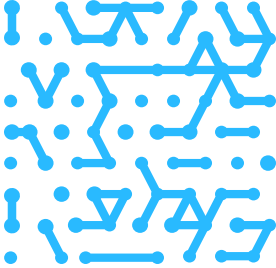
Traditional methods for device discovery and vulnerability scanning, such as network scans (e.g., NMAP), can disrupt the normal operation of ICS devices. These devices are not designed to tolerate the kind of active probing or scanning that is standard practice on IT networks. In many cases, scanning ICS devices poses a risk to critical operations, making such assessments prohibited in most ICS environments. This creates a significant challenge in maintaining visibility into the security posture of ICS devices.

Accessible

ICS devices were historically designed with the assumption they would operate in isolated or highly controlled environments. Many of these devices were built with minimal cybersecurity protections, assuming they would not be connected to broader networks. However, as these devices become increasingly interconnected within modern operational networks, their original security models are not sufficient to withstand sophisticated cyberattacks.

ICS Security Challenges

- Unpatchable
- Unagentable
- Disruptable
- Accessible
- Proprietary Protocols
- Proliferation



Proprietary Protocols

Many ICS devices operate using proprietary communication protocols, often to optimize performance or reduce processing overhead. These proprietary protocols have not undergone the same rigorous security testing, peer reviews, or development standards as widely used, standardized protocols. As a result, they are prone to vulnerabilities and threats that can be difficult to identify and address. Additionally, because these protocols are niche, they are rarely the focus of the broader cybersecurity research community, meaning vulnerabilities in ICS-specific protocols may not be well-documented in vulnerability databases like CVE. This creates an additional layer of risk for organizations managing ICS devices.

Proliferation

The rapid growth of the Internet of Things (IoT) has led to a dramatic increase in the number and variety of ICS devices. This proliferation has heightened the competitive pressures to deliver devices quickly and at lower costs. As a result, manufacturers may prioritize speed to market over thorough testing and security development. This shift has led to a broader range of security challenges, including devices with insufficient or outdated security controls, creating a complex environment for defenders. Moreover, the expansion of IoT into critical infrastructure introduces new risks, as many ICS devices were never designed with the security requirements necessary for modern interconnected systems.

These factors together underscore the complex security landscape that organizations must navigate in securing their ICS environments. Given the unique challenges of these systems, understanding the evolving threat landscape, identifying which adversaries are targeting ICS, and implementing appropriate mitigations has never been more critical. In this context, frameworks like MITRE's ATT&CK® for ICS provide valuable insights into how adversaries exploit ICS vulnerabilities and how organizations can better defend against these emerging threats.

The MITRE ATT&CK® Framework

The MITRE ATT&CK® (Adversarial Tactics, Techniques, and Common Knowledge) framework is a methodology that is widely used in cybersecurity to document and categorize the Tactics, Techniques and procedures (TTPs) of adversaries during cyberattacks. It is designed to help organizations understand and defend against these attacks.

Key goals of the framework include

1. **Understanding Adversary Behavior:** The framework outlines the various stages of an attack, from initial access to actions taken after achieving objectives, such as exfiltrating data or disrupting operations. It categorizes adversarial tactics and techniques.
2. **Threat Intelligence Sharing:** MITRE ATT&CK® is used to standardize the way threat intelligence is shared across the cybersecurity community. By using a common framework, analysts and organizations can better communicate and collaborate when discussing TTPs used by cyber adversaries. Sharing knowledge helps build a collective defense strategy across the security community.
3. **Improving Detection and Response**: The framework provides organizations with detailed information on the methods attackers use to exploit systems and evade detection. Security teams can use this information to identify gaps in their defenses, improve detection mechanisms, and fine-tune incident response plans.
4. **Red and Blue Team Exercises**: MITRE ATT&CK® is often used in red teaming and blue teaming. By emulating the tactics and techniques described in the framework, red teams can mimic realistic adversary behavior, while blue teams can strengthen their defensive posture based on real-world attack patterns.
5. **Enhancing Security Posture:** The ATT&CK® framework helps organizations assess their cybersecurity maturity by mapping existing security controls and processes to the techniques in the framework. This allows them to identify which tactics and techniques they may be vulnerable to and take proactive steps to mitigate those risks.
6. **Promoting a Common Language for Cybersecurity**: ATT&CK® provides a standardized vocabulary for describing attack behaviors, helping security professionals across different industries and regions communicate more effectively.
7. **Supporting Cyber Resilience**: By using the ATT&CK® framework, organizations can improve their overall resilience to cyberattacks. It offers a proactive approach to security by allowing teams to anticipate, detect, and respond to attacks quickly. The framework also supports a continuous improvement cycle where security practices can evolve based on emerging threats and attack trends.

While many of these tactics and the underlying 94 techniques share the same names as the ones contained in MITRE's enterprise ATT&CK® framework, the detailed descriptions of the tactics and techniques have been tailored specific to ICS devices. Each technique may be associated with one or more tactics if they have the capability to support different adversarial objectives

The new MITRE ATT&CK® for ICS

MITRE has published two versions of the ATT&CK® for ICS framework:

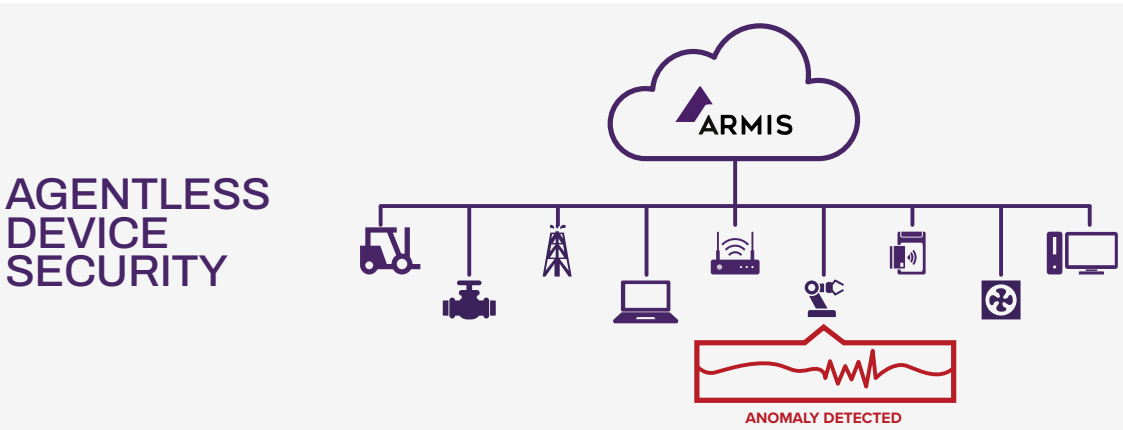
1. **Version 1.0** was the first version of the ATT&CK® framework specifically focused on industrial control systems (ICS). It provided a foundational structure for understanding adversary behaviors and tactics in ICS environments.
2. **Version 2.0** (the current version) was released in October 2023. This version includes updates and additions to better capture the evolving landscape of ICS cybersecurity threats, including more refined tactics and techniques, and greater alignment with emerging threats in the ICS domain.

ATT&CK® for ICS lists the following tactics:

1. **Initial Access** – Gaining access to an ICS environment, often through vulnerabilities in devices or network infrastructure.
2. **Execution** – Running malicious code or commands on ICS systems, typically to manipulate operations or carry out further attacks.
3. **Persistence** – Maintaining long-term access to ICS systems, ensuring that an attacker can continue operations or remain undetected.
4. **Privilege Escalation** – Gaining higher-level permissions or access within ICS devices or networks to further exploit the system.
5. **Defense Evasion** – Using techniques to avoid detection or bypass security measures implemented within the ICS environment.
6. **Credential Access** – Stealing or obtaining valid credentials to access systems within the ICS network.
7. **Discovery** – Identifying the configuration of ICS systems, network layout, and vulnerabilities within the environment.
8. **Lateral Movement** – Moving within the network or ICS environment to gain access to other devices or systems.
9. **Collection** – Gathering information, data, or control information from ICS systems to further the attack.
10. **Command and Control** – Establishing communication channels to issue commands or exfiltrate data from compromised systems.
11. **Exfiltration** – Extracting data or critical information from the ICS environment, usually for espionage or sabotage purposes.
12. **Impact** – Affecting or disrupting the ICS systems, including causing physical damage, data loss, or system shutdowns.

Armis provides comprehensive coverage for ATT&CK® for ICS

Armis helps organizations align with **MITRE ATT&CK® for ICS** by offering Armis Centrix™ a robust, unified platform designed to address the unique security needs of Industrial Control Systems (ICS) across all stages of an attack lifecycle. By integrating asset discovery, continuous monitoring, and real-time threat detection, Armis enables organizations to identify and mitigate adversary tactics and techniques as outlined in the MITRE ATT&CK® for ICS framework. The platform's deep visibility into both managed and unmanaged ICS devices allows for effective detection of threats during the **Initial Access** and **Execution phases**, even for devices that cannot be easily scanned or patched. Through its agentless approach, Armis can monitor and assess the behavior of ICS devices, detecting deviations that may indicate **Evasion, Lateral Movement, or Command and Control activities**. Armis also supports Discovery and Collection by identifying network and device configurations, enabling teams to understand potential vulnerabilities, risk and sensitive data flows. By leveraging advanced AI-powered automation and integrating seamlessly with security operations, Armis helps mitigate **Impact, Inhibit Process Control, and Inhibit Response Function** tactics, ensuring ICS resilience in the face of evolving cyber threats. Armis Centrix™ arms organizations with the robust capabilities ability to continuously assess security posture across critical infrastructure allows organizations to respond swiftly to emerging threats, fulfilling the need for comprehensive ICS cybersecurity coverage within the **MITRE ATT&CK® for ICS** framework.



The table below lists all of the ATT&CK® for ICS techniques organized by tactic. The darker purple represents techniques that Armis can detect at inception, and the lighter purple represents the techniques that Armis can detect subsequently, or where Armis may be one of many indicators necessary to validate that the technique has occurred. Each technique is further described following this table.

ATT&CK® for ICS Techniques

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Drive-by Compromise	Autorun Image	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in -the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Change Operating Mode	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
External Remote Services	Command-Line Interface	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
Internet Accessible Device	Execution through API	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Remote Services	Graphical User Interface	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss of Control
Replication Through Removable Media	Hooking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
Rogue Master	Modify Controller Tasking			System Binary Proxy Execution		Valid Accounts	Monitor Process State Point & Tag Identification		Data Destruction		Loss of Protection
Spearphishing Attachment	Native API						Program Upload		Denial of Service		Loss of Safety
Supply Chain Compromise	Scripting						Screen Capture		Device Restart/ Shutdown		Loss of View
Transient Cyber Asset	User Execution						Wireless Sniffing		Manipulate I/O Image		Manipulation of Control
Wireless Compromise									Modify Alarm Settings		Manipulation of View
									Rootkit		Theft of Operational Information
									Service Stop		
									System Firmware		

Techniques that Armis can **detect at inception**

Techniques that Armis can **detect subsequently**, or where Armis may be one of many **indicators necessary to validate**

* Technique is used in two different tactics

** Technique is used in three different tactics

For brevity, we are not duplicating full descriptions of each Tactic or Technique. Further details on each of these methods are available at

https://collaborate.mitre.org/attackics/index.php/All_Techniques.

ATT&CK® Tactic: Initial Access

The adversary is trying to get into your ICS environment.

MITRE ATT&CK® Tactic	Technique Number	How Armis Helps
Drive-by Compromise	**T0817**	Identifies risky or unauthorized access to malicious websites, correlates anomalous device behaviors, and blocks access using threat intelligence feeds.
Exploit Public-Facing Application	**T0819**	Continuously monitors for vulnerabilities, alerts on exposed systems, and prioritizes mitigations through vulnerability deduplication and prioritization. Connects find to fix.
Exploitation of Remote Services	**T0866**	Detects unauthorized access attempts, monitors device behavior, and enforces granular least-privilege access and Zero Trust through IAM integration.
External Remote Services	**T0822**	Maps connections to external services, detects anomalies, and identifies shadow IT usage of unauthorized remote services.
Internet Accessible Device	**T0883**	Identifies internet-accessible devices in real time, assesses vulnerabilities, and blocks unauthorized access with firewall/NAC integration and micro-segmentation capabilities.
Remote Services	**T0886**	Monitors traffic for suspicious activities, alerts on unauthorized access, and detects compromised endpoints.
Replication Through	**T0847**	Detects unauthorized or suspicious removable media usage, alerts on unusual traffic flows and file transfers. Provides detailed audit trails.
Removable Media Rogue Master	**T0848**	Identifies unauthorized master devices, detects configuration changes, and prevents rogue devices from interacting with critical systems.
Spearphishing Attachment	**T0865**	Detects behaviors consistent with payload execution, integrates with email security tools, and isolates impacted endpoints.
Supply Chain Compromise	**T0862**	Monitors third-party integrations for anomalies and policy violations. Identifies vulnerabilities in supply chain devices and provides risk assessments. device on customers' networks. Armis compares every device's real-time activity to the established and "known-good" activity baseline for the specific device which is stored in our Device Knowledge Base. When abnormal behavior in the network is detected, Armis updates the risk score based on asset criticality and generates a security alert.
Transient Cyber Asset	**T0864**	Discovers and monitors transient assets, flags unapproved devices or operations. Enforces security through NAC and endpoint protection integration.
Wireless Compromise	**T0860**	Detects rogue access points, monitors wireless communication for anomalies, and provides full visibility into wireless environments. Armis monitors all communications in the 2.3 and 5 GHz frequency spectrum which is used by Wi-Fi, Bluetooth, BLE, Zigbee, and other peer-to-peer protocols. Through this monitoring, Armis is able to detect and alert on unauthorized devices and unexpected or malicious wireless activity.

ATT&CK® Tactic: Execution

The adversary is trying to run malicious code.

MITRE ATT&CK® Tactic	Technique Number	How Armis Helps
Autorun Image	**T0895**	Monitors for unauthorized modifications to device configurations, including autorun scripts or processes, and alerts on suspicious changes.
Change Operating Mode	**T0858**	Tracks changes in device states or operating modes, detects anomalous behavior in OT/ICS environments, and prevents unauthorized mode transitions through integration with policy enforcement tools.
Command-Line Interface	**T0807**	Detects and logs unusual or unauthorized command-line activities and unauthorized personnel. Correlates commands with threat intelligence and early warning data. Provides forensic data for investigation.
Execution through API	**T0871**	Monitors API calls for abnormal patterns, unauthorized usage, or potential malicious payloads, ensuring only legitimate API interactions occur.
Graphical User Interface	**T0823**	Provides visibility into GUI-based activities, detecting unusual user interactions and potential exploitation attempts, especially in ICS and OT environments.
Hooking	**T0874**	Identifies and alerts on suspicious hooking attempts on processes or device drivers, leveraging behavior-based detection to prevent malicious activity.
Modify Controller Tasking	**T0821**	Tracks and logs changes to controller tasking in OT environments, ensures compliance with policies, and prevents unauthorized modifications through policy enforcement.
Native API	**T0834**	Monitors interactions with native APIs to detect suspicious or anomalous behaviors, such as malware leveraging low-level APIs for execution.
Scripting	**T0853**	Identifies unauthorized or suspicious script executions, blocks known malicious scripts through integration with threat intelligence feeds and provides full script visibility for analysis.
User Execution	**T0863**	Detects malicious files or payloads initiated by users, alerts on anomalous behaviors triggered by user interactions, and integrates with endpoint and security tools to mitigate risks from phishing or malware execution.

ATT&CK® Tactic: Persistence

The adversary is trying to maintain their foothold in your ICS environment.

MITRE ATT&CK® Tactic	Technique Number	How Armis Helps
Hardcoded Credentials	**T0891**	Detects and alerts on the use of default or hardcoded credentials across devices, identifies exposed credentials, and enforces password hygiene policies.
Modify Program	**T0889**	Monitors and detects unauthorized program modifications, such as binaries or scripts being altered, and alerts on anomalous changes using behavior-based detection.
Module Firmware	**T0839**	Monitors firmware and codeplug integrity for connected devices, detects unauthorized modifications, and enforces firmware update policies to prevent persistence through module firmware.
Project File Infection	**T0873**	Detects suspicious modifications or infections in project files, monitors file integrity, and alerts on unusual behaviors linked to infected project files.
System Firmware	**T0857**	Continuously monitors system firmware for integrity violations, detects anomalous firmware updates, and ensures compliance with secure boot policies to prevent unauthorized persistence mechanisms.
Valid Accounts	**T0859**	Detects unauthorized account usage or anomalies in account behavior, identifies credential misuse, and integrates with identity and access management solutions to enforce least-privilege (Zero Trust) and multi-factor authentication.

ATT&CK® Tactic: Privilege Escalation

The adversary endeavors to gain additional privileges to take system command and control.

MITRE ATT&CK® Tactic	Technique Number	How Armis Helps
Exploitation for Privilege Escalation	**T0890**	Detects exploitation attempts targeting vulnerabilities that enable privilege escalation, monitors for anomalous activities post-exploitation, and integrates with vulnerability management to proactively identify, deduplicate, prioritize, assign and remediate known security findings.
Hooking	**T0874**	Identifies suspicious hooking activities, such as malicious attempts to intercept API calls or modify processes, and alerts on abnormal behaviors indicative of privilege escalation attempts.

ATT&CK® Tactic: Evasion

The adversary is trying to avoid being detected.

MITRE ATT&CK® Tactic	Technique Number	How Armis Helps
Change Operating Mode	**T0858**	Tracks and detects unauthorized changes to device operating modes, particularly in OT environments, alerts on deviations from normal behavior, and enforces policies to prevent privilege escalation through mode changes.
Exploitation for Evasion	**T0820**	Detects exploitation attempts targeting vulnerabilities used for privilege escalation and evasion, monitors anomalous behaviors, and integrates with threat intelligence to block known exploitation methods as well as lateral (east-west) creep of an attack.
Indicator Removal on Host	**T0872**	Monitors devices for activities indicating attempts to delete logs, artifacts, or traces of malicious activity, and alerts on unusual behaviors that suggest tampering with evidence of compromise.
Masquerading	**T0849**	Detects suspicious file names, process names, or execution paths designed to mimic legitimate software, leveraging behavioral baselines to identify masquerading attempts.
Rootkit	**T0851**	Monitors for the presence of rootkits by identifying kernel-level modifications, hidden processes, or unauthorized changes to critical system components (eg: backplane manipulation), ensuring real-time detection and alerting.
Spoof Reporting Message	**T0856**	Tracks and detects spoofed reporting messages in devices, especially in OT/ICS environments, to prevent attackers from misleading system administrators or gaining elevated privileges.
System Binary Proxy Execution	**T0894**	Identifies unauthorized usage of legitimate system binaries to execute malicious payloads, ensuring abnormal execution behaviors are flagged and investigated.

ATT&CK® Tactic: Discovery

The adversary is trying to figure out your ICS environment.

MITRE ATT&CK® Tactic	Technique Number	How Armis Helps
Network Connection Enumeration	**T0840**	Armis provides real-time, deep visibility into network connections, identifying and mapping all assets (both physical and virtual), including unauthorized devices, to mitigate risks from connection enumeration.
Network Sniffing	**T0842**	Armis leverages multi-detection engine monitoring to detect unauthorized sniffing and other suspicious activities, ensuring network traffic is analyzed without disruptive active probes.
Remote System Discovery	**T0846**	Detect and monitor devices making remote connections to the network, ensuring all remote systems are known and validated to prevent unauthorized access.
Remote System Information Discovery	**T0888**	Identify devices accessing the network remotely and provides visibility into their configurations, aiding in the detection of malicious or unauthorized remote system discovery.
Wireless Sniffing	**T0887**	Monitors wireless networks and connected devices, helping organizations detect and prevent unauthorized sniffing of network traffic, including IT, IoT, and OT devices and assets.

ATT&CK® Tactic: Lateral Movement

The adversary is trying to get into your ICS environment.

MITRE ATT&CK® Tactic	Technique Number	How Armis Helps
Default Credentials	**T0812**	Continuously monitor devices for the use of default or weak credentials, helping to detect unauthorized access and preventing lateral movement using such credentials.
Exploitation of Remote Services	**T0866**	Armis identifies vulnerabilities and misconfigurations in remote services, enabling real-time alerts and allowing rapid mitigation to prevent exploitation during lateral movement.
Hardcoded Credentials	**T0891**	Detect abnormal network behavior and unauthorized connections, identifying hardcoded credentials being exploited for lateral movement within the organization.
Lateral Tool Transfer	**T0867**	Track the movement of tools across the network, alerting on any unauthorized transfer of lateral movement tools between devices, ensuring rapid detection and response.
Program Download	**T0843**	Armis detects suspicious activity by monitoring network traffic for unauthorized or unusual program downloads, providing insights into potential lateral movement tools.
Remote Services	**T0886**	Armis detects remote service access by continuously monitoring and validating legitimate connections, ensuring that only authorized remote services and processes are in use during lateral movement.
Valid Accounts	**T0859**	Identify valid account usage and suspicious login patterns across the network, helping to detect lateral movement attempts using compromised credentials.

ATT&CK® Tactic: Collection

The adversary is trying to gather data of interest and domain knowledge on your ICS environment to inform their goal.

MITRE ATT&CK® Tactic	Technique Number	How Armis Helps
Adversary-in-the-Middle	**T0830**	Detect suspicious network traffic and potential man-in-the-middle (MITM) attacks by monitoring communication flows and alerting on anomalies or policy violations that could indicate interception.
Automated Collection	**T0802**	Provide visibility into automated processes running on devices across the network, helping detect automated collection activities that could gather sensitive data.
Data from Information	**T0811**	Monitor data access and retrieval patterns from internal information repositories, detecting unauthorized access to sensitive data stored on networked systems.
Repositories Data from Local	**T0893**	Track data transfers from local systems, identifying suspicious data extraction or movements from individual machines to ensure sensitive data is not being exfiltrated.
System Detect Operating	**T0868**	Detect changes in device or network behavior, identifying when systems transition between different operating modes that may signal data collection or compromise activities.
Mode	**T0877**	Armis monitors input/output activity on devices, ensuring any unauthorized data image creation or manipulation is detected across endpoints and critical infrastructure.
I/O Image	**T0801**	Continuously monitor process activity on devices, detecting when unusual or unauthorized processes are active, indicating potential collection of sensitive data.
Monitor Process State	**T0861**	Identify network activity and device tagging behaviors, helping detect attempts to mark or label devices for future collection or attack.
Point & Tag Identification	**T0845**	Track and alert on unauthorized program uploads or file transfers across the network, helping detect data exfiltration programs that may facilitate the collection of sensitive information.
Program Upload Screen Capture	**T0852**	Detect anomalies in screen-sharing or screenshot activity across endpoints, alerting on potential screen capture attempts used to gather sensitive data.
Wireless Sniffing	**T0887**	Identify unauthorized wireless sniffing by continuously monitoring wireless network traffic and connected devices, preventing data capture by unauthorized actors.

ATT&CK® Tactic: Command & Control

The adversary is trying to communicate with and control compromised systems, controllers, and platforms with access to your ICS environment.

MITRE ATT&CK® Tactic	Technique Number	How Armis Helps
Commonly Used Port	**T0885**	Armis continuously monitors network traffic across the organization, identifying anomalous traffic over commonly used ports, such as HTTP/ HTTPS or SMB, which are often used for C2 communications.
Connection Proxy	**T0884**	Detect the use of proxies or unusual network routes that could be used for command and control, alerting on devices using unauthorized proxy servers or hidden communication pathways.
Standard Application Layer Protocol	**T0869**	Monitor network traffic and detects the use of standard application layer protocols (such as HTTP, DNS, or SMTP) for C2 communications, identifying unauthorized uses of these protocols for C2 activity.

ATT&CK® Tactic: Inhibit Response Function

The adversary is trying to prevent your safety, protection, quality assurance, and operator intervention functions from responding to a failure, hazard, or unsafe state.

MITRE ATT&CK® Tactic	Technique Number	How Armis Helps
Activate Firmware Update Mode	**T0800**	Detect suspicious attempts to enter firmware update mode, alerting on any unauthorized changes to device firmware or update behaviors, helping prevent exploitation.
Alarm Suppression	**T0878**	Continuously monitor security alerts and alarms across devices and networks, identifying attempts to suppress or disable alarm systems and ensuring proper responses.
Block Command Message	**T0803**	Monitor communication channels and network traffic for blocked or altered command messages, helping detect unauthorized attempts to disrupt control commands.
Block Reporting Message	**T0804**	Armis detects when reporting messages from critical devices are blocked or altered, ensuring that security teams receive proper notifications and alerts in the event of attacks.
Block Serial COM	**T0805**	Monitors serial communication ports (COM ports) and can detect blocking attempts, ensuring secure communication channels are not compromised by malicious actors.
Change Credential	**T0892**	Identify when credentials are changed or compromised by monitoring authentication patterns and detecting unusual login attempts or credential changes across devices.
Data Destruction	**T0809**	Visibility into data deletion and destruction activities, alerting security teams to unauthorized attempts to erase critical data or files on devices.
Denial of Service	**T0814**	Armis tracks network and device health, identifying signs of a denial-of-service attack, and helping prevent or mitigate network disruptions caused by malicious traffic.
Device Restart/ Shutdown	**T10816**	Detect abnormal device restarts or shutdowns by tracking system uptime and shutdown events, ensuring unauthorized reboots are flagged immediately.
Manipulate I/O Image	**T0835**	Monitor input/output activity on devices and alerts when malicious manipulation of I/O images is detected, protecting against unauthorized changes to data or settings.
Modify Alarm Settings	**T0838**	Identify attempts to modify alarm configurations or settings, ensuring that critical alarms remain active and alert security teams to malicious changes.
Rootkit	**T0851**	Detect hidden processes and unusual system behaviors that may indicate the presence of a rootkit, helping to identify and mitigate rootkit threats in real time.
Service Stop	**T0881**	Continuously monitor active services on devices, alerting on any unauthorized service stops or modifications that could impact the security posture of a network.
System Firmware	**T0857**	Deep visibility into system firmware and tracks changes or unauthorized updates, helping detect malicious firmware modifications that could compromise device integrity.

ATT&CK® Tactic: Impair Process Control

The adversary is trying to manipulate, disable, or damage physical control processes.

MITRE ATT&CK® Tactic	Technique Number	How Armis Helps
Brute Force I/O	**T0806**	Armis monitors I/O operations on devices and can detect patterns indicative of brute force attacks, alerting on unusual or repetitive input/output actions that may signal an attempt to compromise process control.
Modify Parameter	**T0836**	Track device configurations and settings, identifying any unauthorized modifications to critical parameters that could impact the performance or safety of process control systems.
Module Firmware	**T0839**	Visibility into system firmware and modules, detecting unauthorized modifications or updates to firmware that may impair process control operations and potentially introduce vulnerabilities.
Spoof Reporting Message	**T0856**	Detect anomalies in device reporting messages, identifying attempts to spoof or manipulate reporting mechanisms, ensuring accurate reporting for process control systems.
Unauthorized Command Message	**T0855**	Monitor command messages sent across the network, identifying any unauthorized or malicious command messages targeting process control systems, thus preventing malicious interference.

ATT&CK® Tactic: Impact

The adversary is trying to manipulate, interrupt, or destroy your ICS systems, data, and their surrounding environment.

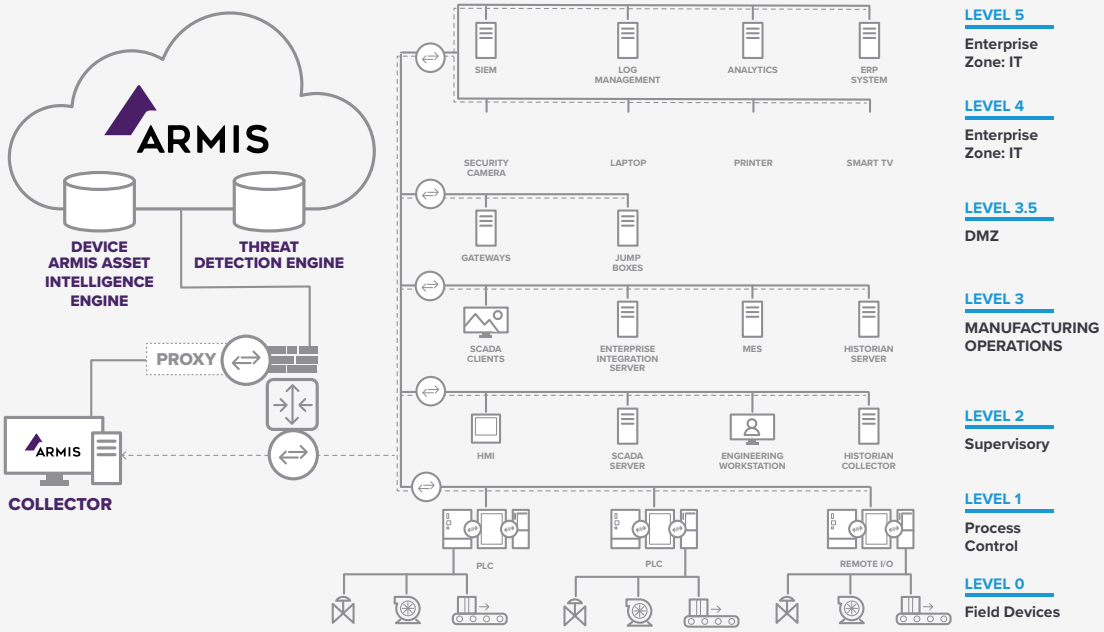
NOTE: The techniques MITRE lists within the Impact section are generally different than the techniques listed in the previous sections. Many of these techniques describe a business impact or a physical impact, not a specific detectable or observable action, but rather an effect of the technique being used. Generally, Armis Centrix™ will not be able to detect the impact (e.g. property damage), but it can help a customer avoid, provide telemetry, or recover from these impacts as described below.

MITRE ATT&CK® Tactic	Technique Number	How Armis Helps
Damage to Property	**T0879**	Detects malicious behaviors that could result in damage to property, including unauthorized access to critical devices or systems, helping to prevent physical (safety) and operational damage.
Denial of Control	**T0813**	Track and alert on anomalies in network traffic or device behavior that suggest a denial of control, ensuring that process or operational control is not hijacked or impaired.
Denial of View	**T0815**	Visibility by monitoring data flow and device connections, alerting when attackers attempt to obscure or prevent visibility into critical systems, preventing a loss of oversight.
Loss of Availability	**T0826**	Monitor devices and networks for signs of Denial of Service (DoS) attacks or other disruptions, ensuring that critical systems maintain availability and are not taken offline.
Loss of Control	**T0827**	Real-time alerts when unauthorized control of critical systems or devices is detected, helping to prevent attackers from compromising control or disrupting operations.
Loss of Productivity and Revenue	**T0828**	Prevent attacks that could disrupt business operations, such as ransomware or denial of service, ensuring that productivity and revenue streams are not negatively impacted.
Loss of Protection	**T0837**	Identify and alerts when security measures are disabled or bypassed, helping to ensure that critical systems maintain their protective mechanisms and remain secure.
Loss of Safety	**T0880**	Armis detects any attempts to manipulate or disable safety systems, alerting on potential changes that could put operational safety at risk, ensuring these systems remain intact.
Loss of View	**T0829**	Assurance that systems maintain visibility into network activity and critical devices, alerting when attacks are launched to obscure or block essential data and operational views.
Manipulation of Control	**T0831**	Monitor control messages, detecting any attempts to manipulate or alter control communications, ensuring the integrity of operational command.
Manipulation of View	**T0832**	Track data integrity and reporting flows, detecting when attackers attempt to manipulate system views by altering or blocking reporting, ensuring transparency and oversight.
Theft of Operational Information	**T0882**	Monitors and alert on unauthorized access or exfiltration of sensitive operational data, helping to prevent theft of critical business or operational information.

Deploying Armis to protect ICS

Armis enables organizations to safeguard their ICS environments through:

- **Comprehensive Asset Discovery and Visibility:** Armis offers real-time, agentless discovery of every connected device in an ICS environment. This includes operational technology (OT), IT, IoT, and medical device assets, creating a complete and continuously updated inventory. With granular insights into asset behavior, firmware versions, communication protocols, and vulnerabilities, Armis ensures no device goes unnoticed or unmonitored.
- **Risk Assessment and Cyber Exposure Management:** Using its extensive threat intelligence database and advanced analytics, Armis identifies vulnerabilities, misconfigurations, and deviations from normal behavior that could signal a security risk. This proactive approach ensures that organizations can prioritize and address critical exposures before they lead to system compromise.
- **Continuous Monitoring and Threat Detection:** ICS environments require non-intrusive monitoring to avoid disrupting sensitive operations. Armis uses passive traffic analysis and AI-driven anomaly detection to identify indicators of compromise, unauthorized access, or lateral movement. The platform instantly alerts security teams to suspicious activity while providing actionable insights to mitigate risks.
- **Incident Response and Remediation:** Armis facilitates swift and effective incident response by integrating with security tools like SIEM, SOAR, and EDR. This ensures that threats are contained without impacting operational continuity, helping organizations recover quickly from security events.



Armis Intergrations

Armis Centrix™ is designed to provide unparalleled visibility and security for Industrial Control System (ICS) environments by fully integrating with all connected devices. From SCADA (Supervisory Control and Data Acquisition) systems and DMI (Dynamic Machine Interfaces) to PLCs (Programmable Logic Controllers), DCS (Distributed Control Systems), IoT devices, and traditional IT assets, Armis provices comprehensive coverage without requiring agents or causing operational disruption.

How Armis Centrix™ Integrates Across ICS and IT

- **SCADA and DCS Systems -** Armis monitors SCADA and DCS systems to provide real-time insights into operational data flows, configurations, and behaviors, ensuring these critical components remain secure from unauthorized changes and malicious activity.
- **PLCs and DMIs -** By analyzing network traffic and via optional smart active querying, Armis discovers and monitors PLCs and DMIs, identifying vulnerabilities, firmware issues, or abnormal command execution while ensuring no interference with sensitive operations.
- **IoT and IIoT Devices -** Armis extends its reach to IoT and IIoT devices, recognizing unique protocols and communication patterns. This ensures visibility into devices like sensors, actuators, and connected machinery, which are often overlooked by traditional security solutions.
- **IT Assets -** Armis seamlessly integrates with IT systems, including servers, workstations, and networking equipment, providing unified visibility and security for hybrid environments that blend IT and OT operations.

The Armis Advantage for Integration

- **Agentless Deployment -** No software installation is required on devices, ensuring quick deployment and uninterrupted operations.
- **Protocol Expertise -** Armis supports proprietary ICS protocols, enabling full understanding of device communications in industrial environments.
- **Comprehensive Context -** Armis correlates data across IT, OT, IoT and medical devices, delivering a holistic view of the environment and potential risks.
- **Actionable Intelligence -** Security teams receive prioritized, actionable insights for effective risk management and incident response.

Armis Centrix™ bridges the gap between IT and ICS environments, offering a unified, scalable solution that secures every connected device, ensuring resilience and operational continuity critical infrastructure and industrial environments.

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