HOW ARMIS SUPPORTS THE MITRE ATT&CK™ FOR ICS MATRIX

MITRE ATT&CK™ for ICS provides a useful framework for security managers to assess and improve their security controls for industrial control systems (ICS) and operational technology (OT) environments. Traditional IT security controls that utilize agents will not work for these environments, and network-based scans and probes can often adversely impact such devices, even potentially taking the devices and corresponding business capabilities offline.

This white paper proposes an alternative approach — one based on passive traffic monitoring, a massive device knowledgebase, and an advanced threat detection engine — that can alert against a broad range of the tactics and techniques listed in the new ATT&CK for ICS framework.

TABLE OF CONTENTS

INTRODUCTION

Industrial Control Systems (ICS) are increasingly vulnerable to cyberattacks. In recent years, we have seen various types of malware with names like WannaCry, NotPetya, LockerGoga, and Triton shut down operations at major firms such as Maersk, Renault-Nissan, Norsk Hydro, and others. Each firm suffered major financial loss.

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.[1]

To help solve this problem, The MITRE Corporation has developed a new version of their highly popular MITRE ATT&CK™ framework. This new version is focused on Industrial Control Systems. Unlike previous ATT&CK frameworks that were oriented towards traditional and mobile computing environments, the new ATT&CK for ICS is designed to help enterprise security practitioners understand adversary behavior and plan appropriate security systems that are tailored to the unique challenges of operational technology (OT) and ICS environments.

This white paper reviews the reasons why ICS environments are increasingly exposed to cyberattacks and proposes a new type of security system that can alert against a broad range of the tactics and techniques listed in ATT&CK for ICS. This new approach relies on passive traffic monitoring, a massively scalable device knowledgebase, and an advanced threat detection engine.

66%

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

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."[2]

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 the environments listed above 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.

Unpatchable

ICS devices range from complex large-scale robots to small sensors built on a single circuit board. Many of these devices were never designed to be updated, or if the capability exists, it requires a very manual process to accomplish. This means that any vulnerabilities disclosed post-manufacture will either persist through the lifecycle of the device or will be very difficult to patch manually.

Unagentable

Most ICS devices do not give administrators the ability to gain root access to the underlying operating system, thus eliminating the possibility of installing an agent on the device. Often, the ICS device includes a tailored operating system which is unable to host agents designed for the mass market of manageable computers. The result is that traditional endpoint protection agents that are commonly used within the IT environment won't work with ICS devices.

ICS SECURITY CHALLENGES

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

Disruptable

A standard method for device discovery and vulnerability assessment on an IT network is to perform a network scan using something like NMAP. However, it is commonly known that network scans and probes can disrupt the functionality of an ICS device. ICS devices have historically not been designed to be able to tolerate the same kinds of scans and probes that are commonly used on IT networks. Therefore, in the vast majority of ICS environments, scanning of ICS devices is prohibited simply because of the risk of disrupting critical business operations.

Accessible

Most ICS devices in use today were designed under the assumption that they would either be installed as a standalone device or placed on an isolated network. Therefore, they were designed to be highly accessible, and they contained few (or no) built-in protections. Once they are placed onto a network, they are unable to withstand a cyberattack.

Proprietary Protocols

Some ICS devices operate using proprietary protocols, either due to the specific nature of the device itself or to reduce the computational burden associated with other protocols. The result of using these protocols is that development, quality assurance, peer review and security processes have not matured in the manner that widely-used protocols have. This leads to inherent vulnerabilities that cannot be resolved without extensive development changes or replacing the protocol itself.

It's also worth noting that the security research community has traditionally focused on widely used, common protocols when hunting for and reporting vulnerabilities to software providers and hardware manufacturers. In turn, though many ICS devices are vulnerable to a variety of cyberattacks, these exposures have not been recorded within standard vulnerability databases such as CVD.

Proliferation

The rapid proliferation of the Internet of Things (IoT) has made an impact beyond the consumer marketplace and has exponentially increased the number of ICS devices available. This has changed the competitive marketplace for these devices, increasing the importance of time to market and cost savings. For all manufactures, these priorities reduce the time and resources available to develop, implement, and test their products.

The combination of the factors listed above explain the unique security challenges that are associated with ICS devices. It can be overwhelming to understand how attacks against ICS devices occur, who is targeting these devices, and what mitigations can be effective in defending this arena. It is for this reason that MITRE has developed the ATT&CK for ICS framework.

THE MITRE ATT&CK FRAMEWORK

MITRE ATT&CK is a well-known framework which outlines the tactics, techniques, and procedures (TTP) that are typically employed by adversaries. Effectively, each MITRE ATT&CK framework helps a business to:

- **Identify** the most active and/or effective threat actors targeting your industry
- **Understand** the techniques used by the threat actors
- **Prioritize** each technique based on probability and potential impact to your business
- **Assess** current defenses, understand gaps, and plan improved defenses

Security vendors should be able to articulate which ATT&CK techniques their products address. In this way, ATT&CK gives enterprise security architects an "apples to apples" comparison across different security products. ATT&CK simplifies this discussion by standardizing the tactics and techniques and giving solid examples of what specific threat actors' procedures are in those areas.

MITRE ATT&CK FOR ICS

MITRE has previously published two ATT&CK frameworks — one for enterprise environments and another for mobile devices. The vast majority of techniques included in those frameworks are unique to Windows, macOS, iOS, and Android devices. They provide little help to security managers who are interested in understanding techniques that are used to attack ICS environments.

In January 2020, MITRE released the first version of ATT&CK for ICS. This new framework is unique to the operating systems, TTPs, and adversaries of concern for users of ICS devices.

The new ATT&CK for ICS lists the following tactics:

- Initial Access
- Execution
- Persistence
- Evasion
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Inhibit Response Function
- Inhibit Process Control
- Impact

While many of these tactics and the underlying 81 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 following enterprise tactics are not included in ATT&CK for ICS:

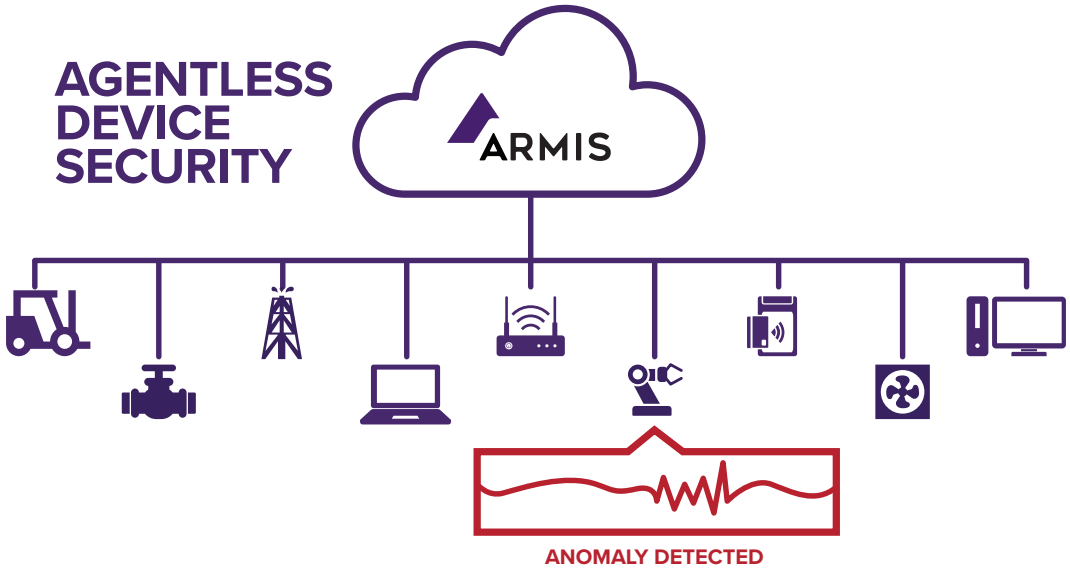
- Credential Access
- Exfiltration

This does not imply that an adversary will not use these techniques when targeting ICS, but rather that these techniques will be used within the victim's enterprise network, which in turn may bridge into the victim's ICS environment.

ARMIS PROVIDES COMPREHENSIVE COVERAGE FOR ATT&CK FOR ICS

The **Armis agentless device security platform** provides comprehensive coverage of the cyber attack techniques listed in the MITRE ATT&CK for ICS matrix. The Armis platform discovers every device on your network as well as devices that are transmitting in your airspace. Once each device has been discovered, The Armis platform analyzes device behavior to identify risks and detect cyber attack techniques. the platform is cloud-based, agentless, and integrates easily with your existing network and security products.

The Armis platform 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 and to understand its behavior without disruption. The **Armis Risk Analysis Engine** analyzes this data and uses device profiles and characteristics stored in the **Armis Device Knowledgebase** to assess each device's risk, detect threats, and block threats automatically.



The Role of Programmable Logic Controllers (PLCs)

As addressed above, there are many different devices under the category of Industrial Control Systems. PLCs are commonly used as an abstraction layer for dumber devices, and as such represent the primary attack surface for those devices. For many of the ICS techniques, The Armis platform's ability to detect the techniques against PLCs enables it to provide protection for a broad range of ICS devices.

The table below lists all of the ATT&CK for ICS techniques organized by tactic. The darker purple represents techniques that the Armis platform can detect at inception, and the lighter purple represents the techniques that it can detect subsequently, or where it 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	Evasion	Discovery	Lateral Movement	Collection	Command & Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State *	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware *	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State *	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download **	Masquerading *	Network Connection Enumeration	External Remote Services *	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading *	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection *	Rogue Master Device *	Network Service Scanning	Program Organization Units *	Detect Program State		Block Reporting Message	Modify Control Logic *	Loss of Availability
External Remote Services *	Man in the Middle	System Firmware *	Rootkit *	Network Sniffing	Remote File Copy	I/O Image		Block Serial Comm	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units *	Valid Accounts *	Spoof Reporting Message *	Remote System Discovery	Valid Accounts *	Location Identification		Data Destruction	Module Firmware *	Loss of Productivity and Revenue
Replication Through Removable Media	Project File *		Utilize/Change Operating Mode *	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download **	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart / Shutdown	Rogue Master Device *	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message *	Manipulation of View
						Screen Capture		Modify Control Logic *	Unauthorized Command Message	Theft of Operational Information
								Program Download **		
								Rootkit *		
								System Firmware *		
								Utilize / Change Operating Mode *		

Techniques that the Armis platform can **detect at inception**

Techniques that the Armis platform can **detect subsequently,** or where it 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.

NAME	THE ARMIS PLATFORM'S CAPABILITIES
T810: Data Historian Compromise	The Armis platform is able to detect and alert on abnormal traffic or communication behavior which may indicate that an adversary is attempting to compromise, or has already compromised, the Data Historian.
T817: Drive-by Compromise	The Armis platform's policy engine can be configured to alert and take action whenever Armis observes a device accessing unauthorized or known malicious websites. The Armis platform's threat feeds automatically populate the list of known malicious sites, and a predefined policy can alert if a device reaches out to a site on the list.
T818: Engineering Workstation Compromise	The Armis platform is able to alert on abnormal traffic or communication behavior which may indicate that an engineering workstation, SCADA or HMI has been compromised.
T819: Exploit Public-Facing Application	The Armis platform is able to detect software vulnerabilities on Internet-facing applications; this helps security managers take proactive steps to update the software or otherwise mitigate the risk of exploitation. Also, it continuously monitors the behavior of systems hosting public-facing applications to detect if they have been compromised.
T822: External Remote Services*	The Armis platform passively monitors device communications and associates active ports, services, and protocols. The Armis platform's policy engine can be configured to alert when Armis observes a device utilizing unauthorized services.
T883: Internet Accessible Device	The Armis platform's passive monitoring can identify specific devices that are communicating with the internet and therefore are internet accessible, and can alert on those devices that should not be exhibiting this type of communication.
T847: Replication Through Removable Media	The Armis platform monitors network traffic, so once a malicious application is active on the network, even those transferred through removable media, Armis will be able to detect malicious activity.

ATT&CK TACTIC: **INITIAL ACCESS**

The adversary is trying to get into your ICS environment.

T865: Spearphishing Attachment	If a system has been compromised through a spearfishing attachment, the Armis platform will detect and alert on abnormal behavior caused by the malware/attacker.
T862: Supply Chain Compromise	The Armis platform passively and continuously monitors the behavior of every device on our customers' networks. The platform compares every device's real-time activity to the established and "known-good" activity baseline for the specific device which is stored in the Armis Device Knowledge Base. When abnormal behavior in your network is detected, Armis updates the risk score and generates a security alert. In the event of a supply chain compromise, the Armis platform will alert when the compromised product behaves abnormal compared to other legitimate products.
T860: Wireless Compromise	The Armis platform passively 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, the Armis platform 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.

NAME	THE ARMIS PLATFORM'S CAPABILITIES
T875: Change Program State*	The Armis platform is able to detect and alert on a wide range of PLC-specific network traffic, including the commands related to changing the program state on a device.
T807: Command-Line Interface	The Armis platform is able to monitor remote access services such as SSH, Telnet, and RDP which are likely to be used by attackers who are attempting to access ICS environments via the command-line interface. When such remote access activity is abnormal (e.g. at an unusual time of the day, or the first such remote access ever observed), Armis can alert on the remote access service activity.
T871: Execution through API	The Armis platform can detect API calls and, through its threat detection engine, alert if the API activity, or the source of the API calls, is abnormal.
T823: Graphical User Interface	The Armis platform's passive monitoring of device communications patterns allows it to detect abnormal traffic which may indicate an adversary is remotely accessing a GUI to conduct malicious behavior.
T830: Man in the Middle	The Armis platform's passive monitoring of device communications, including network traffic characteristics like TCP options and latency, allows it to detect anomalies which may indicate a Man-in-the-Middle attack.
T844: Program Organization Units*	The Armis platform is able to detect and alert on a wide range of PLC specific network traffic, including the commands related to changing the program on a device.
T873: Project File Infection*	The Armis platform is able to detect when a PLC has been reprogrammed and alert on that activity.
T853: Scripting	If a malicious script is used to attack or alter a device, causing the device to behave abnormally, The Armis platform will detect and alert on the abnormal behavior.
T863: User Execution	If a system is compromised through user execution, then the Armis platform will detect when the system acts abnormally.

ATT&CK TACTIC: **PERSISTENCE**

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

NAME	THE ARMIS PLATFORM'S CAPABILITIES
T874: Hooking	The Armis platform's passive network monitoring and device profiling enables it to detect when a system has been compromised and is redirecting API calls across the network. If the system acts abnormally or redirects the API calls across the network, then Armis will generate an alert.
T839: Module Firmware*	The Armis platform detects when firmware is downloaded to PLCs. Then, if the new firmware causes the behavior of a PLC to change abnormally, Armis will detect and issue an alert.
T843: Program Download**	The Armis platform detects when programs are downloaded to PLCs. Then, if the new program causes the behavior of a PLC to change abnormally, Armis will detect the abnormality and issue an alert.
T873: Project File Infection*	The Armis platform is able to detect when a PLC has been reprogrammed and alert on that activity.
T857: System Firmware*	The Armis platform passively monitors device communications across the network, and is able to profile every device to determine the current version of system firmware that is operating. This gives our customer the ability to monitor the firmware version across devices, understand the known threats to the firmware, and intelligently manage their firmware upgrade strategy. In addition, it has the ability to detect when a PLC firmware has been changed and to alert on that activity.
T859: Valid Accounts*	The Armis platform's passive monitoring and device profiling can detect when abnormal network connections are being made, which is indicative of an adversary using valid accounts to conduct lateral movement outside of the normal behavior for the legitimate account holder.

ATT&CK TACTIC: **EVASION**

The adversary is trying to avoid being detected.

NAME	THE ARMIS PLATFORM'S CAPABILITIES
T820: Exploitation for Evasion	The Armis platform identifies all known software vulnerabilities. This facilitates proactive attempts to remediate vulnerable devices, remove them from the network, or provide other forms of risk mitigations. Once a device has been exploited for evasion, it can detect and alert on behavioral changes.
T872: Indicator Removal on Host	The Armis platform's passive network monitoring is able to detect an adversary's remote commands related to removing indications of their presence on a specific host.
T849: Masquerading*	Since the Armis platform monitors the behavior of devices, not the files on the devices, it is not fooled by attackers' masquerading techniques. The platform passively and continuously monitors the behavior of every device to detect and alert on abnormal behavior.
T848: Rogue Master Device*	The Armis platform passively monitors device communications and can alert whenever a device communicates with a rogue master device.
T851: Rootkit*	The Armis platform's passive network monitoring enables its to detect abnormal behavior which is indicative of a rootkit. If the adversary is targeting a PLC for the rootkit, the platform will detect when the configuration and firmware have been altered.
T856: Spoof Reporting Message*	The Armis platform's passive network monitoring allows it to detect abnormal message traffic which may be indicative of message spoofing.
T858: Utilize/ Change Operating Mode*	The Armis platform is able to detect and alert on PLC Mode Changes.

ATT&CK TACTIC: **DISCOVERY**

The adversary is trying to figure out your ICS environment.

NAME	THE ARMIS PLATFORM'S CAPABILITIES
T808: Control Device Identification	The Armis platform can detect abnormal network traffic which may indicate an adversarial attempt at conducting control device identification.
T824: I/O Module Discovery	The Armis platform's passive network monitoring enables it to detect when an adversary attempts to conduct input/output discovery over the network.
T840: Network Connection Enumeration	The Armis platform passively monitors device communications and can be configured to alert on the presence of unauthorized network scans, netstat use, or other abnormal network traffic indicative of network connection enumeration.
T841: Network Service Scanning	The Armis platform detects and alerts on port scanning.
T842: Network Sniffing	The Armis platform's passive network monitoring detects when an adversary attempts to exfiltrate information sniffed from a network.
T846: Remote System Discovery	The Armis platform's passive network monitoring and device profiling allows it to detect unauthorized or abnormal network traffic associated with remote system discovery.
T854: Serial Connection Enumeration	The Armis platform's passive network monitoring and device profiling allows it to detect unauthorized or abnormal network traffic associated with querying a device for its serial connections information.

ATT&CK TACTIC: **LATERAL MOVEMENT**

The adversary is trying to get into your ICS environment.

NAME	THE ARMIS PLATFORM'S CAPABILITIES
T812: Default Credentials	The Armis platform's passive monitoring of the network traffic, combined with device profiling, allows it to detect and alert on credentials transitioning across the network. It can also detect when one device connects to another, and is able to create alerts which may indicate that default credentials are being used.
T866: Exploitation of Remote Services	The Armis platform's passive network monitoring allows it to detect when a device uses remote services in an abnormal manner, e.g. for lateral movement.
T822: External Remote Services*	The Armis platform's passive network monitoring allows it to characterize the behavior of all network participants, even if they are entering the network through an external remote service. The network traffic from external remote services are monitored, and alerts can be created to alert on abnormal or suspicious behavior.
T844: Program Organization Units*	The Armis platform is able to detect when a PLC has been reprogrammed, and policies can be created to alert on this behavior.
T867: Remote File Copy	The Armis platform's passive monitoring and device profiling can detect when a system is remotely copying files.
T859: Valid Accounts	The Armis platform's passive monitoring and device profiling can detect when abnormal network connections are being made, which is indicative of an adversary using valid accounts to conduct lateral movement outside of the normal behavior for the legitimate account holder.

ATT&CK TACTIC: **COLLECTION**

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

NAME	THE ARMIS PLATFORM'S CAPABILITIES
T802: Automated Collection	The Armis platform's passive network monitoring is able to detect and alert on new or abnormal network activity to include the use of tools and scripts which are used for automated collection.
T811: Data from Information Repositories	The Armis platform's passive network monitoring is able to detect and alert on unauthorized or abnormal connection attempts to connect to information repositories.
T868: Detect Operating Mode	The Armis platform is able to detect and alert on a wide range of PLC specific network traffic, including the commands related to monitoring the PLC status which would be used by an adversary to determine the current state of the PLC.
T870: Detect Program State	The Armis platform is able to detect and alert on a wide range of PLC specific network traffic, including the commands related to monitoring the PLC status which would be used by an adversary to determine the current state of the PLC.
T877: I/O Image	The Armis platform's passive network monitoring and device profiling can detect and alert on unauthorized connections to ICS devices which could be used to extract I/O images.
T825: Location Identification	The Armis platform's passive network monitoring and device profiling can detect and alert on unauthorized connections to ICS devices which could be used to identify the device's location.
T801: Monitor Process State	The Armis platform's passive network monitoring and device profiling can detect and alert on unauthorized connections to ICS devices which could be used to detect the devices' process state.
T861: Point & Tag Identification	The Armis platform's passive network monitoring and device profiling can detect and alert on the network traffic associated with querying devices for their point and tag information.

ATT&CK TACTIC: **COLLECTION**

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

T845: Program Upload	The Armis platform passively monitors device communications and can alert whenever it observes unauthorized file transfer such as a program upload.
T850: Role Identification	The Armis platform passively monitors device communications and can be configured to alert whenever it observes connections made to the network which an adversary may use to conduct reconnaissance to conduct role identification.
T852: Screen Capture	The Armis platform's passive network monitoring allows it to detect when a device is attempting to exfiltrate a screen capture to the adversary, and to cause an alert when detected.

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.

NAME	THE ARMIS PLATFORM'S CAPABILITIES
T885: Commonly Used Port	The Armis platform's threat detection engine can detect when a commonly used port is being used to communicate in an abnormal manner.
T884: Connection Proxy	The Armis platform passively monitors device communications and associates active ports, services, and protocols. The platform's policy engine can be configured to alert or remediate (e.g. quarantine) whenever it observes the use of an unauthorized connection proxy. If the traffic outbound of the proxy is monitored by the Armis platform, then it can alert on traffic that is connecting to known malicious sites.
T869: Standard Application Layer Protocol	The Armis platform's passive network monitoring and device profiling allows it to establish “known good” traffic patterns over commonly used application protocols. If an adversary attempts to establish command and control over these commonly used protocols, it will detect and alert on this abnormal behavior.

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.

NAME	THE ARMIS PLATFORM'S CAPABILITIES
T800: Activate Firmware Update Mode	The Armis platform is able to detect a wide range of PLC specific commands including the commands related to updating or modifying the firmware.
T878: Alarm Suppression	The Armis platform's deep understanding of ICS protocols allows it to detect when a PLC has been altered or is behaving outside of normal parameters. If so, this may indicate that an adversary is attempting to suppress that device's alarms.
T803: Block Command Message	The Armis platform's passive network monitoring, device profiling, and deep understanding of ICS protocols allow it to detect when a PLC has been altered or if the device is behaving outside of normal parameters which would be required prior to an adversary being able to block command messages.
T804: Block Reporting Message	The Armis platform's passive network monitoring, device profiling, and deep understanding of ICS protocols allow it to detect when a PLC has been altered or if the device is behaving outside of normal parameters which would be required prior to an adversary being able to block reporting messages.
T805: Block Serial COM	The Armis platform's passive network monitoring, device profiling, and deep understanding of ICS protocols allow it to detect when a PLC has been altered or if the device is behaving outside of normal parameters which would be required prior to an adversary being able to block a serial communications port.
T809: Data Destruction	The Armis platform's passive network monitoring and device profiling allow it to detect and alert on abnormal network traffic associated with data destruction commands.
T814: Denial of Service	The Armis platform is able to detect intentional or unintentional denial of service events and can be configured to alert when certain network thresholds are met.

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.

T816: Device Restart/Shutdown	The Armis platform's passive monitoring is able to detect and alert on a wide variety of PLC messages including those used to shut down and restart a device.
T835: Manipulate I/O Image	The Armis platform's deep understanding of ICS protocols allows it to detect when a PLC has been altered, e.g. by an adversary is attempting to manipulate the device's I/O image.
T838: Modify Alarm Settings	The Armis platform can detect abnormal PLC modification which may be used by an adversary to modify the alarm settings.
T833: Modify Control Logic*	The Armis platform can detect abnormal PLC modification which may be used by an adversary to modify the control logic.
T843: Program Download**	The Armis platform's passive network monitoring allows it to detect abnormal PLC modification which may be used by an adversary to modify the existing program in the PLC.
T851: Rootkit*	The Armis platform's passive network monitoring allows it to detect abnormal PLC modification such as the installation of a rootkit. And for any network device, the Armis platform is able to detect abnormal behavior which may be indicative of a system which has an active rootkit installed. If an adversary manages to install a rootkit on a non-PLC host, the platform can detect and alert on abnormal behavior associated with the rootkit behavior.
T857: System Firmware*	The Armis platform's passive monitoring is able to detect and alert on a wide variety of PLC messages including those used to update the firmware on a device.
T858: Utilize/ Change Operating Mode*	The Armis platform's passive monitoring is able to detect and alert on a wide variety of PLC messages including those used to change the operating mode of a device.

ATT&CK TACTIC: **IMPAIR PROCESS CONTROL**

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

NAME	THE ARMIS PLATFORM'S CAPABILITIES
T806: Brute Force I/O	The Armis platform's passive network monitoring allows it to detect abnormal I/O related network traffic indicative of brute force I/O.
T875: Change Program State	The Armis platform's passive monitoring is able to detect and alert on a wide variety of PLC activities and commands including configure commands which are used to change the program loaded on the device.
T849: Masquerading*	Since the Armis platform monitors the behavior of devices, not the files on the devices, it is not fooled by attackers' masquerading techniques. The platform passively and continuously monitors the behavior of every device to detect and alert on abnormal behavior or unauthorized devices.
T833: Modify Control Logic*	The Armis platform's passive monitoring is able to detect and alert on a wide variety of PLC activities and commands including configure commands which are used to change the program loaded on the device.
T836: Modify Parameter	The Armis platform's passive monitoring is able to detect and alert on a wide variety of PLC activities and commands including configure commands which are used to change the configuration of the device.
T839: Module Firmware*	The Armis platform's passive monitoring is able to detect and alert on a wide variety of PLC activities and commands including configure commands which are used to change the firmware of the device.
T843: Program Download**	The Armis platform's passive monitoring is able to detect and alert on a wide variety of PLC activities and commands including configure commands which are used to change the programming of the device.
T848: Rogue Master Device*	The Armis platform's can be configured such that all control messages not generated from a legitimate master device triggers the alert.
T881: Service Stop	The Armis platform's passive monitoring is able to detect and alert on a wide variety of PLC activities and commands including Stop commands which are used to stop the service of the device.
T856: Spoof Reporting Message*	The Armis platform's passive network monitoring allows it to detect abnormal message traffic which may be indicative of message spoofing.
T855: Unauthorized Command Message	Armis can create an alert if command messages are transmitted by unauthorized controllers.

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, the Armis platform will not be able to detect the impact (e.g. property damage), but the Armis platform can help a customer avoid, provide telemetry, or recover from these impacts as described below.

NAME	THE ARMIS PLATFORM'S CAPABILITIES
T879: Damage to Property	The Armis platform detects device vulnerabilities in the ICS environment which allows security managers to take proactive steps to mitigate risks in order to prevent a successful attack and prevent damage to property. If devices begin to act abnormally, alerts will be generated ideally in time to prevent any damage to property.
T813: Denial of Control	The Armis platform's passive network monitoring and device profiling enables it to detect and alert on the PLC messages required to prevent ICS devices from attempting to communicate with its controllers. Armis can be configured with policies which generate alerts if the devices do not connect to the controller as scheduled.
T815: Denial of View	The Armis platform's passive network monitoring detects and tracks all device communications and can provide insight into when devices have last appeared on the network.
T826: Loss of Availability	The Armis platform's passive network monitoring, device profiling, asset discovery, and vulnerability analysis allow it to help the customer secure their network and ICS devices, as well as detect adversarial efforts to cause a loss of availability.
T827: Loss of Control	The Armis platform's passive network monitoring, device profiling, asset discovery, and vulnerability analysis allow it to help the customer secure their network and ICS devices, as well as detect adversarial efforts to cause a loss of control.
T828: Loss of Productivity and Revenue	The Armis platform's passive network monitoring, device profiling, asset discovery, and vulnerability analysis allow it to help the customer secure their network and ICS devices, as well as detect adversarial efforts to cause a loss of productivity and revenue.

ATT&CK TACTIC: **IMPACT**

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

T880: Loss of Safety	The Armis platform's passive network monitoring, device profiling, asset discovery, and vulnerability analysis allow it to help the customer secure their network and ICS devices, as well as detect adversarial efforts to cause a loss of safety.
T829: Loss of View	The Armis platform can support a loss of view situation by providing customers detailed information on each device, when last seen on the network, and their last risk profile. This will assist customers to prioritize restoration of the connections to the ICS devices.
T831: Manipulation of Control	The Armis platform's passive monitoring is able to detect and alert on a wide variety of PLC messages including those used to change the configuration and settings of the device.
T832: Manipulation of View	The Armis platform's passive monitoring is able to detect and alert on a wide variety of PLC messages including those used to change the configuration and settings of the device.
T882: Theft of Operational Information	The Armis platform's passive monitoring can be implemented with policies that generate alerts when unauthorized devices attempt to make connections to include the collection and exfiltration of operational data.

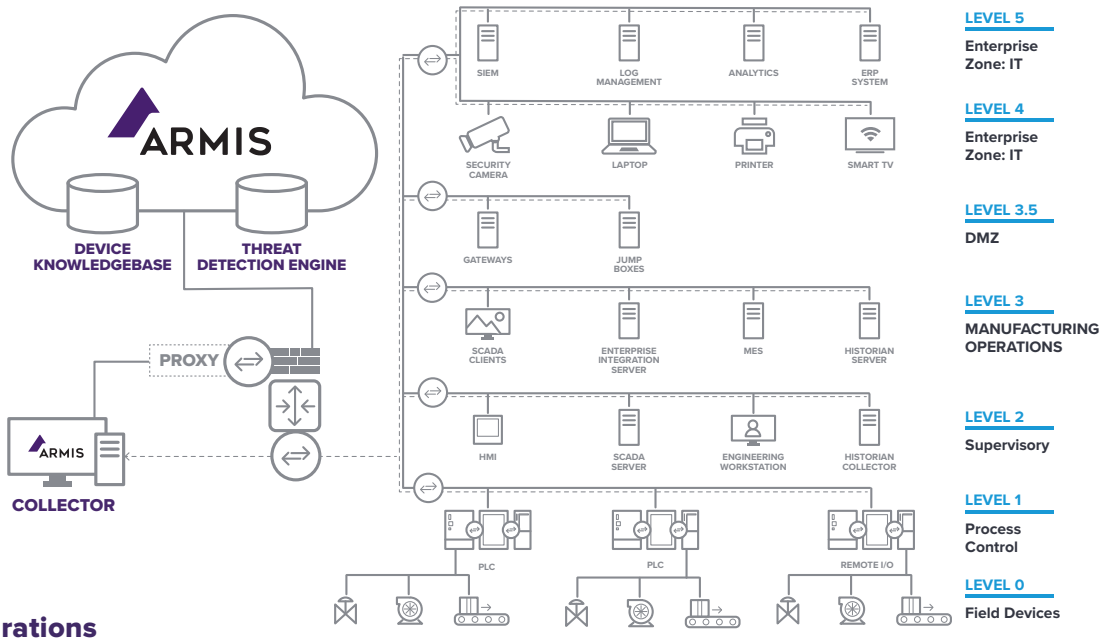
* Technique seen in two tactics
** Technique seen in three tactics

DEPLOYING THE ARMIS PLATFORM TO PROTECT ICS

Since the Armis platform does not utilize agents or require new hardware, it deploys very quickly. An Armis virtual appliance passively monitors network traffic, turns the traffic into metadata, and sends that metadata to the Armis cloud for analysis. The metadata includes:

- Device profile attributes, for example: details like IP, MAC addresses, user names, type / category, model, OS, running apps, etc.
- Device communication details, for example: the wireless MAC layer (WiFi / BlueTooth), protocols used (HTTP, HTTPS, VOIP, etc.), the amount of data transmitted, time of transmission, encryption level, etc.
- Headers of the communication, but not the actual data payloads (the requests and the headers of responses, DHCP packets, etc.).
- Metadata representing connection and session setup exchanges, such as handshakes, synchronization, channel / encryption negotiation.

The Armis virtual appliance is called the **"collector,"** as shown below. The collector is able to provide information about every device in the enterprise, across every level of the Purdue model. The volume of metadata that the collector sends to the Armis cloud for processing is very small, typically a 10,000:1 reduction compared to the network traffic that is being monitored.



Integrations

The Armis platform is able to integrate with your existing security tools and management systems. This lets you leverage your existing investments and automate responses to the threats identified by Armis. The following is a brief list of the types of systems that the platform integrates with.

ARMIS INTEGRATIONS

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)	SIEMs are only as good as the data they receive. They often have a visibility gap with respect to ICS devices (not to mention many kinds of enterprise IoT devices such as VoIP phones, printers, etc.). The Armis platform solves this problem. It can provide your SIEM full visibility to all devices in your environment — both on your network and in your airspace. This allows your SIEM to produce more complete reports, and it helps you shorten your response time in crisis mode.
FIREWALL	When the Armis platform detects abnormal and/or malicious device behavior, it can communicate with your firewall which can then break the command and control. The firewall can also prevent data from being exfiltrated from the compromised device.
NETWORK ACCESS CONTROL	When the Armis platform detects that a device in your environment is behaving suspiciously or maliciously, the platform can trigger your NAC to take appropriate action, such as moving that device to a more restricted network segment. Armis can also provide a detailed inventory of all your devices including their location on the network; this allows you to audit the integrity of the network segmentation that your NAC system has established.
SWITCHES AND ROUTERS	The Armis platform is able to integrate with switches and routers through SNMP and SSH, allowing Armis to alter the configuration of the switches and routers based on the Armis collected data for automated network segmentation or enforcement (e.g. isolating or quarantining a device due to suspicious or malicious behavior).
VULNERABILITY SCANNERS	In many OT environments, the use of vulnerability scanners is prohibited because they can cause OT devices to crash. Since the Armis platform utilizes 100% passive technologies, Armis is able to fill in the gaps by providing vulnerability information for the OT environment. Also, in areas of the network where scanners can be used, the platform is able to trigger the vulnerability scanner upon certain conditions. For example, if a new device joins the enterprise network, or if a device on the enterprise network is detected by the platform as having a potential critical vulnerability, it can immediately trigger the vulnerability scanner to scan that device and incorporate the results.
TICKETING AND INCIDENT RESPONSE	When the Armis platform detects a policy violation or threat on your network, it generates tickets and sends alerts or actions automatically (e.g. to investigate or quarantine a suspicious device) to your existing workflow or incident response systems. This allows your existing investments in security operations center process and automation tools and procedures to be extended to your un-agentable devices.
ITAM AND CMDB	The Armis platform can provide a customer's ITAM and CMDB information about all of the devices in your environment, including unmanaged devices and IoT devices on your network and in your airspace. This helps you maintain a trusted single-source-of-truth repository for better decision-making.

CONCLUSION

The MITRE ATT&CK for ICS framework outlines the tactics and techniques used in real-world Industrial Control System attacks. Leveraging this knowledge will assist ICS cybersecurity professionals in understanding where their ICS exposures lie and allow them to remediate these gaps using appropriate measures.

The Armis platform is an agentless device security platform uniquely suited to detect a broad range of the ATT&CK for ICS techniques. This is driven by the convergence of:

- Comprehensive **visibility** into every IT and OT asset the network
- Thorough **understanding** of the ICS devices and their protocols
- The ability to **profile** devices, assess risk, detect threats and vulnerabilities and abormal device behavior.

The Armis platform provides comprehensive coverage of the cyber attack techniques listed in the MITRE ATT&CK for ICS matrix. It can also detect attack techniques focused on enterprise IoT devices such as printers, video cameras, Smart TVs, VoIP phones etc. These devices are just as vulnerable as ICS devices, they are present in vast numbers in all enterprise environments, and, just like ICS devices, they can't be monitored by agents.

ENDNOTES

[1] "State of Enterprise IoT Security: A Spotlight on Manufacturing," Sept. 2019, Forrester Consulting
https://www.armis.com/resources/analyst-reports/forrester-state-of-enterprise-iot-security-a-spotlight-on-manufacturing/

[3] https://csrc.nist.gov/glossary/term/industrial-control-system

ABOUT ARMIS

Armis the leading unified asset visibility & security platform designed to address the new threat landscape that connected devices create. Fortune 1000 companies trust our real-time and continuous protection to see with full context all managed, unmanaged, and IoT devices, including medical devices (IoMT), operational technology (OT) and industrial control systems (ICS). Armis provides passive and unparalleled cybersecurity asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in Palo Alto, California.

1.888.452.4011 armis.com