DRAGOS

Executive Summary

A GUIDE TO UNDERSTANDING THE 2021 MITRE ENGENUITY ATT&CK® EVALUATIONS FOR ICS

Discover more about MITRE Engenuity's first evaluation of the Industrial Control Systems (ICS) threat detection market and how the Dragos Platform and other participants' solutions performed in a realistic demonstration attack against an Operational Technology (OT) environment.

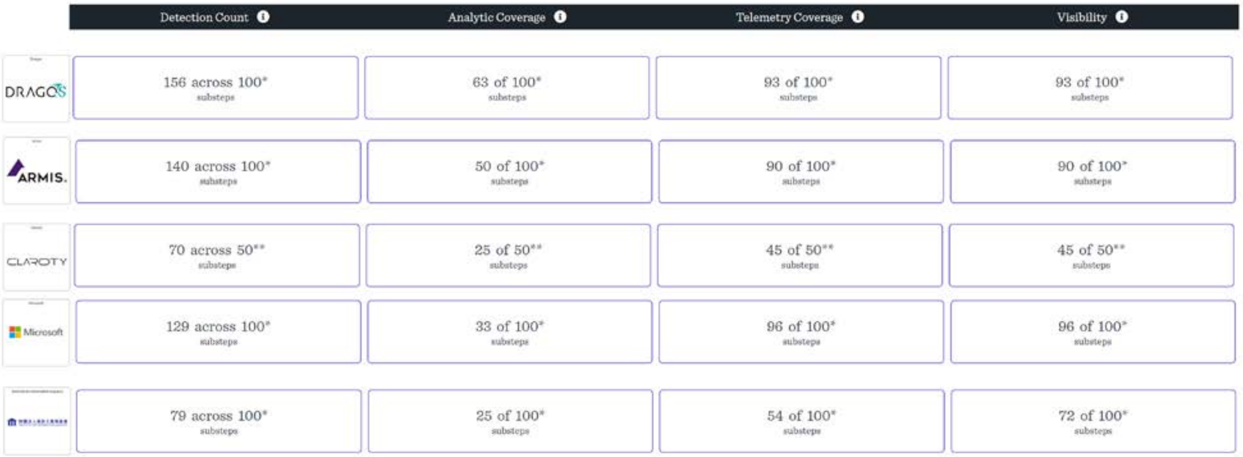
OVERVIEW

The 2021 MITRE Engenuity ATT&CK® Evaluations for Industrial Control Systems (ICS) is **MITRE Engenuity's** first evaluation of the ICS threat detection market and the most realistic demonstration attack to date against an Operational Technology (OT) environment. Key to this simulation was that it leveraged a real-world threat group, XENOTIME, which was responsible for the 2017 safety instrumented system (SIS)-focused attack in Saudi Arabia, and a full ICS range with emulated safety and environmental impacts. The attack culminated with a manipulated **Burner Management System (BMS)** that resulted in the destruction of the fictional facility.

As a result of the ATT&CK Evals, the community now has a **complete dataset for an end-to-end attack on an ICS system.**

This is a significant development because one of the challenges we face in ICS cybersecurity is the lack of detection and collection capability within most ICS environments. We often struggle to piece together the complete attack chain in actual ICS incidents because the environments are not capable of collecting the required evidence. The real value of these evaluations is to the community members and customers who see vendors step up to be tested and get independent insights into how they performed. The scenario provided by MITRE can then be studied by the vendors who participated to greatly enhance the threat detection capabilities of their products.

View the full list of participants and the ATT&CK Evaluations results at:
attackevals.mitre-engenuity.org/ics/participants/



	Detection Count	Analytic Coverage	Telemetry Coverage	Visibility
DRAGOS	156 across 100* substeps	63 of 100* substeps	93 of 100* substeps	93 of 100* substeps
ARMIS.	140 across 100* substeps	50 of 100* substeps	90 of 100* substeps	90 of 100* substeps
CLAROTY	70 across 50** substeps	25 of 50** substeps	45 of 50** substeps	45 of 50** substeps
Microsoft	129 across 100* substeps	33 of 100* substeps	96 of 100* substeps	96 of 100* substeps
[illegible]	79 across 100* substeps	25 of 100* substeps	54 of 100* substeps	72 of 100* substeps

THE MITRE ATT&CK FOR ICS FRAMEWORK

HOW IT STARTED

MITRE ATT&CK for ICS is the world's first encyclopedia of publicly observed ICS-focused adversary tactics, techniques, and procedures (TTPs). Security professionals such as network defenders, incident responders, threat hunters, and pen testers can quantify their industrial cybersecurity coverage or capabilities using this single resource.

The ATT&CK for ICS framework is a powerful taxonomy to better understand and prioritize multistage attacks. Before ATT&CK for ICS, you had to collect all the public and non-public reports from numerous sources and create a dataset to understand the industrial adversary landscape. MITRE has worked behind the scenes to develop and carefully organize that dataset for the benefit of industrial network defenders everywhere.

The ATT&CK for ICS framework is also widely thought of as a new industry standard for securing ICS environments against malicious behaviors. Each technique is linked to a description, examples, and references of publicly known attacks on ICS environments. The framework is a cornerstone resource that has been missing for the past two decades of ICS cybersecurity.

MITRE ATT&CK for ICS WAS CREATED BY THE ICS CYBERSECURITY COMMUNITY

100+ participants

39+ organizations

<5 years

ATT&CK for ICS continues to evolve. Anyone can contribute data today by emailing: attack@mitre.org

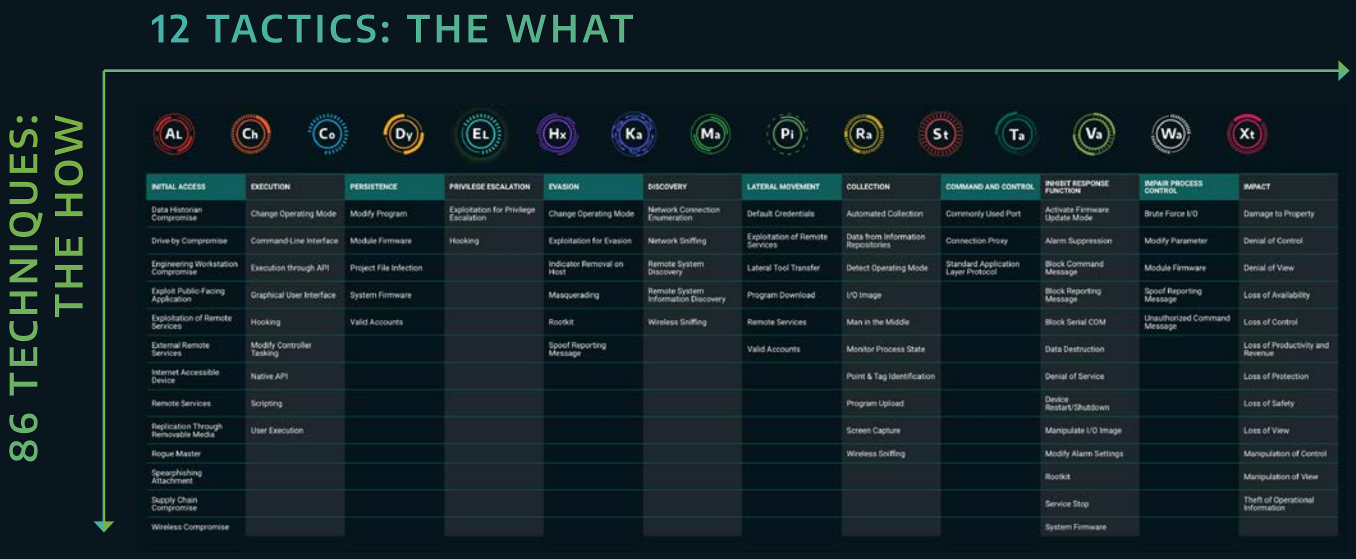
THE MITRE ATT&CK FOR ICS FRAMEWORK

HOW IT WORKS

MITRE ATT&CK for ICS defines 12 behavioral tactics: Initial Access, Execution, Persistence, Privilege Escalation, Evasion, Command and Control, Collection, Lateral Movement, Discovery, Inhibit Response Function, Impair Process Control, and Impact.

These behavioral tactics, or categories, are further refined into behavioral techniques (there are 86 of them) and together outline how ICS networks worldwide are being threatened daily and provide a common view on which all ICS threats can be mapped.

With ATT&CK for ICS there is now a common community lexicon and framework from which to discuss ICS threat detection effectiveness.

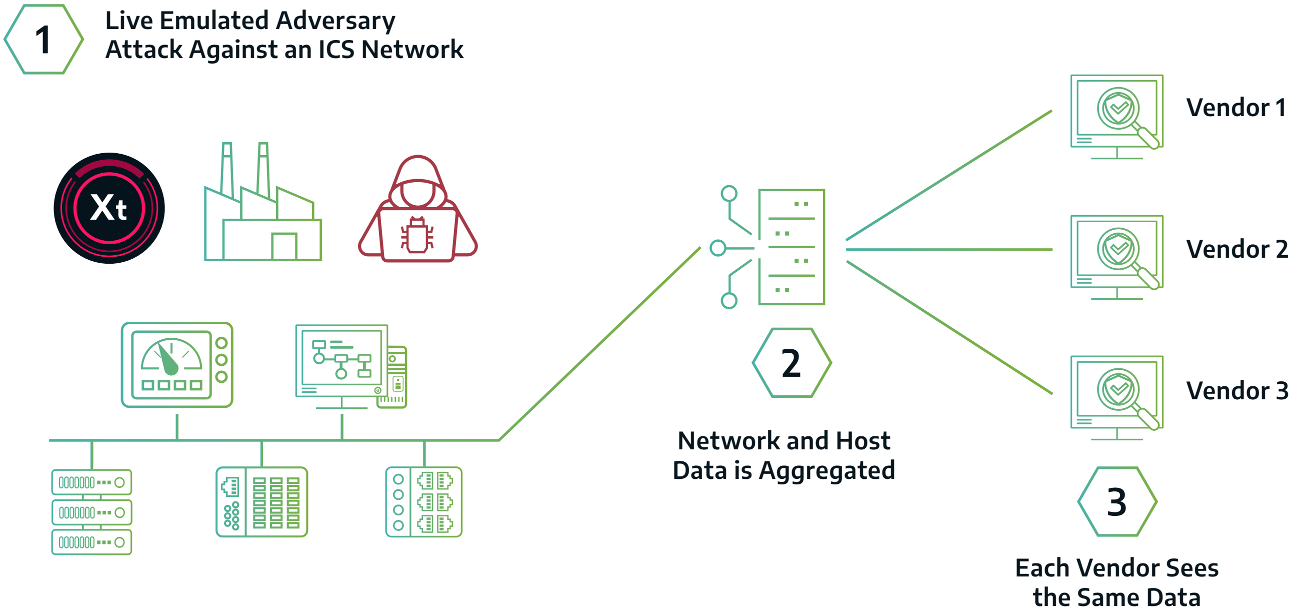

12 TACTICS: THE WHAT
86 TECHNIQUES: THE HOW
AL
Ch
Co
Dy
EL
Hx
Ka
Ma
Pi
Ra
St
Ta
Va
Wa
Xt

INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	EVASION	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND AND CONTROL	INHIBIT RESPONSE FUNCTION	IMPAIR PROCESS CONTROL	IMPACT
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 Compromise	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
Wireless Compromise									System Firmware		

ATT&CK EVALUATIONS FOR ICS SCENARIO

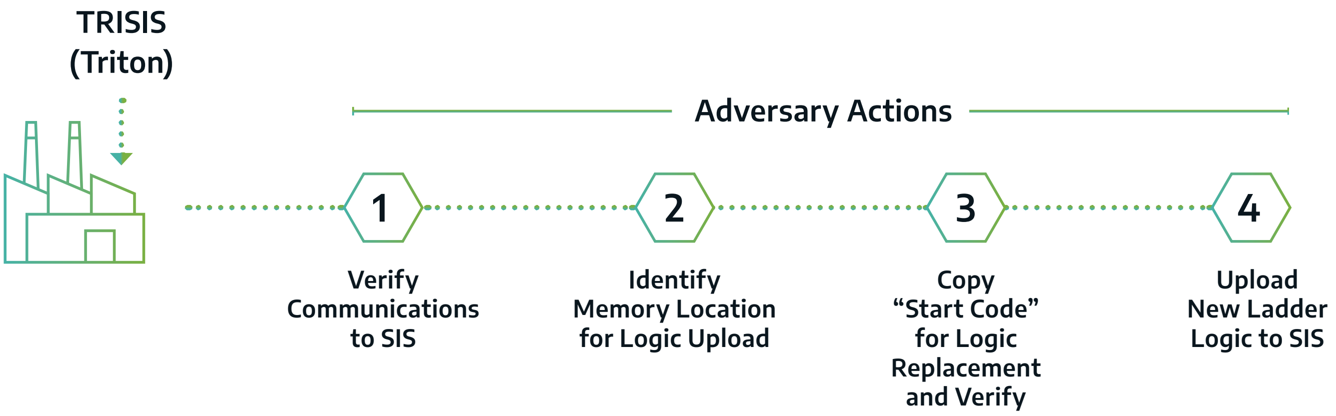
THE METHODOLOGY

The following graphic illustrates the emulated attack approach used in the ATT&CK Evaluations, highlighting how each participating vendor had access to the same data.


1
Live Emulated Adversary Attack Against an ICS Network
Xt
2
Network and Host Data is Aggregated
Vendor 1
Vendor 2
Vendor 3
3
Each Vendor Sees the Same Data

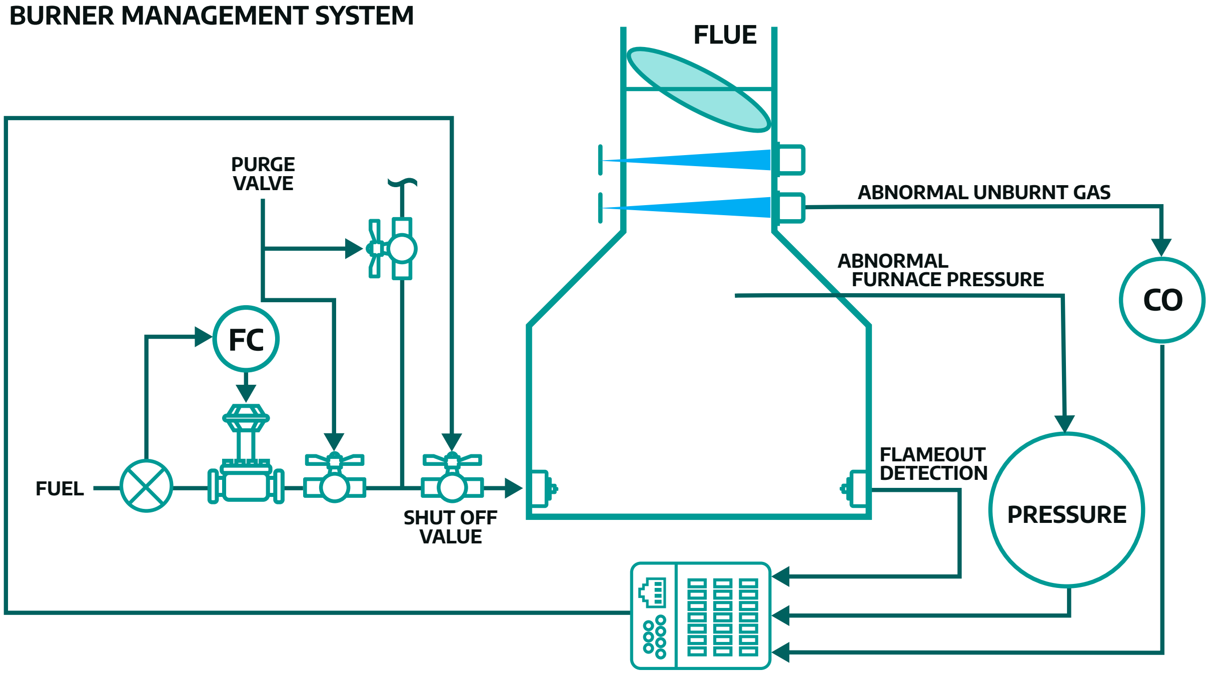
ABOUT THE ADVERSARY

The **XENOTIME activity group** is attributed to the **TRISIS (AKA TRITON)** malware and the attack of the safety instrumented systems at an oil refinery in Saudi Arabia in 2017. Industrial safety instrumented systems comprise part of a multi-layer engineered process control framework to protect life and the environment.


TRISIS (Triton)
Adversary Actions
1
Verify Communications to SIS
2
Identify Memory Location for Logic Upload
3
Copy "Start Code" for Logic Replacement and Verify
4
Upload New Ladder Logic to SIS

THE ENVIRONMENT

The evaluation scenario was focused on a Burner Management System (BMS). We see BMSs in a wide range of industry verticals such as Oil & Gas, Food & Beverage, Building Management, and in the Electric sector. BMSs support processes such as boilers, ovens, heaters, and steam generators. Steam generators are an important part of combined-cycle natural gas power generation. Within a BMS, there should always be a safety system component as they are regulated by multiple industry safety standards.



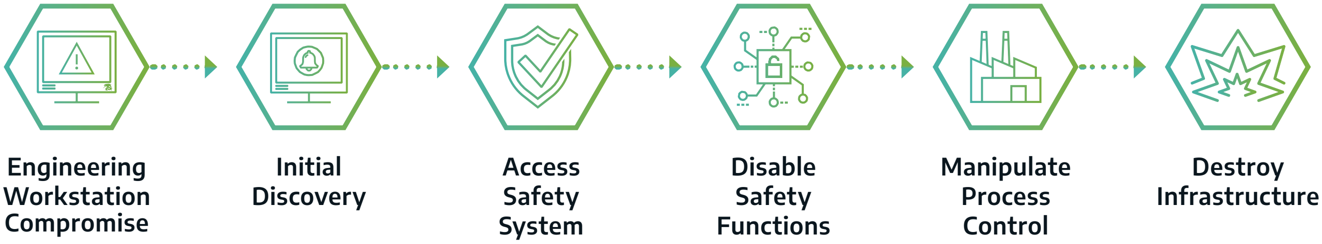
The environment was uncomplicated and divided into two halves: Control and Safety.

- The Control half was a Rockwell ControlLogix 1756-L71/B LOGIX5571 controller (v20.54) serving as the Control Programmable Logic Controller (Control PLC) and an associated Control Engineering Workstation (Control EWS) and Control Human Machine Interface (Control HMI).
- The Safety half was a mirror image of the Control half with another ControlLogix 1756-L71/B LOGIX5571 (v20.54) controller serving as the Safety PLC and an associated Safety EWS and Safety HMI.

Both controllers had remote IO to support the simulation of a live plant during the ATT&CK Evaluations.

THE EMULATED ATTACK FLOW

The following graphic represents the operational flow and intended objective of the emulated attack. See the **MITRE Engenuity** website to learn more.



UNDERSTANDING THE EVALUATION RESULTS

MITRE Engenuity released the results of its ATT&CK Evaluations for ICS results in July 2021. You can view the official results of the ATT&CK Evaluations on the **MITRE Triton ICS Evaluation 2021 web page.**

MITRE Engenuity does not declare a "winner" and does not assign overall scores, rankings, or ratings to the vendors or their cybersecurity technology. Instead, they are very transparent and present the evaluation results based on four separate, but related, categories of visibility and detection so other organizations may provide their own analysis and interpretation.

THE EVALUATION CATEGORIES

Each of the MITRE ATT&CK matrices is comprised of **Tactics** and **Techniques.**

- **Tactics** represent the "why" of an ATT&CK technique or sub-technique. It is the adversary's tactical goal: the reason for performing an action. For example, an adversary may want to achieve credential access.
- **Techniques** represent "how" an adversary achieves a tactical goal by performing an action. For example, an adversary may dump credentials to achieve credential access.

The ATT&CK Evaluations adversary actions were broken into 25 main **steps** and 100 **sub-steps.**

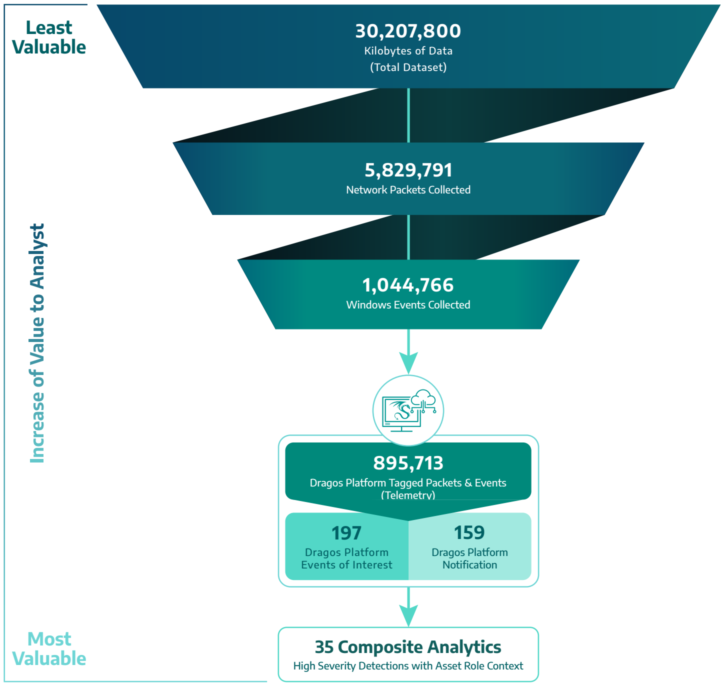
- **Steps** in the MITRE Evaluation represent an adversary's objective. Steps could be loosely associated with Tactics.
- **Sub-steps** represent the specific actions taken to complete an objective. Sub-steps could be loosely associated with Techniques.

The ATT&CK Evaluations results provide a rich dataset in four different categories: **Detection count, Analytic coverage, Telemetry coverage, and Visibility.**

DETECTION COUNT	ANALYTIC COVERAGE	TELEMETRY COVERAGE	VISIBILITY
The total number of detections related to the evaluation. Measures depth of detections/multiple methods of measuring the same type of threat behavior. Depth adds resiliency to threat behavior-based detections. An adversary can change one or more aspects of their technique but a detection will still fire.	The proportion of sub-steps that contained a detection that provides additional context (e.g., General, Tactic, Technique). Number of adversary sub-steps which triggered a detection. Measures the ability of the product to convert telemetry into actionable threat detections. Measures breadth of detections, number of threat behaviors that are covered by a detection.	The proportion of sub-steps that produced a detection with minimal processing. Telemetry is the fundamental data which detections process their logic against to determine if they should activate. As an ICS network defender, it is often valuable to be able to look at the telemetry that triggered a particular detection or telemetry prior to or after an event.	The proportion of sub-steps with either an analytic or a telemetry detection. Visibility is the combination of Analytic Coverage and Telemetry Coverage. It represents the vendor's ability to see each sub-step taken by the adversary at some level. To better understand the portion of the visibility that is actionable by a network defender, we must look at ratio Analytic Coverage to Telemetry Coverage.

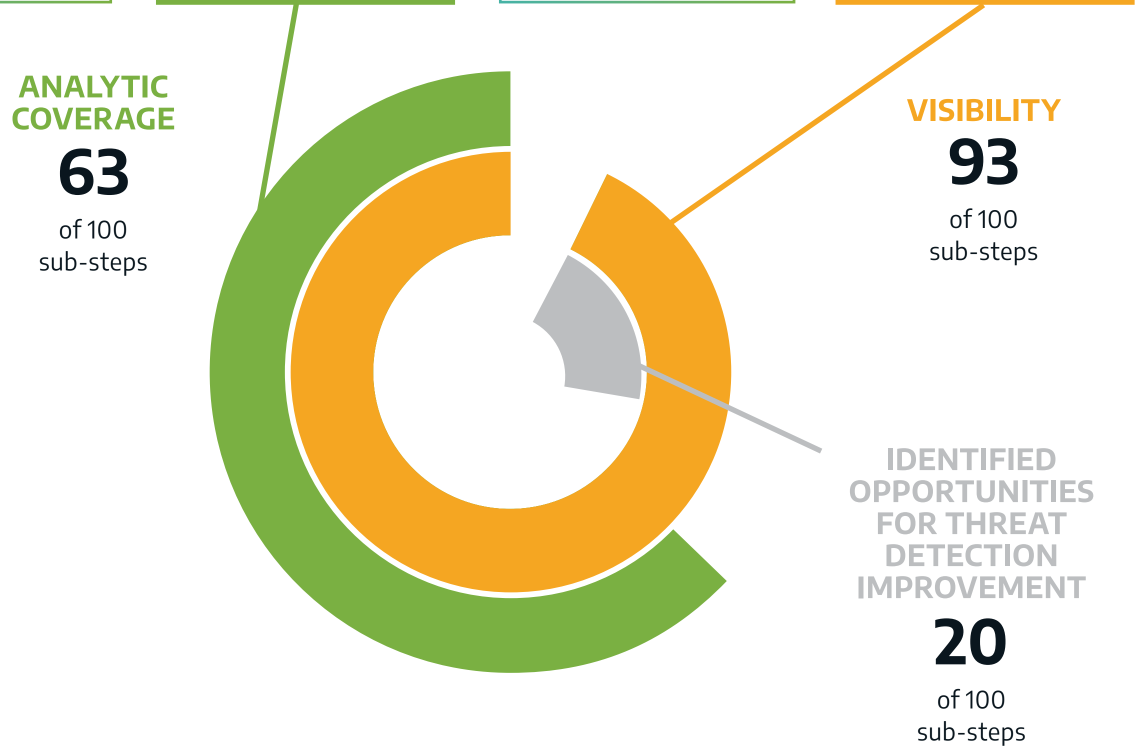
HOW DRAGOS PERFORMED

We were consistently impressed with the MITRE Engenuity™ team's ability to accurately re-interpret the XENOTIME threat behaviors into a Rockwell Automation-focused attack simulation that was both eerily similar yet new. We were also excited, and a little proud, to see how well the Dragos Platform tracked the adversary through each step of the ICS Cyber Kill Chain.



The Dragos Platform generated 35 composite analytics from the evaluations' total dataset. Those 35 context-enriched analytics covered and helped us identify 63 of the 100 adversary sub-steps taken in the emulated attack.

DETECTION COUNT	ANALYTIC COVERAGE	TELEMETRY COVERAGE	VISIBILITY
156 across 100 sub-steps	63 of 100 sub-steps	93 of 100 sub-steps	93 of 100 sub-steps



THE LESSONS LEARNED & THE VALUE TO THE ICS COMMUNITY

VETTED TECHNOLOGIES TO TACKLE REAL-WORLD OT THREATS

The ATT&CK Evaluations for ICS validate the leading cybersecurity vendors and their ability to detect industrial adversary TTPs targeting OT environments. IT and OT systems converged years ago using similar technologies, but cybersecurity has been primarily focused on IT systems, creating an IT-OT cybersecurity gap. The reasons for this lag have been multi-faceted, as many stakeholders operated under common misapprehensions:

- that OT systems remained air gapped or that air gaps are still sufficient,
- that physical risk management measures were enough to keep industrial systems secure,
- that cybersecurity measures always incur disproportionate operational risks, and
- that existing tools cannot yet address the unique nature of OT cybersecurity.

In the face of these persistent OT cybersecurity myths, digital transformation marches on, further increasing the connectedness of OT systems with the broader enterprise and internet. Having a program like the MITRE Engenuity ATT&CK Evaluations for ICS ensures ongoing support and understanding of real-world cyber threats to increasingly connected OT environments.

The ATT&CK Evaluations enable businesses to accelerate digital transformation securely and manage their growing risks to protect core business operations.

CONTINUOUS IMPROVEMENT IN THREAT DETECTION

The ATT&CK Evaluations for ICS has provided numerous learning opportunities and has helped us to identify areas where we can improve the Dragos Platform. As a direct result of what we learned from these evaluations, we are actively working to improve our technology.

- **During a few of the adversary sub-steps, the Dragos Platform did not identify the specific tags being forced by the Control EWS / Safety EWS on the Control PLC / Safety PLC using CIP (Common Industrial Protocol).**

  Although the Dragos Platform was able to identify the status codes being used by the CIP protocol, the ability to see the specific values being forced provides context around attacks that leverage the control system to create an impact. Dragos is actively working to enhance our existing CIP protocol dissection to better cover CIP I/O values and forced values over CIP.

- **The Dragos Platform did not directly identify the use of PowerShell OpenSSH as a Command and Control (C2) channel. However, the Dragos Platform was able to extract the command that created the OpenSSH C2 channel from the host event logs.**

  To fully address this, Dragos will create a new detection to specifically call out SSH (and other interactive protocols) on a non-standard port as potential C2.

- **The Dragos Platform has Notifications for a wide range of port scanning and ICMP sweeping techniques. However, during the MITRE Evaluation, the network was too small to trigger the threshold (number of assets scanned) to fire our ICMP Sweep Notification.**

  To address the ICMP sweep high-threshold issue, Dragos is introducing the ability for users to tune detections more granularly. The new tuning will allow customization of various thresholds, such as the sensitivity of ICMP Sweep detections, on a per-network basis, allowing for different types of environments to have different thresholds.

A COMMUNITY APPROACH ENABLES BETTER SECURITY OUTCOMES

The ICS community should understand that a lot of the OT adversary behavior today is focused on quiet prepositioning and reconnaissance work that wouldn't be evident without the right visibility in place. Industrial adversaries often build programs and campaigns slowly over time, with later campaigns being more successful and disruptive due to previous efforts.

Many threats represented in the MITRE ATT&CK for ICS framework may not induce headline-causing disruption, but they often lay the groundwork for evolving into future attacks with potential to be disruptive and destructive. The ATT&CK Evaluations allow vendors and end-users to know what cybersecurity tools are available to effectively stop cyber threats in their tracks and prohibit them from causing further harm.

As a true community-led effort, the ATT&CK for ICS framework will continue to evolve based on ongoing input from the ICS/OT cyber community and enable every industrial organization to proactively stay ahead of their know adversaries, today and into the future.

ABOUT DRAGOS, INC.

Dragos has a global mission: to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. The practitioners who founded Dragos were drawn to this mission through decades of government and private sector experience.

Dragos codifies the knowledge of our cybersecurity experts into an integrated software platform that provides customers critical visibility into ICS and OT networks so that threats are identified and can be addressed before they become significant events. Our solutions protect organizations across a range of industries, including power and water utilities, energy, and manufacturing, and are optimized for emerging applications like the Industrial Internet of Things (IIoT).

Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

TO LEARN MORE ABOUT DRAGOS AND OUR TECHNOLOGY, SERVICES, AND THREAT INTELLIGENCE FOR THE INDUSTRIAL COMMUNITY, VISIT WWW.DRAGOS.COM.

THANK YOU

Last modified September, 2021