The 2021 MITRE ATT&CK® Evaluation for Industrial Control Systems (ICS)

Safeguarding Civilization

Sergio Caltagirone, VP of Threat Intelligence
Alex Larson, Principal Reverse Engineer
Austin Scott, Principal Detection Engineer

SERGIO CALTAGIRONE

Vice President
of Threat Intelligence

ALEX LARSON

Principal
Reverse Engineer

AUSTIN SCOTT

Principal
Detection Engineer

Before We Get Started

- Webinar is being recorded
- Phones are muted
- Please ask questions using Zoom Q&A
- Enjoy the webinar!

Dragos Platform Performance

100%

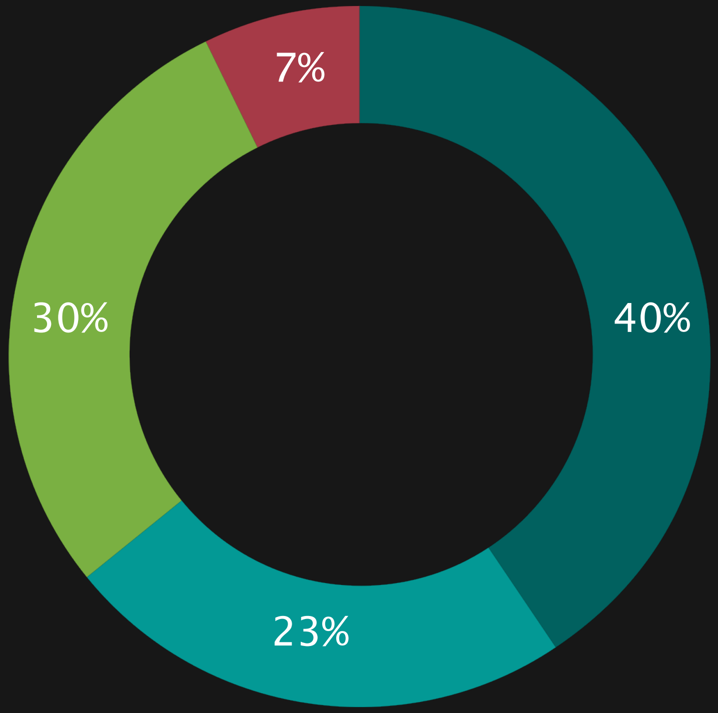
Adversary Step Coverage

Dragos Platform Performance

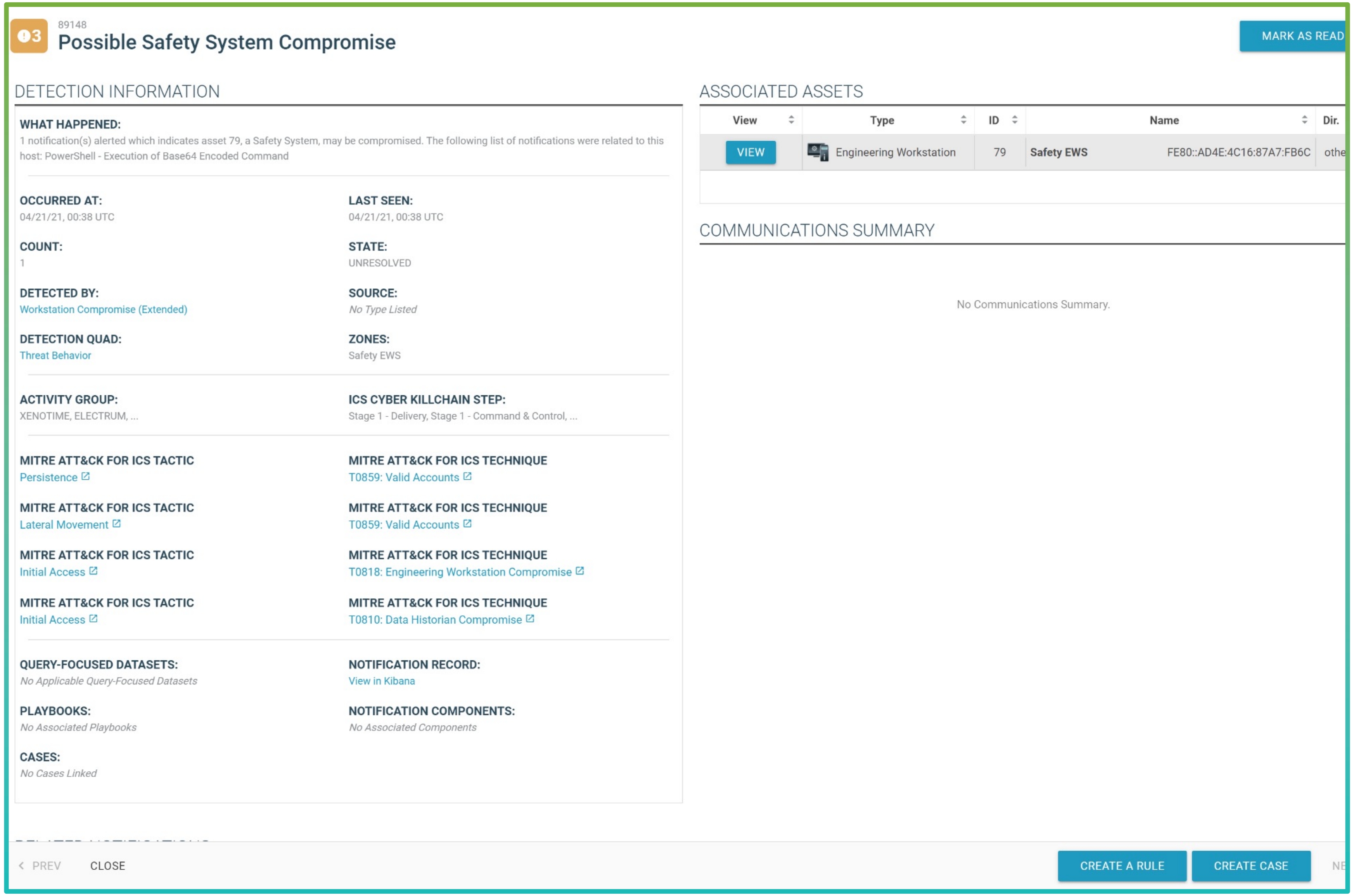
93%

Adversary Sub Step Coverage

ATT&CK Dragos Platform Adversary Activity Coverage By Category



Highlighted Detection from Evaluation



89148

Possible Safety System Compromise

DETECTION INFORMATION

WHAT HAPPENED:
1 notification(s) alerted which indicates asset 79, a Safety System, may be compromised. The following list of notifications were related to this host: PowerShell - Execution of Base64 Encoded Command

OCCURRED AT: 04/21/21, 00:38 UTC	**LAST SEEN:** 04/21/21, 00:38 UTC
COUNT: 1	**STATE:** UNRESOLVED
DETECTED BY: Workstation Compromise (Extended)	**SOURCE:** *No Type Listed*
DETECTION QUAD: Threat Behavior	**ZONES:** Safety EWS
ACTIVITY GROUP: XENOTIME, ELECTRUM, ...	**ICS CYBER KILLCHAIN STEP:** Stage 1 - Delivery, Stage 1 - Command & Control, ...
MITRE ATT&CK FOR ICS TACTIC Persistence	**MITRE ATT&CK FOR ICS TECHNIQUE** T0859: Valid Accounts
MITRE ATT&CK FOR ICS TACTIC Lateral Movement	**MITRE ATT&CK FOR ICS TECHNIQUE** T0859: Valid Accounts
MITRE ATT&CK FOR ICS TACTIC Initial Access	**MITRE ATT&CK FOR ICS TECHNIQUE** T0818: Engineering Workstation Compromise
MITRE ATT&CK FOR ICS TACTIC Initial Access	**MITRE ATT&CK FOR ICS TECHNIQUE** T0810: Data Historian Compromise
QUERY-FOCUSED DATASETS: *No Applicable Query-Focused Datasets*	**NOTIFICATION RECORD:** View in Kibana
PLAYBOOKS: *No Associated Playbooks*	**NOTIFICATION COMPONENTS:** *No Associated Components*
CASES: *No Cases Linked*	

ASSOCIATED ASSETS

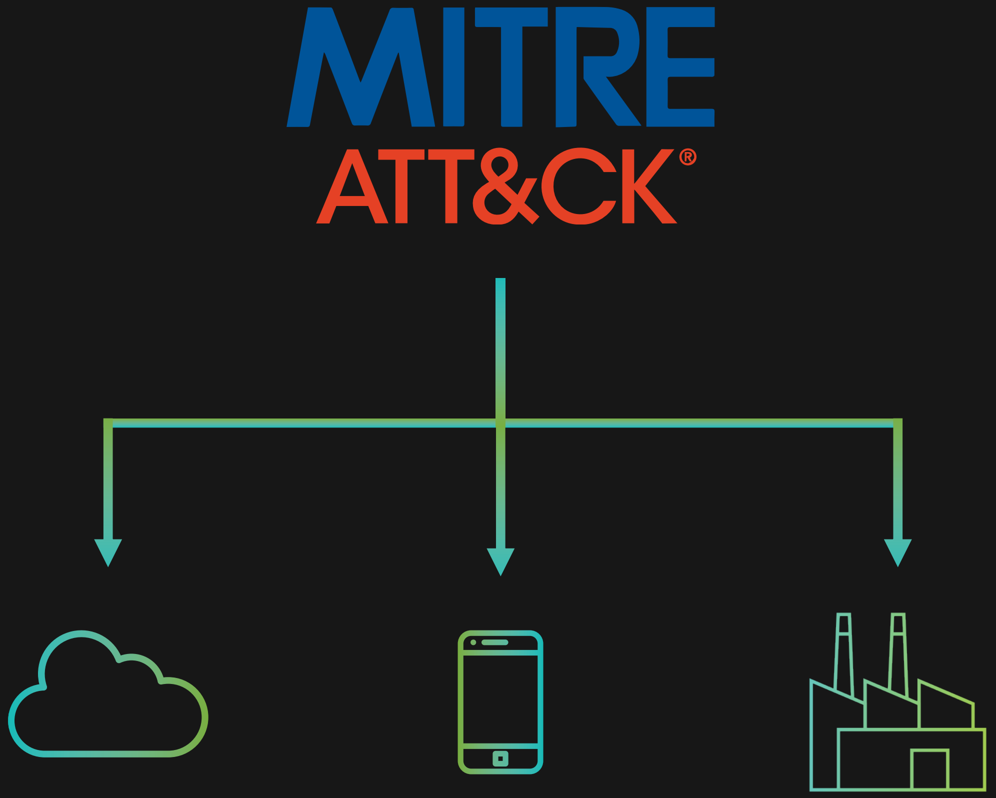
View	Type	ID	Name		Dir.
VIEW	Engineering Workstation	79	**Safety EWS**	FE80::AD4E:4C16:87A7:FB6C	othe

COMMUNICATIONS SUMMARY

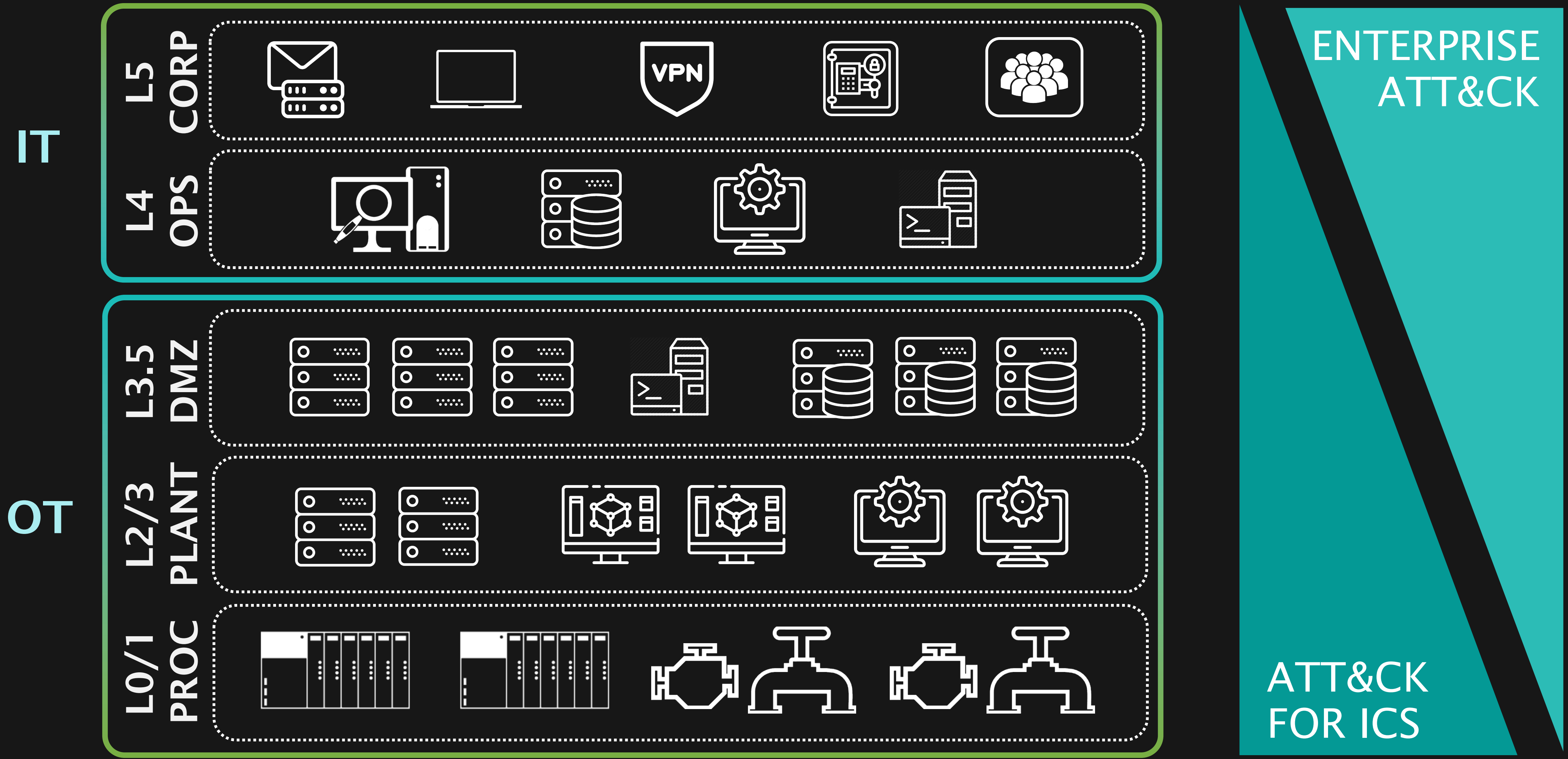
No Communications Summary.

What is MITRE ATT&CK® for ICS?

ATT&CK for ICS is an encyclopedia of ICS **threat behaviors.**



ATT&CK For Enterprise Vs. ATT&CK For ICS



How was MITRE ATT&CK® for ICS created?

MITRE ATT&CK for ICS was created by the ICS cybersecurity community.

100+

100+ participants

39

39+ Organizations

5

Over 5 Years

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

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

MITRE ENGENUITY™

ATT&CK® Evaluations

Vendors

Provide vendors with an assessment of their ability to defend against specific adversary tactics and techniques.

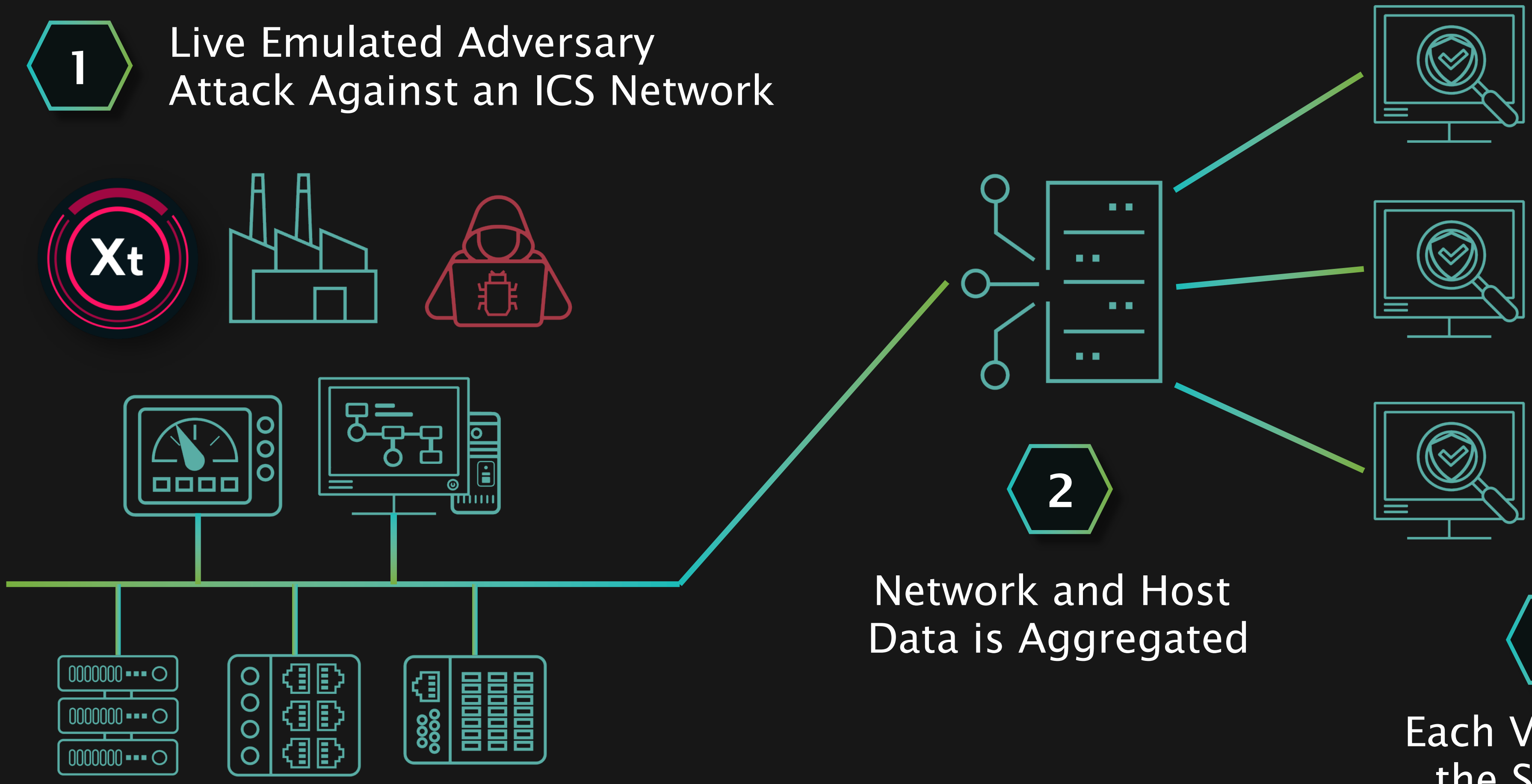
End Users

Provide industry end-users with information to make decisions that work best for their organizations.

No “Winners”

Not a competitive analysis. There are no scores, rankings, or ratings.

ATT&CK for ICS Evaluation Methodology



1 Live Emulated Adversary Attack Against an ICS Network

2 Network and Host Data is Aggregated

Vendor 1

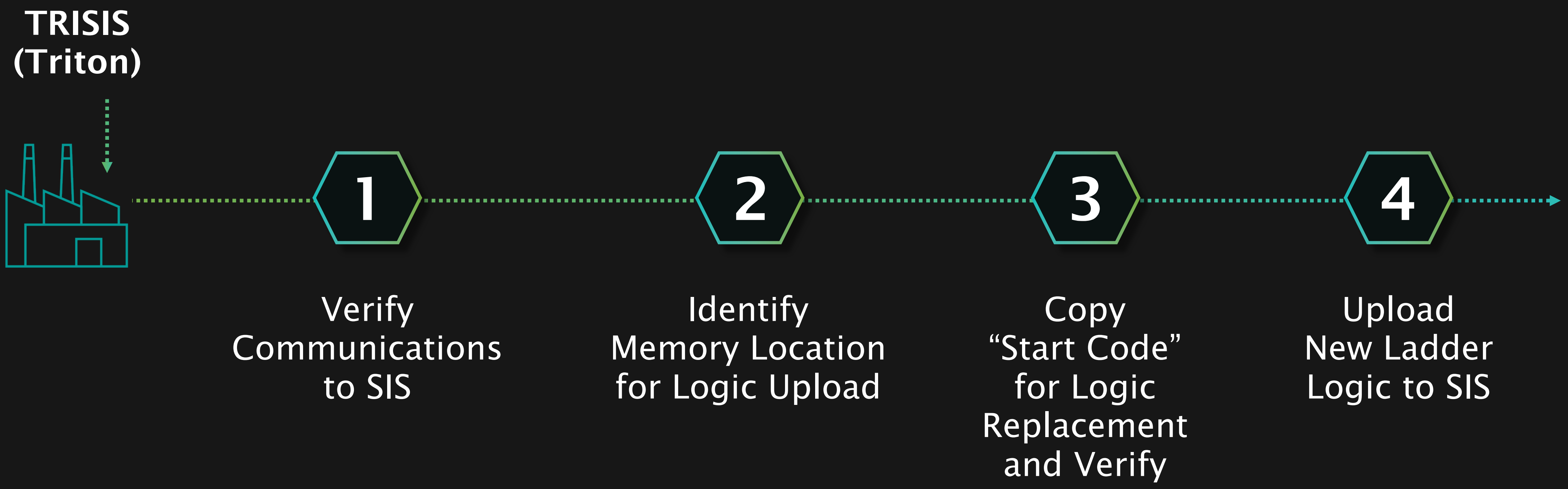
Vendor 2

Vendor 3

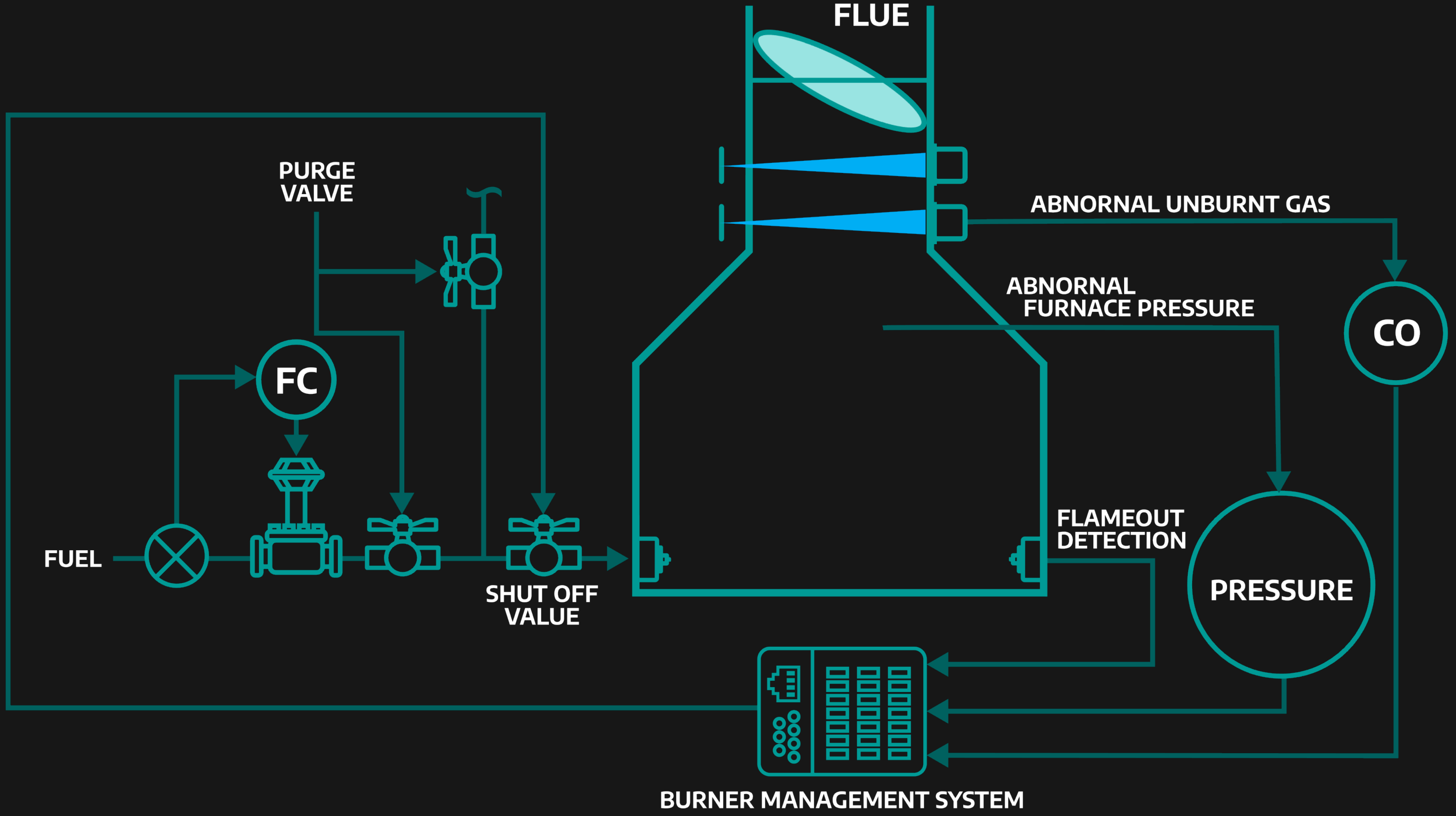
3 Each Vendor Sees the Same Data

XENOTIME

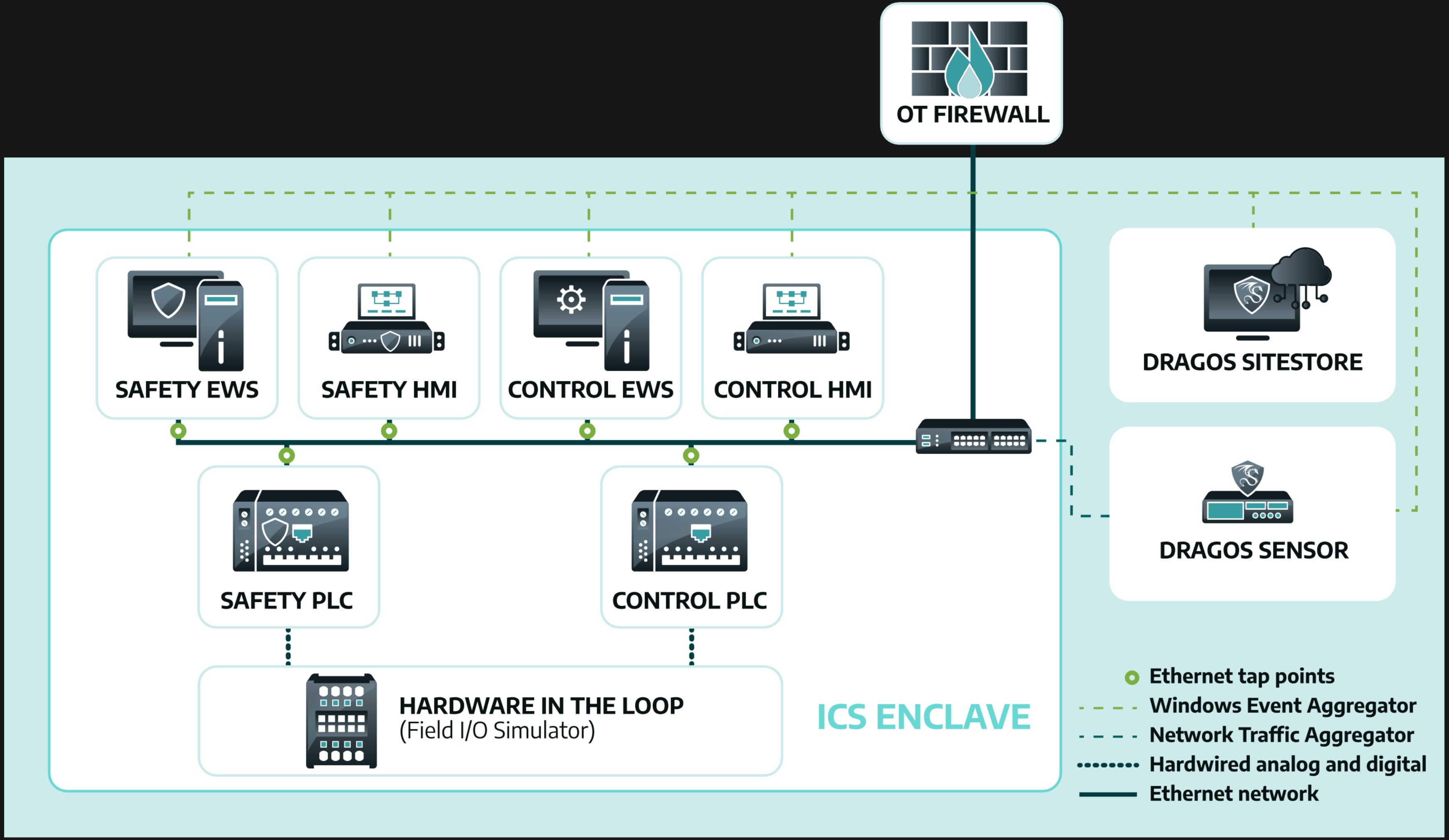
The **XENOTIME activity group** is attributed to the **TRISIS (AKA Triton)** malware and the attack of the safety instrumented systems at an oil refinery in Saudi Arabia in 2017. Industrial safety instrumented systems comprise part of a multi-layer engineered process control framework to protect life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


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

Burner Management System (BMS)

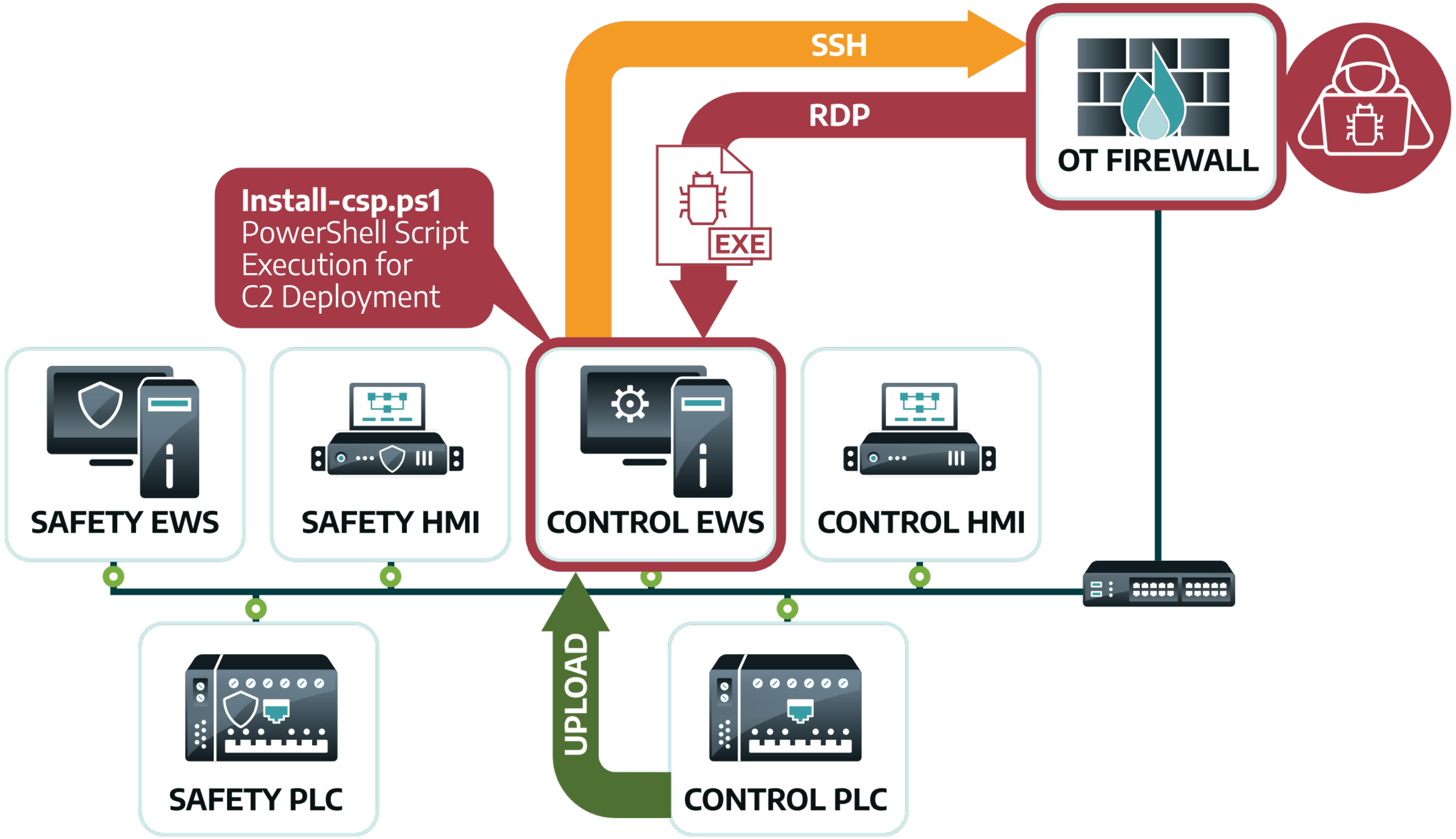


Dragos Platform/Network Architecture



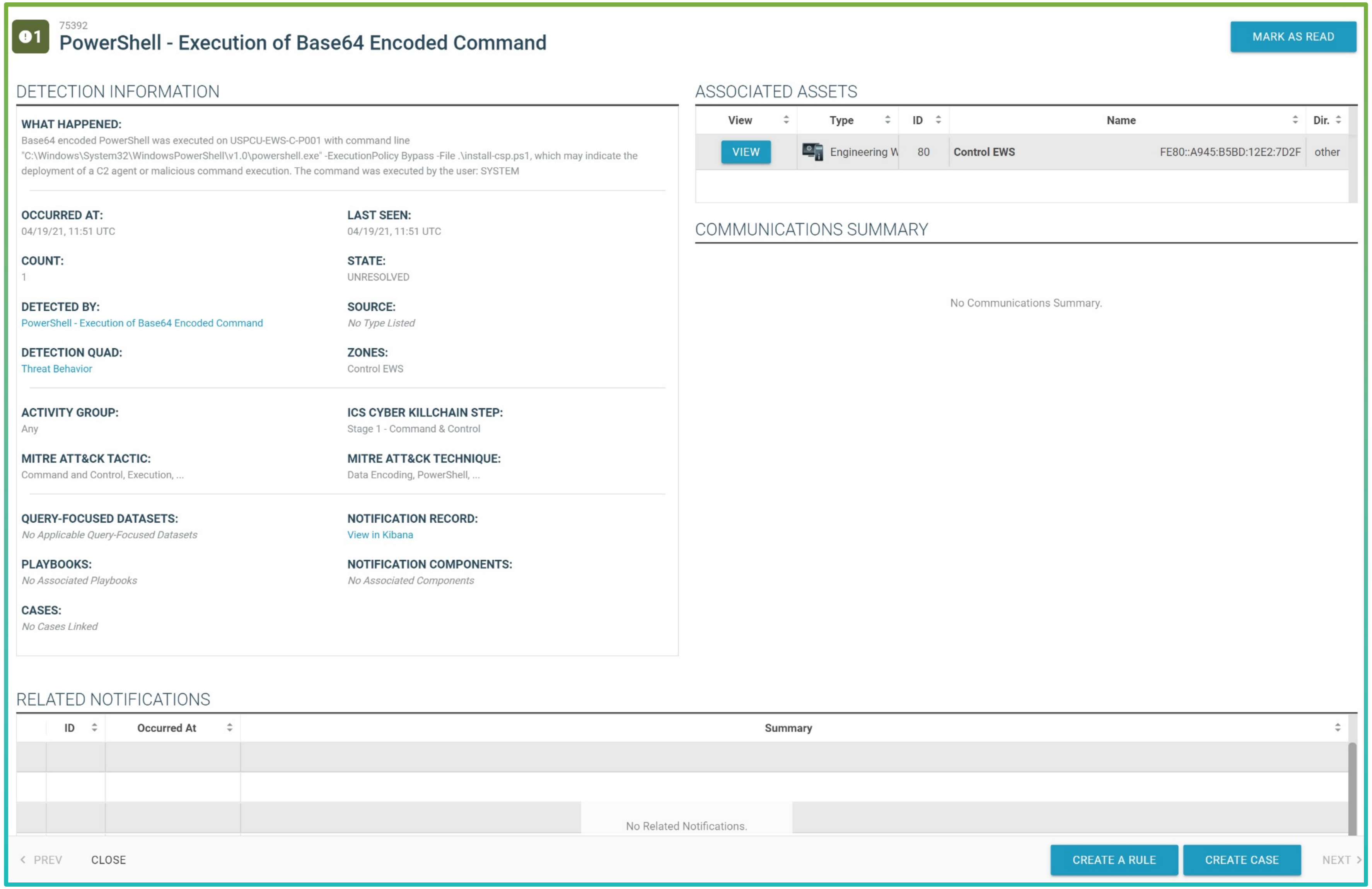
Day 1

Initial Pivot from IT into the OT Environment and Control Engineering Workstation Compromise



Day 1

Initial Pivot from IT into the OT Environment and Control Engineering Workstation Compromise



75392

PowerShell - Execution of Base64 Encoded Command

DETECTION INFORMATION

WHAT HAPPENED:
Base64 encoded PowerShell was executed on USPCU-EWS-C-P001 with command line "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ExecutionPolicy Bypass -File .\install-csp.ps1, which may indicate the deployment of a C2 agent or malicious command execution. The command was executed by the user: SYSTEM

OCCURRED AT: 04/19/21, 11:51 UTC

LAST SEEN: 04/19/21, 11:51 UTC

COUNT: 1

STATE: UNRESOLVED

DETECTED BY: PowerShell - Execution of Base64 Encoded Command

SOURCE: *No Type Listed*

DETECTION QUAD: Threat Behavior

ZONES: Control EWS

ACTIVITY GROUP: Any

ICS CYBER KILLCHAIN STEP: Stage 1 - Command & Control

MITRE ATT&CK TACTIC: Command and Control, Execution, ...

MITRE ATT&CK TECHNIQUE: Data Encoding, PowerShell, ...

QUERY-FOCUSED DATASETS: *No Applicable Query-Focused Datasets*

NOTIFICATION RECORD: View in Kibana

PLAYBOOKS: *No Associated Playbooks*

NOTIFICATION COMPONENTS: *No Associated Components*

CASES: *No Cases Linked*

ASSOCIATED ASSETS

View	Type	ID	Name		Dir.
VIEW	Engineering W	80	**Control EWS**	FE80::A945:B5BD:12E2:7D2F	other

COMMUNICATIONS SUMMARY

No Communications Summary.

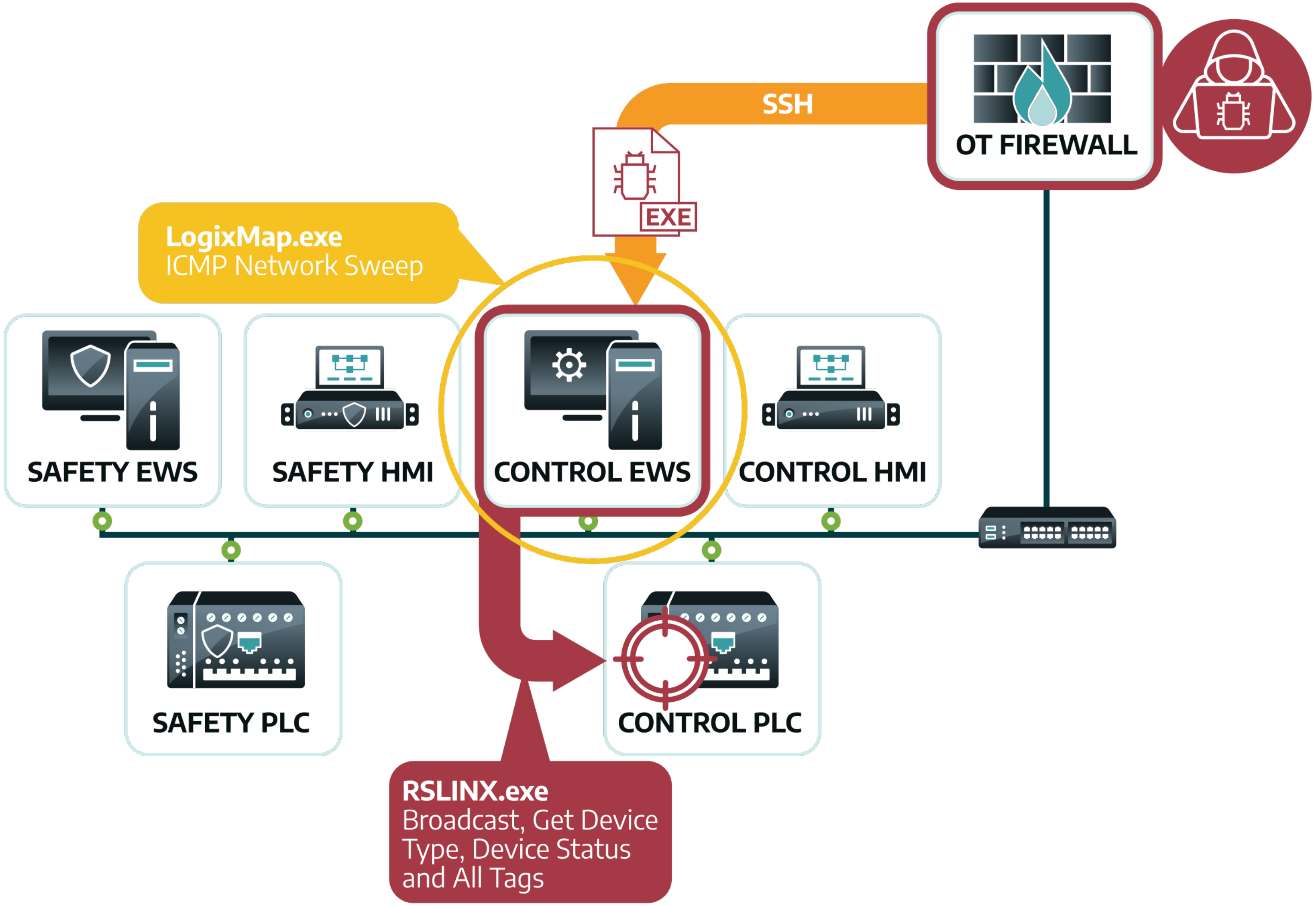
RELATED NOTIFICATIONS

ID	Occurred At	Summary

No Related Notifications.

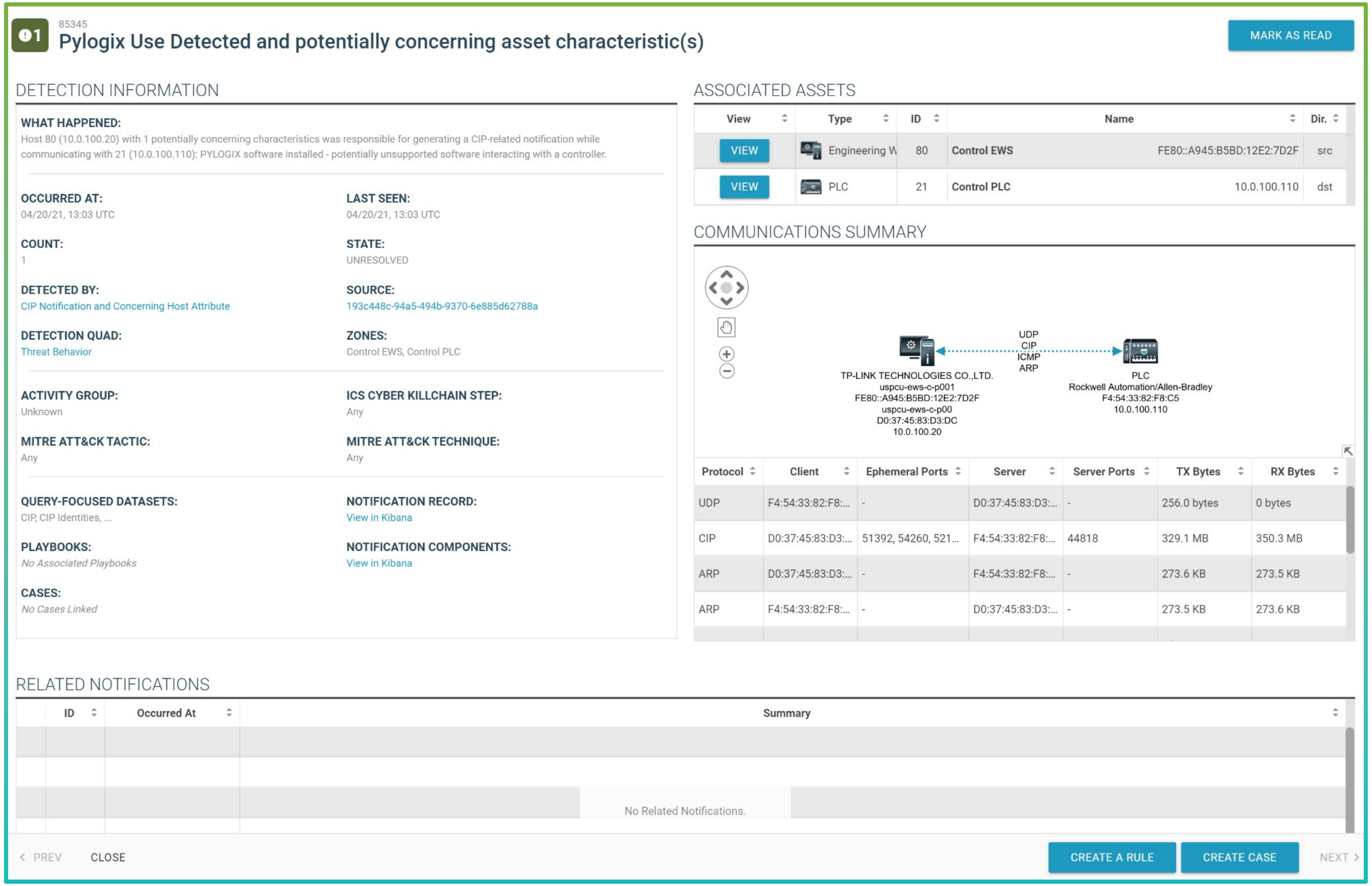
Day 2

PLC Enumeration Using Python Compiled Windows Binaries



Day 2

PLC Enumeration Using Python Compiled Windows Binaries



85345

Pylogix Use Detected and potentially concerning asset characteristic(s)

DETECTION INFORMATION

WHAT HAPPENED:
Host 80 (10.0.100.20) with 1 potentially concerning characteristics was responsible for generating a CIP-related notification while communicating with 21 (10.0.100.110): PYLOGIX software installed - potentially unsupported software interacting with a controller.

OCCURRED AT: 04/20/21, 13:03 UTC

LAST SEEN: 04/20/21, 13:03 UTC

COUNT: 1

STATE: UNRESOLVED

DETECTED BY: CIP Notification and Concerning Host Attribute

SOURCE: 193c448c-94a5-494b-9370-6e885d62788a

DETECTION QUAD: Threat Behavior

ZONES: Control EWS, Control PLC

ACTIVITY GROUP: Unknown

ICS CYBER KILLCHAIN STEP: Any

MITRE ATT&CK TACTIC: Any

MITRE ATT&CK TECHNIQUE: Any

QUERY-FOCUSED DATASETS: CIP, CIP Identities, ...

NOTIFICATION RECORD: View in Kibana

PLAYBOOKS: *No Associated Playbooks*

NOTIFICATION COMPONENTS: View in Kibana

CASES: *No Cases Linked*

ASSOCIATED ASSETS

View	Type	ID	Name		Dir.
VIEW	Engineering W	80	**Control EWS**	FE80::A945:B5BD:12E2:7D2F	src
VIEW	PLC	21	**Control PLC**	10.0.100.110	dst

COMMUNICATIONS SUMMARY

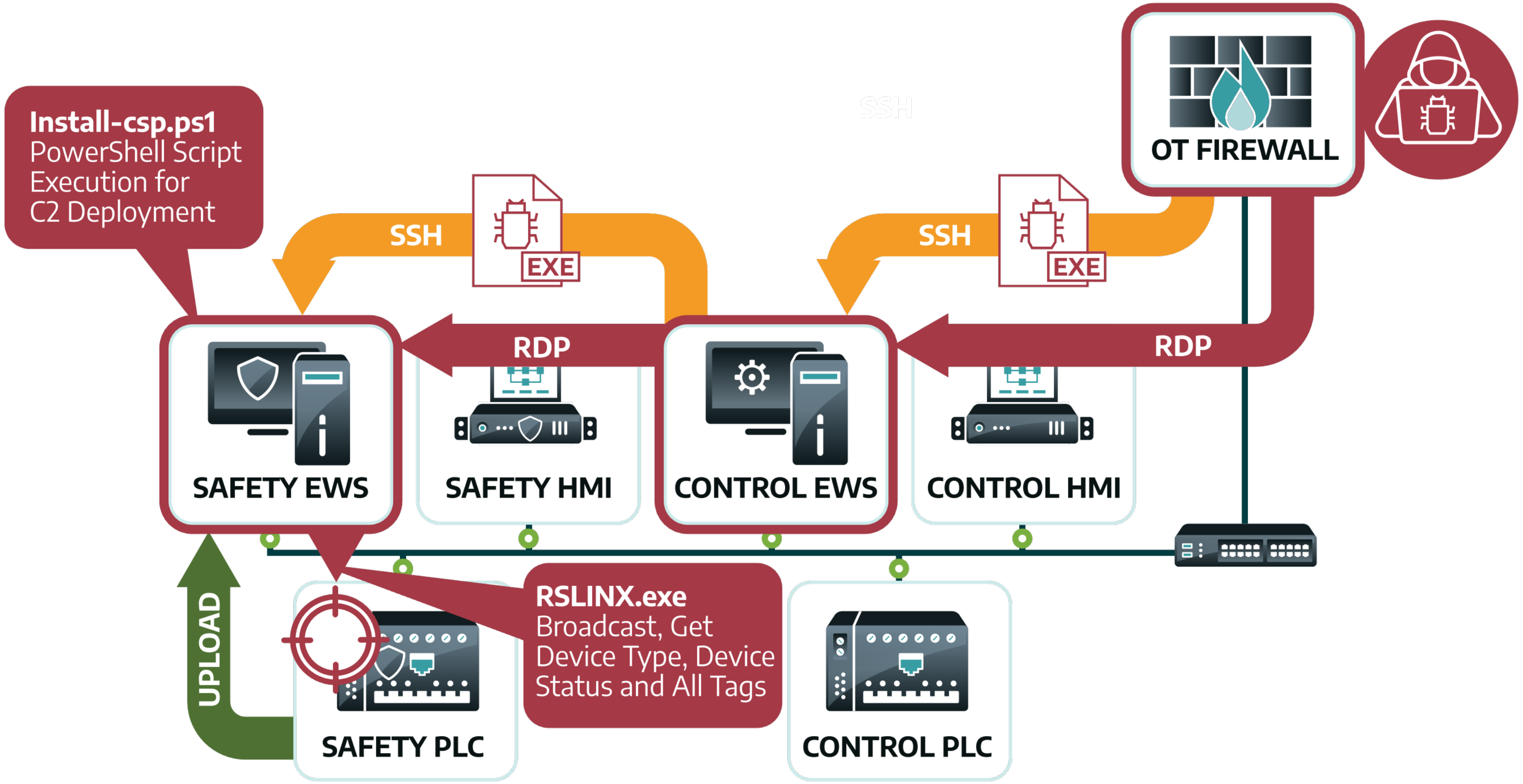
Protocol	Client	Ephemeral Ports	Server	Server Ports	TX Bytes	RX Bytes
UDP	F4:54:33:82:F8:...	-	D0:37:45:83:D3:...	-	256.0 bytes	0 bytes
CIP	D0:37:45:83:D3:...	51392, 54260, 521...	F4:54:33:82:F8:...	44818	329.1 MB	350.3 MB
ARP	D0:37:45:83:D3:...	-	F4:54:33:82:F8:...	-	273.6 KB	273.5 KB
ARP	F4:54:33:82:F8:...	-	D0:37:45:83:D3:...	-	273.5 KB	273.6 KB

RELATED NOTIFICATIONS

ID	Occurred At	Summary
		No Related Notifications.

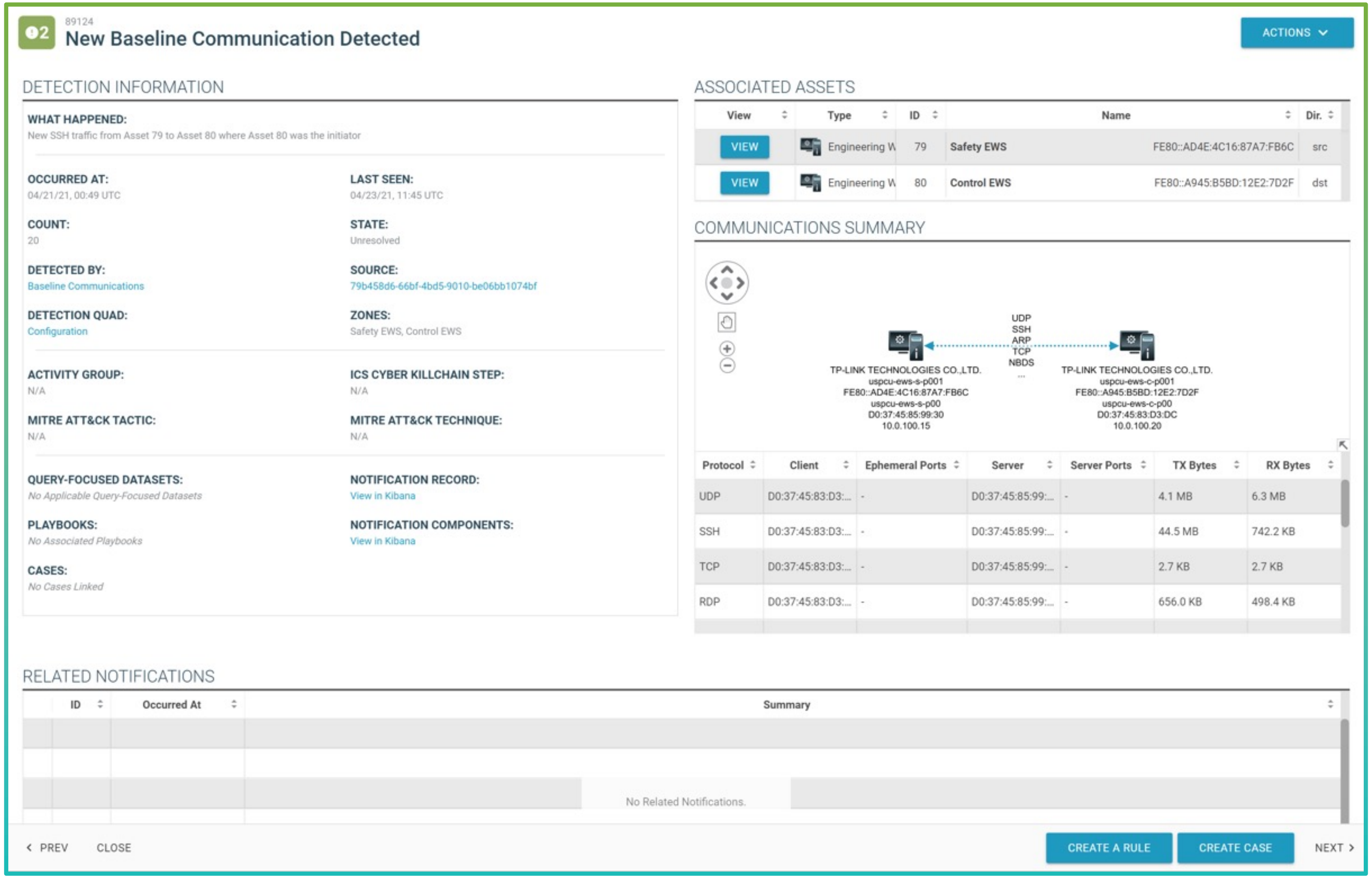
Day 3

Pivot into Safety System



Day 3

Pivot into Safety System



89124

New Baseline Communication Detected

DETECTION INFORMATION

WHAT HAPPENED:
New SSH traffic from Asset 79 to Asset 80 where Asset 80 was the initiator

OCCURRED AT:
04/21/21, 00:49 UTC

LAST SEEN:
04/23/21, 11:45 UTC

COUNT:
20

STATE:
Unresolved

DETECTED BY:
Baseline Communications

SOURCE:
79b458d6-66bf-4bd5-9010-be06bb1074bf

DETECTION QUAD:
Configuration

ZONES:
Safety EWS, Control EWS

ACTIVITY GROUP:
N/A

ICS CYBER KILLCHAIN STEP:
N/A

MITRE ATT&CK TACTIC:
N/A

MITRE ATT&CK TECHNIQUE:
N/A

QUERY-FOCUSED DATASETS:
No Applicable Query-Focused Datasets

NOTIFICATION RECORD:
View in Kibana

PLAYBOOKS:
No Associated Playbooks

NOTIFICATION COMPONENTS:
View in Kibana

CASES:
No Cases Linked

ASSOCIATED ASSETS

View	Type	ID	Name		Dir.
VIEW	Engineering W	79	**Safety EWS**	FE80::AD4E:4C16:87A7:FB6C	src
VIEW	Engineering W	80	**Control EWS**	FE80::A945:B5BD:12E2:7D2F	dst

COMMUNICATIONS SUMMARY

Protocol	Client	Ephemeral Ports	Server	Server Ports	TX Bytes	RX Bytes
UDP	D0:37:45:83:D3:...	-	D0:37:45:85:99:...	-	4.1 MB	6.3 MB
SSH	D0:37:45:83:D3:...	-	D0:37:45:85:99:...	-	44.5 MB	742.2 KB
TCP	D0:37:45:83:D3:...	-	D0:37:45:85:99:...	-	2.7 KB	2.7 KB
RDP	D0:37:45:83:D3:...	-	D0:37:45:85:99:...	-	656.0 KB	498.4 KB

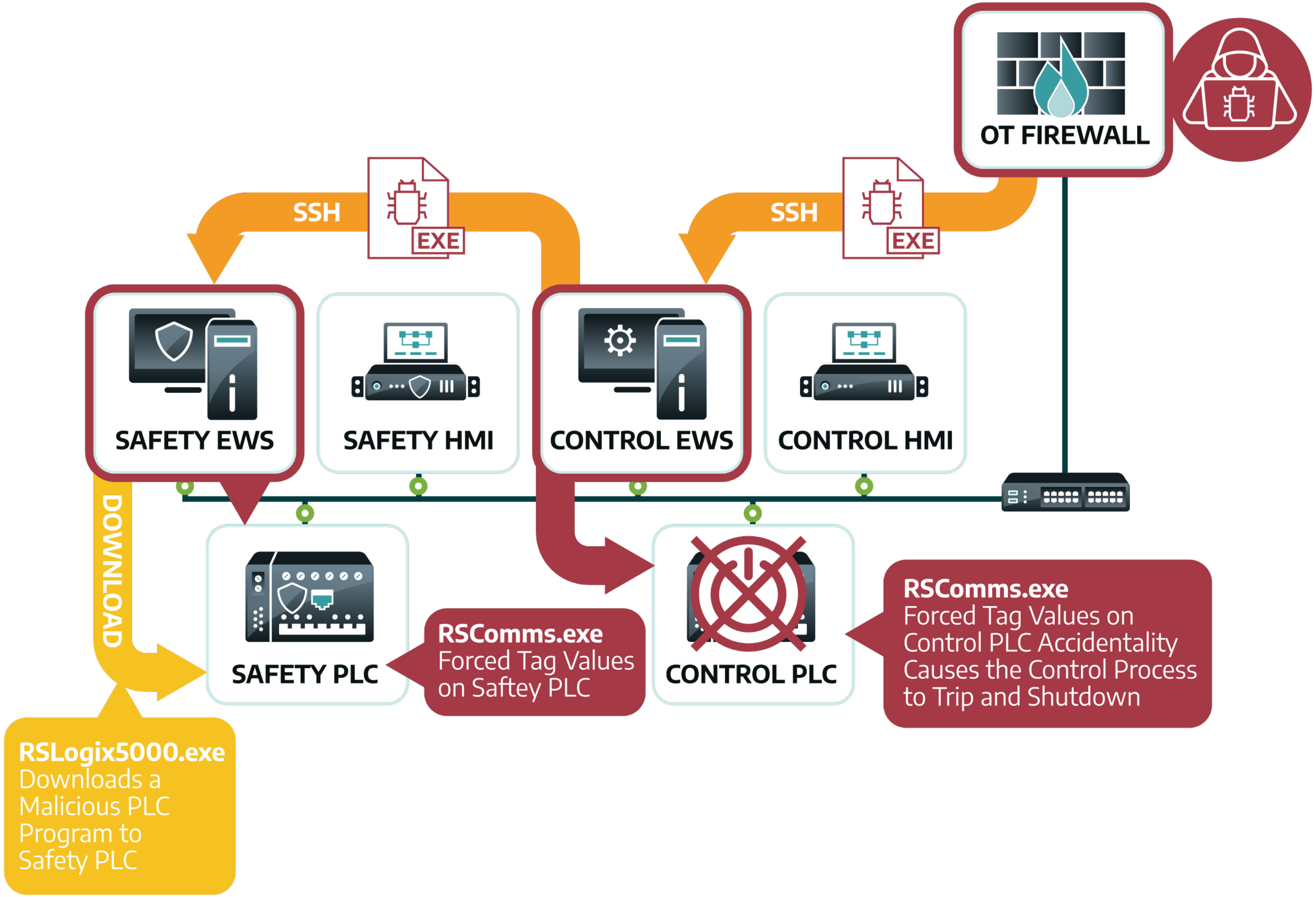
RELATED NOTIFICATIONS

ID	Occurred At	Summary

No Related Notifications.

Day 4

Left of Control PLC and Safety PLC Program Modifications and Plant Trip



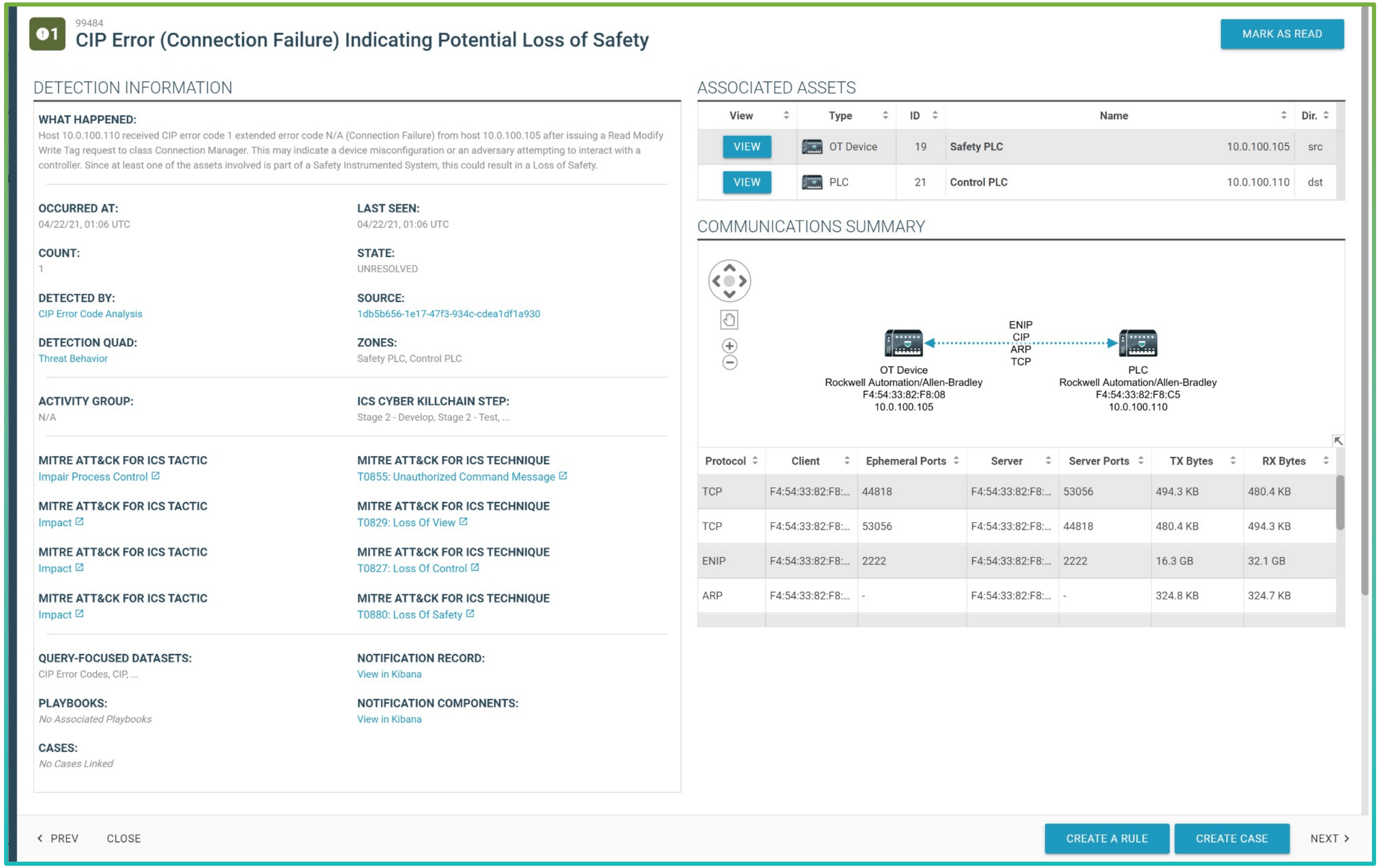
RSLogix5000.exe Downloads a Malicious PLC Program to Safety PLC

RSComms.exe Forced Tag Values on Saftey PLC

RSComms.exe Forced Tag Values on Control PLC Accidentality Causes the Control Process to Trip and Shutdown

Day 4

Left of Control PLC and Safety PLC Program Modifications and Plant Trip



99484

CIP Error (Connection Failure) Indicating Potential Loss of Safety

DETECTION INFORMATION

WHAT HAPPENED:
Host 10.0.100.110 received CIP error code 1 extended error code N/A (Connection Failure) from host 10.0.100.105 after issuing a Read Modify Write Tag request to class Connection Manager. This may indicate a device misconfiguration or an adversary attempting to interact with a controller. Since at least one of the assets involved is part of a Safety Instrumented System, this could result in a Loss of Safety.

OCCURRED AT: 04/22/21, 01:06 UTC

LAST SEEN: 04/22/21, 01:06 UTC

COUNT: 1

STATE: UNRESOLVED

DETECTED BY: CIP Error Code Analysis

SOURCE: 1db5b656-1e17-47f3-934c-cdea1df1a930

DETECTION QUAD: Threat Behavior

ZONES: Safety PLC, Control PLC

ACTIVITY GROUP: N/A

ICS CYBER KILLCHAIN STEP: Stage 2 - Develop, Stage 2 - Test, ...

MITRE ATT&CK FOR ICS TACTIC	MITRE ATT&CK FOR ICS TECHNIQUE
Impair Process Control	T0855: Unauthorized Command Message
Impact	T0829: Loss Of View
Impact	T0827: Loss Of Control
Impact	T0880: Loss Of Safety

QUERY-FOCUSED DATASETS: CIP Error Codes, CIP, ...

NOTIFICATION RECORD: View in Kibana

PLAYBOOKS: *No Associated Playbooks*

NOTIFICATION COMPONENTS: View in Kibana

CASES: *No Cases Linked*

ASSOCIATED ASSETS

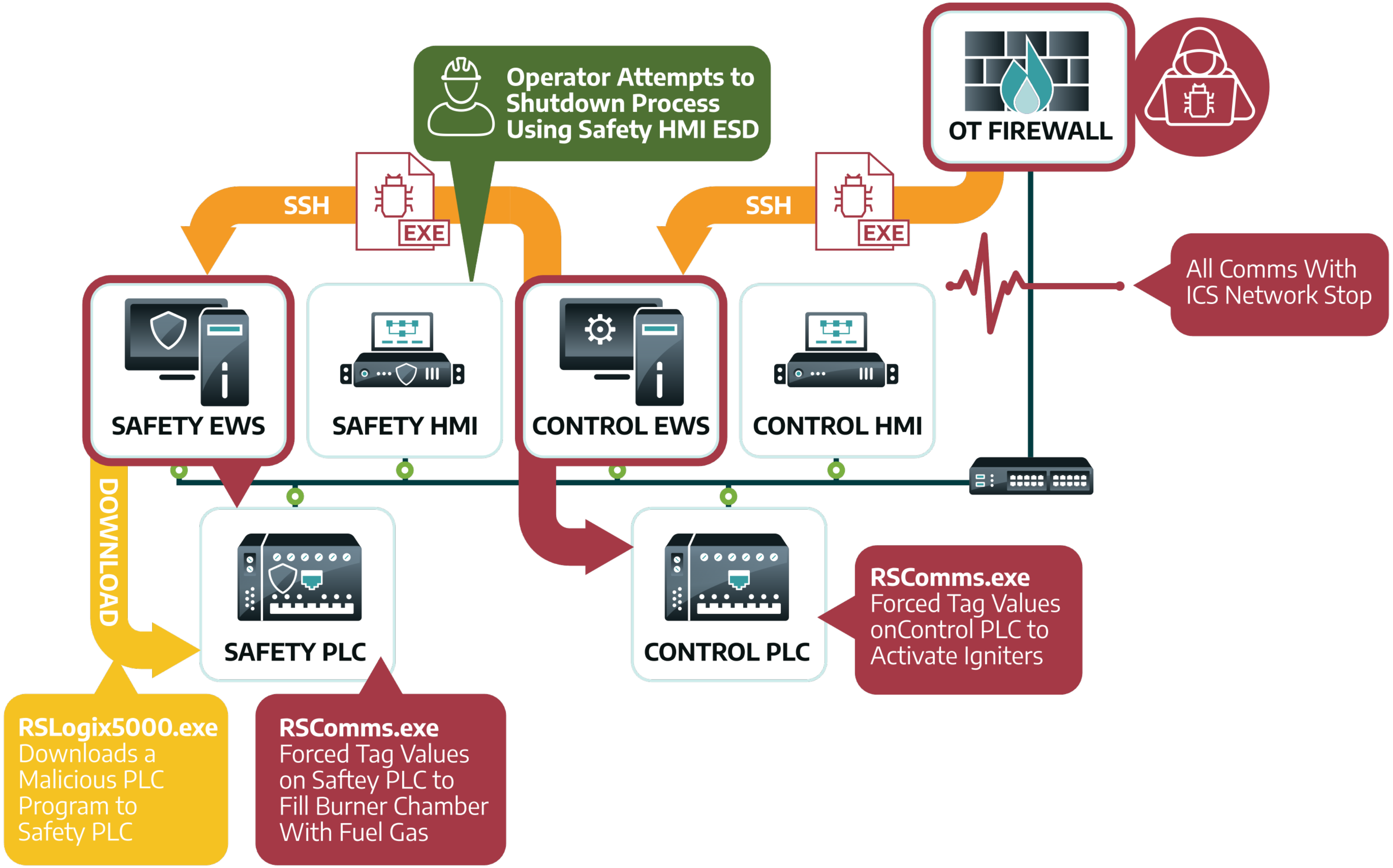
View	Type	ID	Name		Dir.
VIEW	OT Device	19	**Safety PLC**	10.0.100.105	src
VIEW	PLC	21	**Control PLC**	10.0.100.110	dst

COMMUNICATIONS SUMMARY

Protocol	Client	Ephemeral Ports	Server	Server Ports	TX Bytes	RX Bytes
TCP	F4:54:33:82:F8:...	44818	F4:54:33:82:F8:...	53056	494.3 KB	480.4 KB
TCP	F4:54:33:82:F8:...	53056	F4:54:33:82:F8:...	44818	480.4 KB	494.3 KB
ENIP	F4:54:33:82:F8:...	2222	F4:54:33:82:F8:...	2222	16.3 GB	32.1 GB
ARP	F4:54:33:82:F8:...	-	F4:54:33:82:F8:...	-	324.8 KB	324.7 KB

Day 5

Left of Boom



Operator Attempts to Shutdown Process Using Safety HMI ESD

All Comms With ICS Network Stop

RSComms.exe Forced Tag Values onControl PLC to Activate Igniters

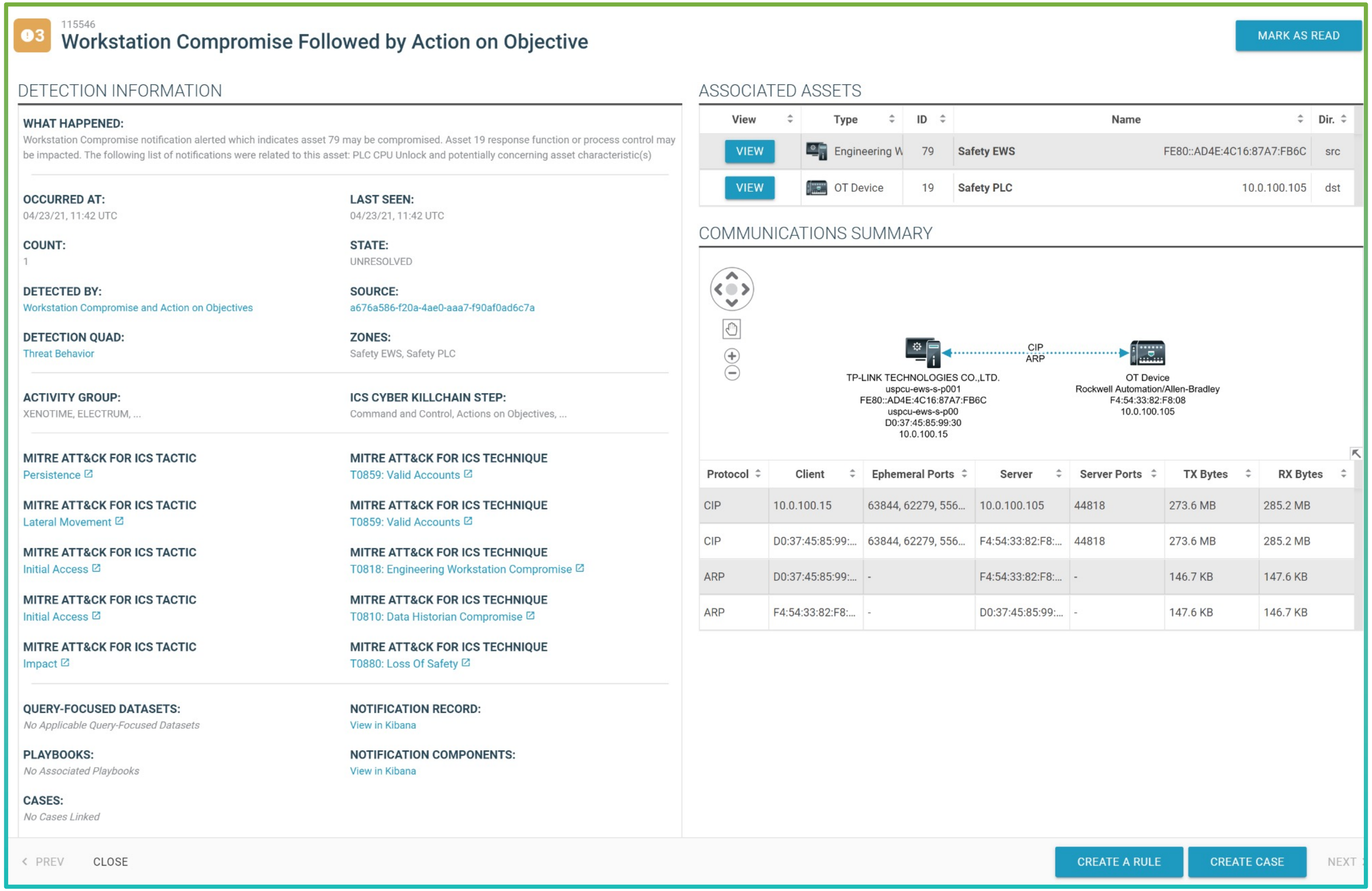
RSLogix5000.exe Downloads a Malicious PLC Program to Safety PLC

RSComms.exe Forced Tag Values on Saftey PLC to Fill Burner Chamber With Fuel Gas

DRAGOS

Day 5

Left of Boom



115546

Workstation Compromise Followed by Action on Objective

DETECTION INFORMATION

WHAT HAPPENED:
Workstation Compromise notification alerted which indicates asset 79 may be compromised. Asset 19 response function or process control may be impacted. The following list of notifications were related to this asset: PLC CPU Unlock and potentially concerning asset characteristic(s)

OCCURRED AT:
04/23/21, 11:42 UTC

LAST SEEN:
04/23/21, 11:42 UTC

COUNT:
1

STATE:
UNRESOLVED

DETECTED BY:
Workstation Compromise and Action on Objectives

SOURCE:
a676a586-f20a-4ae0-aaa7-f90af0ad6c7a

DETECTION QUAD:
Threat Behavior

ZONES:
Safety EWS, Safety PLC

ACTIVITY GROUP:
XENOTIME, ELECTRUM, ...

ICS CYBER KILLCHAIN STEP:
Command and Control, Actions on Objectives, ...

MITRE ATT&CK FOR ICS TACTIC
Persistence

MITRE ATT&CK FOR ICS TECHNIQUE
T0859: Valid Accounts

MITRE ATT&CK FOR ICS TACTIC
Lateral Movement

MITRE ATT&CK FOR ICS TECHNIQUE
T0859: Valid Accounts

MITRE ATT&CK FOR ICS TACTIC
Initial Access

MITRE ATT&CK FOR ICS TECHNIQUE
T0818: Engineering Workstation Compromise

MITRE ATT&CK FOR ICS TACTIC
Initial Access

MITRE ATT&CK FOR ICS TECHNIQUE
T0810: Data Historian Compromise

MITRE ATT&CK FOR ICS TACTIC
Impact

MITRE ATT&CK FOR ICS TECHNIQUE
T0880: Loss Of Safety

QUERY-FOCUSED DATASETS:
No Applicable Query-Focused Datasets

NOTIFICATION RECORD:
View in Kibana

PLAYBOOKS:
No Associated Playbooks

NOTIFICATION COMPONENTS:
View in Kibana

CASES:
No Cases Linked

ASSOCIATED ASSETS

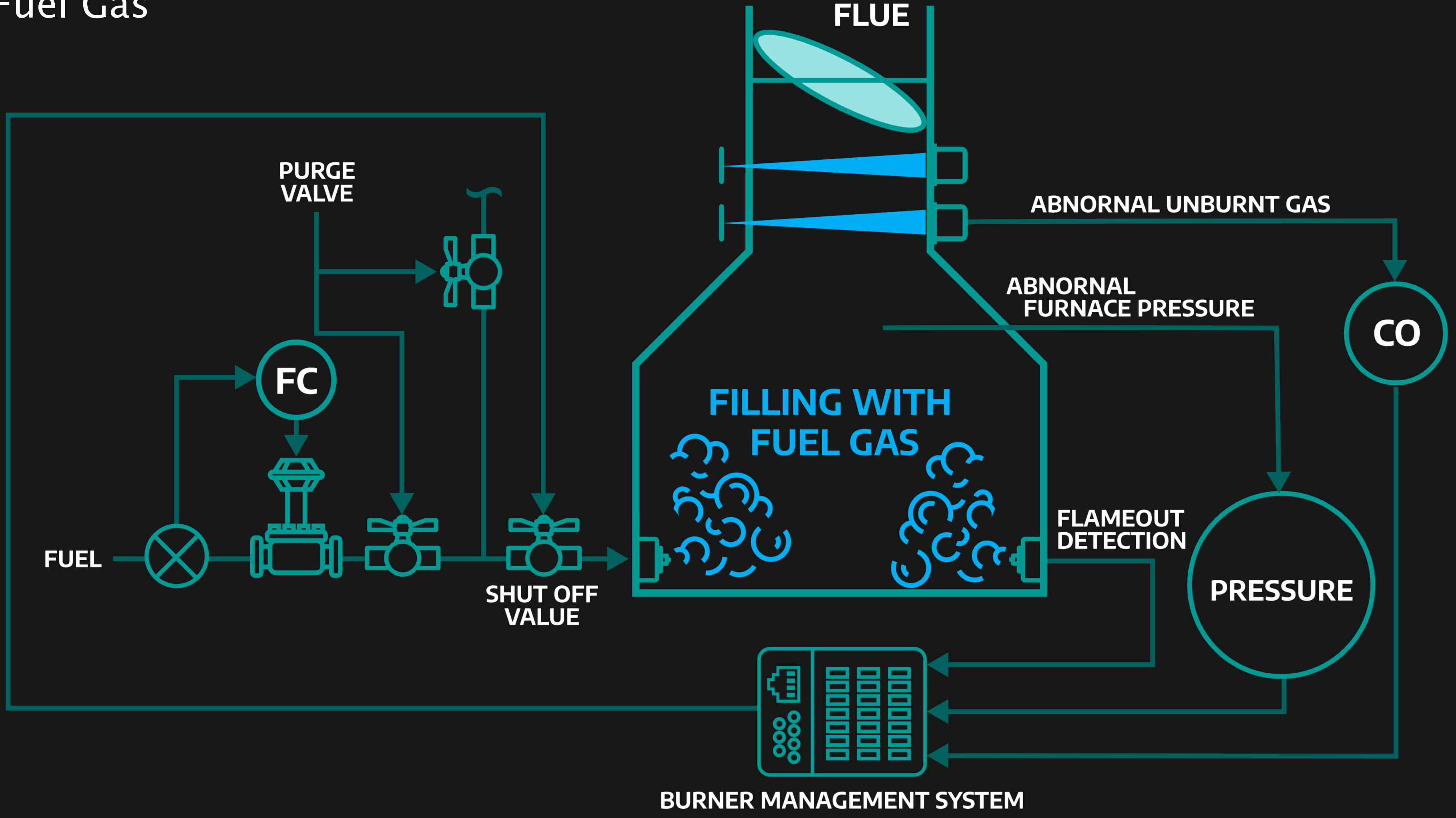
View	Type	ID	Name		Dir.
VIEW	Engineering W	79	Safety EWS	FE80::AD4E:4C16:87A7:FB6C	src
VIEW	OT Device	19	Safety PLC	10.0.100.105	dst

COMMUNICATIONS SUMMARY

Protocol	Client	Ephemeral Ports	Server	Server Ports	TX Bytes	RX Bytes
CIP	10.0.100.15	63844, 62279, 556...	10.0.100.105	44818	273.6 MB	285.2 MB
CIP	D0:37:45:85:99:...	63844, 62279, 556...	F4:54:33:82:F8:...	44818	273.6 MB	285.2 MB
ARP	D0:37:45:85:99:...	-	F4:54:33:82:F8:...	-	146.7 KB	147.6 KB
ARP	F4:54:33:82:F8:...	-	D0:37:45:85:99:...	-	147.6 KB	146.7 KB

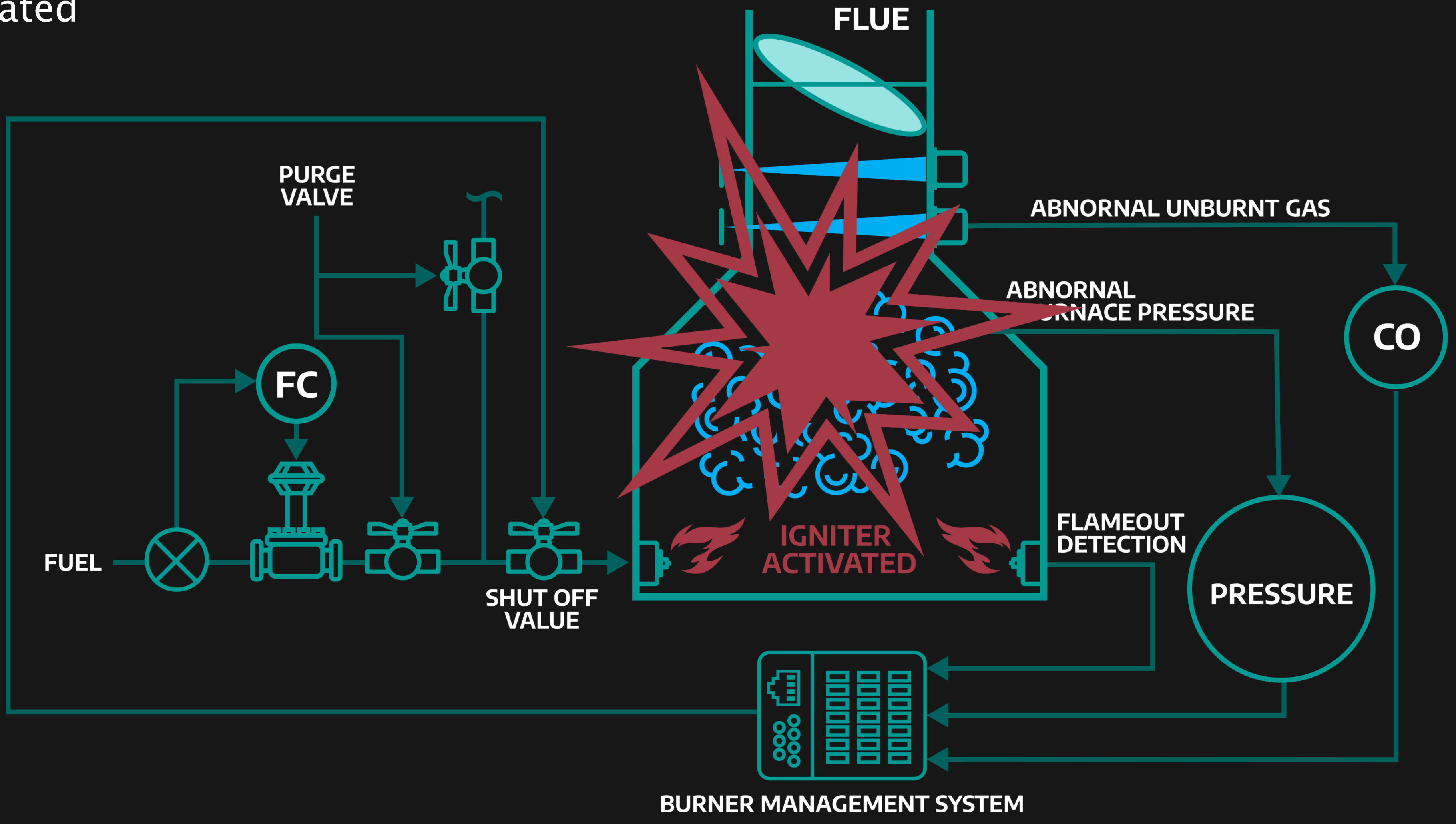
Burner Management System (BMS)

Filling With Fuel Gas

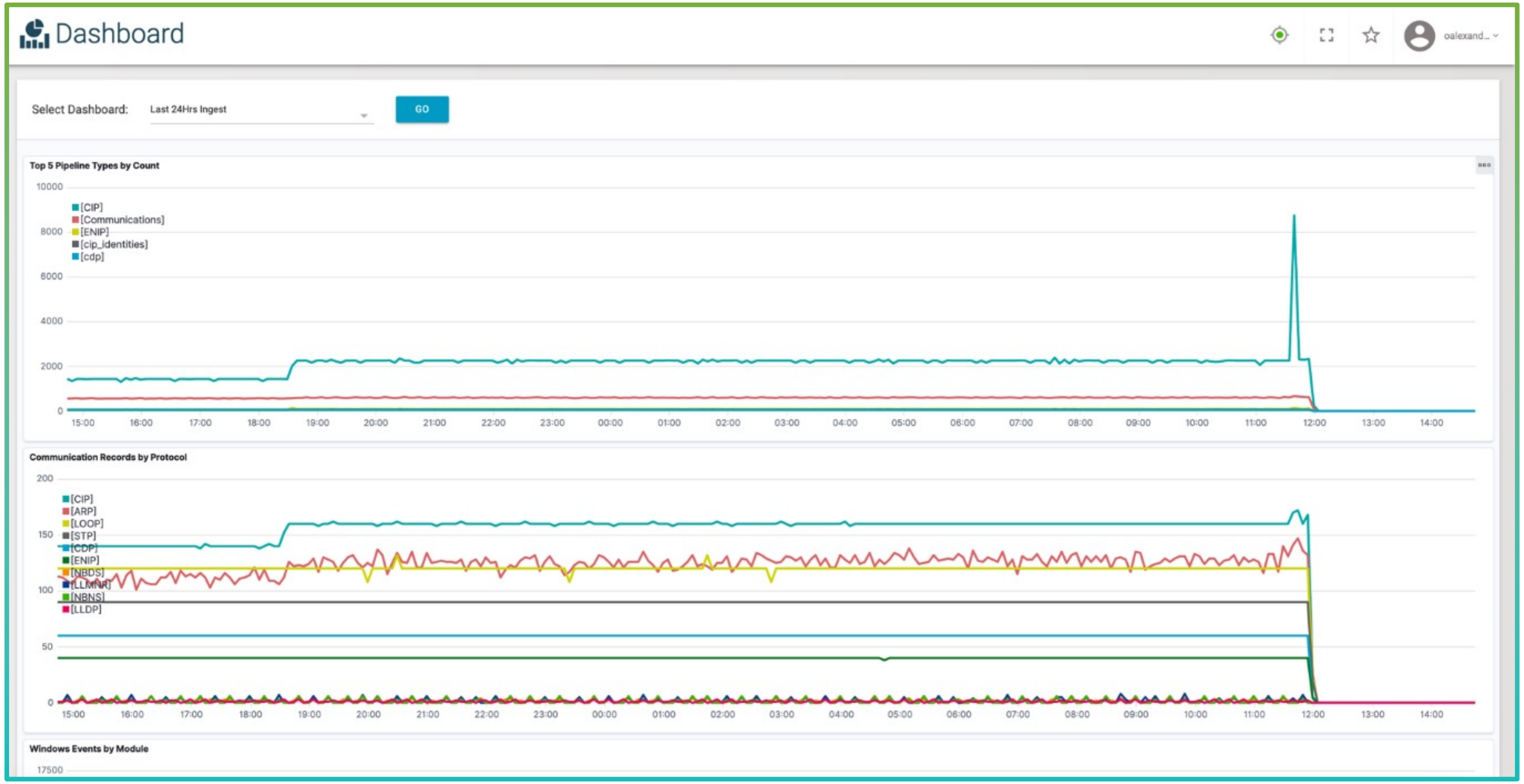


Burner Management System (BMS)

Igniter Activated



Boom



Dashboard

Select Dashboard: Last 24Hrs Ingest

MITRE Evaluation Results

DETECTION COUNT

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.

156 across 100
substeps

ANALYTIC COVERAGE

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.

63 of 100
substeps

TELEMETRY COVERAGE

The proportion of sub-steps that produced a detection with minimal processing.Telemetry is the foundational 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.

93 of 100
substeps

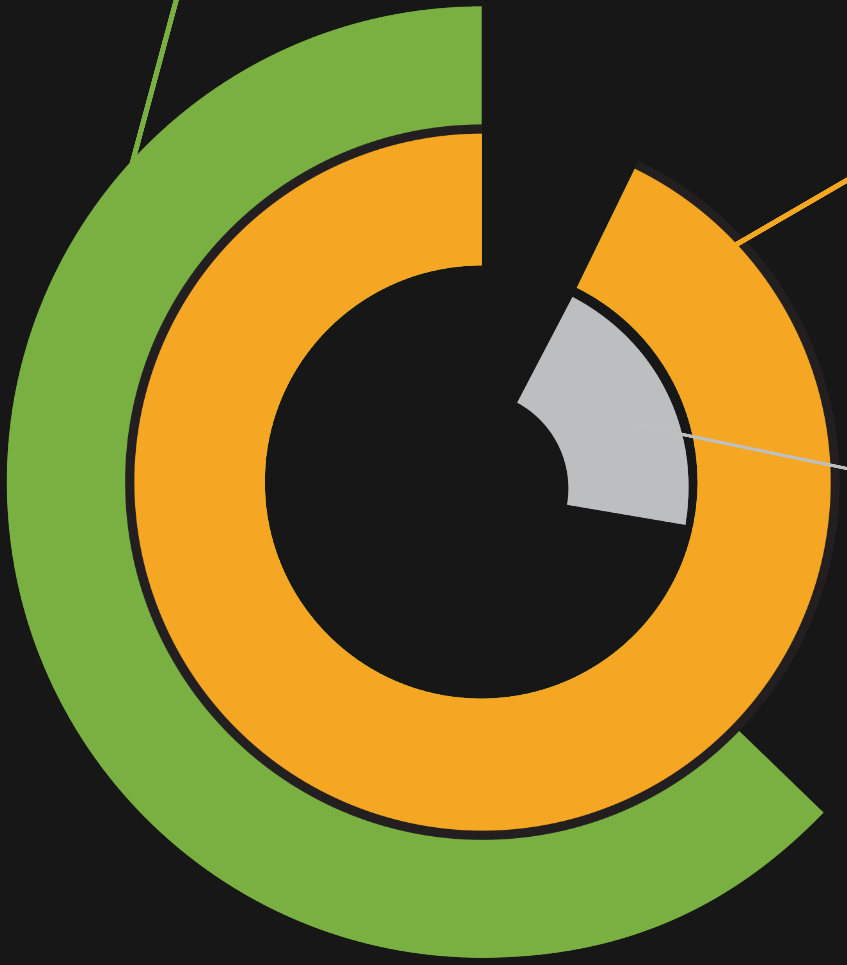
VISIBILITY

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 vendors 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 the ratio of Analytic Coverage to Telemetry Coverage.

93 of 100
substeps

DRAGOS

	DETECTION COUNT	ANALYTIC COVERAGE	TELEMETRY COVERAGE	VISIBILITY
DRAGOS	156 across 100 substeps	63 of 100 substeps	93 of 100 substeps	93 of 100 substeps



ANALYTIC COVERAGE

63

of 100 substeps

VISIBILITY

93

of 100 substeps

IDENTIFIED OPPORTUNITIES FOR THREAT DETECTION IMPROVEMENTS

20

of 100 substeps

Lessons Learned/Platform Improvements

- 20 substeps that we have Telemetry for but did not trigger a Detection.
- Port scanning and ICMP sweeping. Ability to configure analytics on a per network basis.
- 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)
- Improvements to C2 / Lateral movement detections to closely track SSH and other interactive protocols.

About Dragos

- 600+ YEARS OF ICS/OT EXPERIENCE
- 300+ EMPLOYEES
- 135+ CUSTOMERS
- 20 COUNTRIES
- 10 INDUSTRY VERTICALS

WORLD ECONOMIC FORUM 20 YEARS
Technology Pioneers 2020

HQ | Hanover, MD REGIONAL | Houston, TX

Dragos has the largest team of ICS security specialists in the industry which allows us to make the best technology.

- ELECTRIC
- OIL & GAS
- MANUFACTURING
- BLDG AUTO SYS
- CHEMICAL
- WATER
- FOOD & BEV
- MINING
- TRANSPORTATION
- PHARMACEUTICAL

Including 9 of the 10 largest U.S. electric utilities and 5 of the 10 largest oil and gas companies