SOLUTION BRIEF

MITRE ATT&CK FOR ICS

A Definitive Guide to MITRE ATT&CK® for ICS and Armis' Performance in the 2021 ATT&CK Evaluations

In this guide, you will find a brief overview of the MITRE ATT&CK framework, followed by a deep dive into the results of the 2021 MITRE Engenuity ATT&CK Evaluations for ICS.

These quantitative results are intended to help you better understand a given product's capabilities in relation to MITRE's publicly accessible ATT&CK for ICS framework. Numbers alone without context can be difficult to decipher. This guide will peel back the layers and provide concise nuggets of information to make it easier to review.

A LITTLE BACKGROUND

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 an industry.

PRIORITIZE each technique based on probability and potential impact to a business

UNDERSTAND the techniques used by the threat actors.

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 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 software, TTPs, and adversaries of concern for users of ICS devices.

ATT&CK for ICS contains the following tactics:

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
13 techniques	9 techniques	5 techniques	2 techniques	6 techniques	5 techniques	6 techniques	10 techniques	3 techniques	13 techniques	5 techniques	12 techniques

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 specifically to ICS environments. Each technique may be associated with one or more tactics if they have the capability to support different adversarial objectives.

The 2021 MITRE Engenuity ATT&CK Evaluations for ICS

This is the MITRE Engenuity team's first evaluation of the ICS threat detection market. One of the challenges we face in ICS cybersecurity, is the lack of detection and collection capability within most ICS environments. MITRE Engenuity ATT&CK Evaluations are intended to help vendors and end-users better understand a product's capabilities in relation to MITRE's publicly accessible ATT&CK for ICS framework, which is a curated knowledge base of adversary tactics, techniques, and procedures based on known threats to industrial control systems. ATT&CK for ICS provides a common language to describe the tactics and techniques that cyber adversaries use when attacking the systems that operate some of the nation's most critical infrastructures, including energy transmission and distribution plants, oil refineries, wastewater treatment facilities, and more. As a true community-led effort, more than 100 participants from 39 organizations reviewed, provided comments, or contributed to the ATT&CK for ICS framework when it launched in early 2020.

For the ATT&CK Evals, MITRE Engenuity used the MITRE ATT&CK for ICS knowledge base to emulate the tactics, techniques, and procedures (TTPs) associated with the TRISIS/TRITON malware. The malware was the first-ever tailored to attack safety systems including those found within oil and gas and electrical facilities in the Middle East, Europe, and North America. You can view these TTPs on an interactive matrix on our own MITRE ATT&CK for ICS webpage.

Understanding Armis' Performance in the ATT&CK Evaluations for ICS

MITRE Engenuity does not assign scores, rankings or ratings. Nor do they proclaim a "winner". They simply publish numbers on how each vendor performed for each of the 17 ATT&CK Techniques across 10 ATT&CK Tactics. You can view the in-scope techniques of the TRITON evaluation below.

Initial Access 13 techniques	Execution 9 techniques	Persistence 5 techniques	Privilege Escalation 2 techniques	Evasion 6 techniques	Discovery 5 techniques	Lateral Movement 6 techniques	Collection 10 techniques	Command and Control 3 techniques	Inhibit Response Function 13 techniques	Impair Process Control 5 techniques	Impact 12 techniques
Data Historian Compromise	Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	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	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Engineering Workstation	Execution through API	Project File Infection		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
Exploit Public-Facing Application	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Exploitation of Remote Services	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
External Remote Services	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Internet Accessible Device	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Remote Services	Scripting						Program Upload		Device Restart/ Shutdown		Loss of Safety
Replication Through Removable Media	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Rogue Master							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Spearphishing Attachment									Rootkit		Manipulation of View
Supply Chain Compromise									Service Stop		Theft of Operational Information
Wieless Compromise									System Firmware		

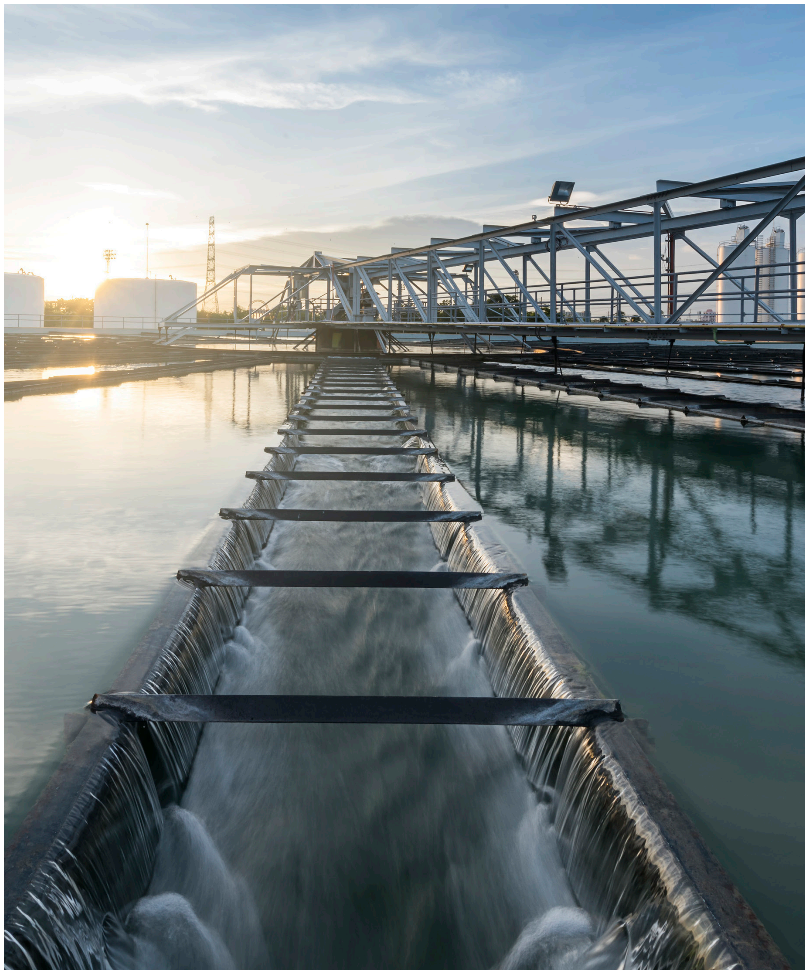
You can find the ATT&CK Evaluations results for Armis in the table below

Evaluations	Detection Count	Analytic Coverage	Telemetry Coverage	Visibility
TRITON (2021)	**140 across 100*** substeps	**50 of 100*** substeps	**90 of 100*** substeps	**90 of 100*** substeps

**Detection for 2 substeps required actively querying the programmable logic controllers. Armis did not leverage this type of capability, so those substeps were removed.*

Asset Visibility Across OT/ICS & IT Environments

Numbers without context can be difficult to decipher. Thankfully, our data team has peeled back the layers and provided some concise nuggets of information that are easy to consume. First, let's talk about visibility. The foundation of a comprehensive ICS security solution is the ability to see every device across the entire infrastructure and beyond, while missing nothing in the process. With the increased frequency and sophistication of today's attacks, depth and breadth of visibility are fundamental capabilities that an ICS security solution must deliver. Most breaches such as the recent Colonial Pipeline cyber-attack, begin on the IT environment and then move laterally to the OT environment. Thus, visibility into both the IT and OT/ICS sides of the house is paramount. Zero gaps means zero blind spots, mitigating an attacker's ability to operate undetected. The table above shows that Armis detected 90 out of 100 substeps in the Visibility category; not 90% of devices in the environment. In fact, Armis had zero misses and provided 100% visibility of all OT/ICS & IT devices.

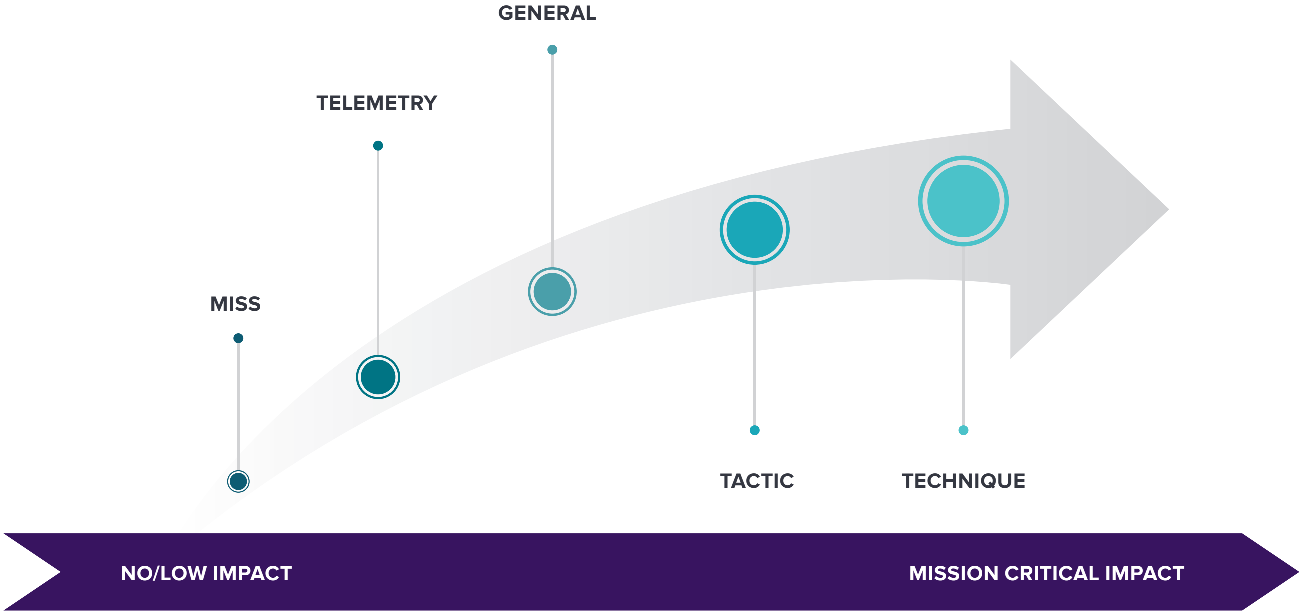


In most situations, such as the one faced in colonial pipeline cyber-attack, visibility into both the IT and the OT/ICS sides of the house is paramount.

Comprehensive Coverage Across All ATT&CK for ICS Tactics and Techniques

Analytics Detection Coverages as opposed to Detection Counts should always be a factor when evaluating an ICS security solution. Having a higher number of general, tactic or technique detections leads to higher quality detections as this ensures that fewer attacks are missed. High-fidelity and high-quality detections give ICS security teams more time to investigate events, rather than sifting through a sea of data that could contain a high amount of false positives.

In the ATT&CK Evaluations, “Tactics” and “Techniques” are the key measures of data precision



- **Tactic –** The next level down the hierarchy, representing categories of techniques that tell us the actor’s steps in achieving their ultimate goals (persistence, data egress, evasions, etc.) In short, the “what” and the “why”.

- **Technique –** The epitome of relevant and actionable data – fully contextualized data points that tell a story, indicating what happened, why it happened, and crucially, how it happened.

These two detection classifications are the core of the MITRE ATT&CK for ICS framework and are of the highest value when creating context. **Armis achieved 100% coverage of all MITRE Engenuity ATT&CK Evaluations for ICS tactics and a 90% detection rate of all steps performed by adversaries during the evaluation.**

Using passive monitoring technology and device profiling, Armis can detect and alert on devices entering into the network (initial access) and communicating across the network (lateral movement).

100% Real-time Detection

Time is a critical factor when detecting an attack. A delayed detection, according to MITRE, is not immediately available to the analyst; it may come minutes or hours after the adversary has performed malicious activity.

A delayed detection during the evaluation often means that the ICS security solution required a human analyst to manually confirm suspicious activity, due to the inability of the solution to do so on its own. The solution typically needs to send data to the analyst team or other third-party services for analysis. However, many critical parts of this process are performed manually, which creates a window of opportunity for the adversary to do real damage. In addition to real-time detection, Armis also provides the ability to explore and investigate the context of a threat directly from the console, including the ability to redirect the alert to a 3rd party SIEM.

Adversaries operating at a high rate of speed need to be countered with a lightning-strike reaction and not one that requires human intervention. As the ATT&CK Evaluations results show, Armis had zero delayed detections.

100% Detection of All Initial Access and Lateral Movement

As mentioned above, protecting both IT and OT/ICS environments is paramount to any ICS security solution. Using passive monitoring technology and device profiling, Armis can detect and alert on devices entering into the network (initial access) and communicating across the network (lateral movement). Armis also detects when a device uses remote services in an abnormal manner and alerts on suspicious or potentially malicious behavior. In the ATT&CK Evaluations, Armis detected 100% of these activities.

Real-time Detection of Critical Changes in PLC Behavior

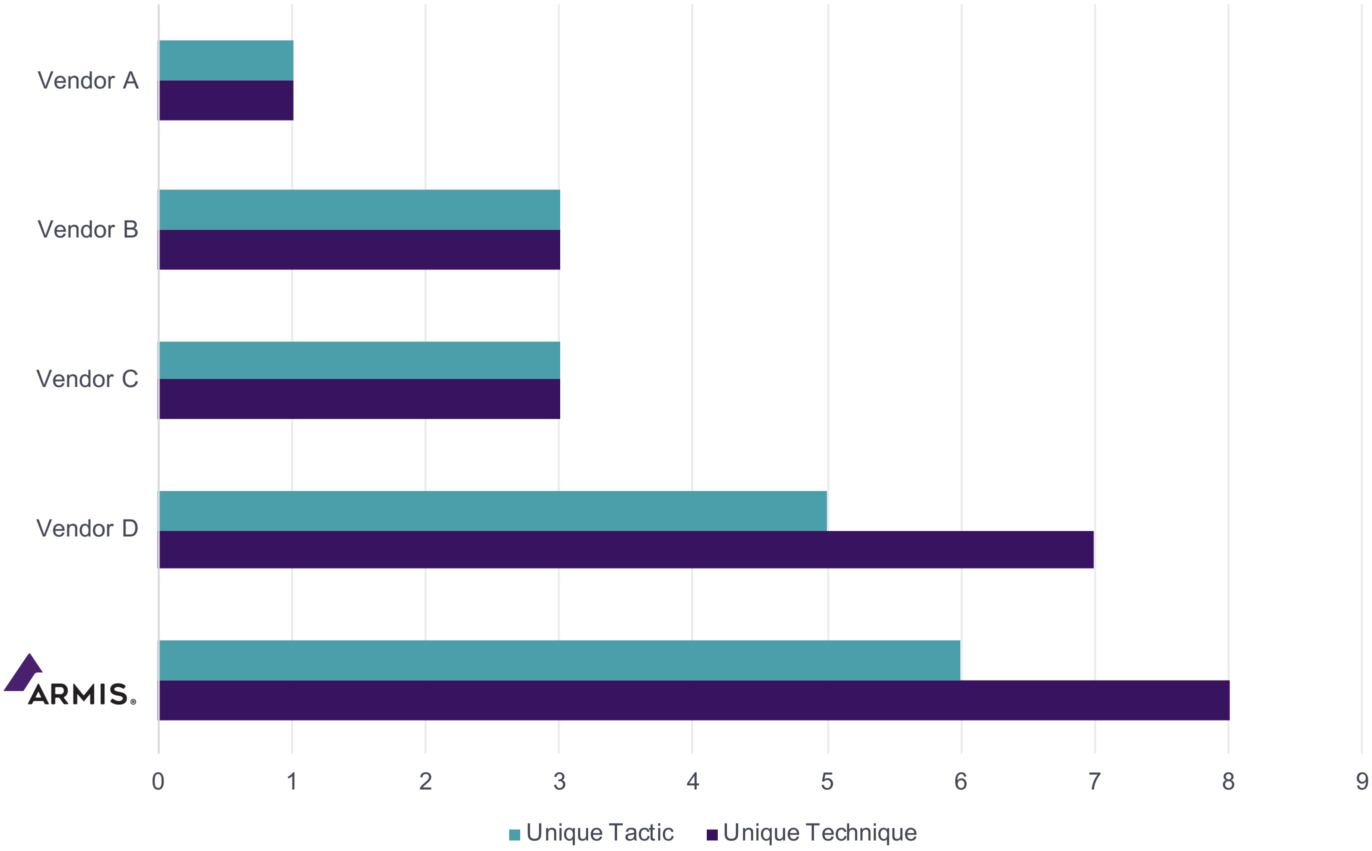
In addition to real-time detection of devices and events, real-time and continuous threat detection for programmable logic controllers (PLCs) is of utmost importance. Adversaries can change/update the operational mode of a PLC to gain access to supervisory functions which can have a detrimental impact to OT operations.

Armis can identify the state and detect in real-time PLC changes such as Program, Mode, State, Firmware, and many others. Real-time detection of these critical changes will ensure that only known-good behavior is exhibited by every PLC and only approved changes are implemented, keeping the OT environment safe and secure.

Armis Has the Broadest Coverage for Unique Tactics and Techniques

In the ATT&CK Evaluations, Armis had the broadest coverage for both unique tactics and techniques of any other vendor. Full context of every event gives Armis users more granular information about what happened and why in order to rectify a security incident with precise, immediate action as opposed to chasing false positives while an adversary plans or executes their next steps.

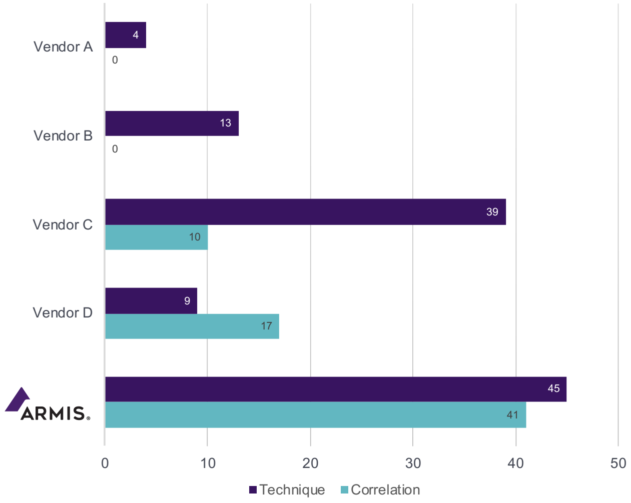
Unique Detection Types and Techniques



Providing Value and Context in Lieu of Alert Fatigue

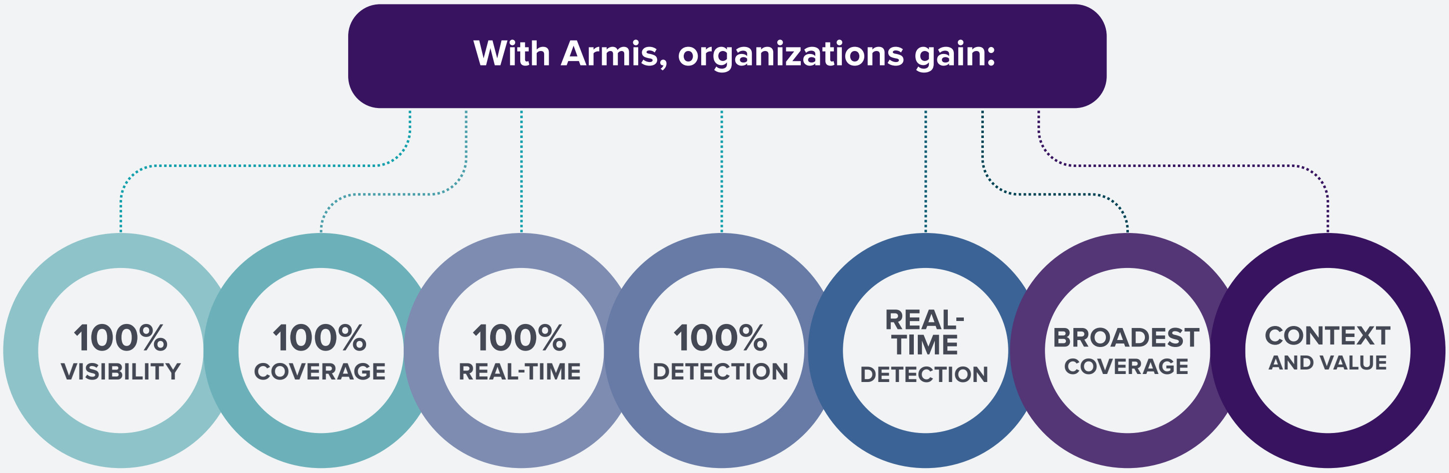
In addition to technique detection, Armis provides correlation and context on specific detections. What the graph below illustrates is that most Armis detections (yellow) include aggregated activities (blue). So instead of alerting on each suspicious activity, Armis understands that it is all part of the same detection and consolidates them into a single alert. This reduces alert fatigue and provides security teams context about specific events, as opposed to just flagging multiple alerts and having to manually correlate them to an activity.

Correlation and Context



What the Results Mean to You:

The Armis platform's exceptional performance in the 2021 MITRE Enginuity ATT&CK Evaluations for ICS proves that purpose-built, forward-thinking solutions such as Armis deliver the broadest, most in-depth visibility across IT, OT/ICS, and automation, that modern OT/ICS environments require to combat adversaries. As evidenced by the results of the evaluation, the Armis platform excels at visibility and detection, and even more importantly, that the autonomous mapping of data into fully indexed and correlated stories that allow users to completely and immediately understand the "what, why and how" when an adversary makes a move. And when combined with Armis' world class threat research team who have discovered & disclosed critical vulnerabilities impacting millions of OT, IoT, and IoMT devices including most recently, ModiPwn which affects Schneider Electric Modicon PLCs, security teams have the tools they need to keep their systems operational.



With Armis, organizations gain:

100% VISIBILITY

100% COVERAGE

100% REAL-TIME

100% DETECTION

REAL-TIME DETECTION

BROADEST COVERAGE

CONTEXT AND VALUE

100% visibility of all assets (OT/ICS & IT)

100% coverage of all MITRE ATT&CK for ICS tactics

100% real-time detection tactics

100% detection of all initial access and lateral movement

Real-time detection of PLC critical changes

Broadest coverage of unique tactics and technique

Context and value over alert fatigue

To learn more about the Armis platform's coverage for the MITRE ATT&CK for ICS framework, click here.
For the full results and more information about MITRE Engenuity's ATT&CK Evaluations, visit attackevals.mitre-engenuity.org.

About Armis

Armis is the leading unified asset visibility and 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.

armis.com

1.888.452.4011

ARMIS.