

Detecting and Understanding Unusual Network Activity in a Plant Environment

The Story of PlantCo

Sam Van Ryder, Dragos



What You'll Learn

- Who is Dragos?
- Case Study: PlantCo
- How to Get Started



BUILT BY PRACTITIONERS FOR PRACTITIONERS



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



ELECTRIC



WATER



OIL & GAS



FOOD & BEV



MANUFACTURING



MINING



BLDG AUTO SYS



TRANSPORTATION



CHEMICAL



PHARMACEUTICAL



HQ | Hanover, MD



REGIONAL | Houston, TX

Including **7** of the **10** largest U.S. electric utilities and **5** of the **10** largest oil and gas companies

YOUR ALLY

- ✓ COMPREHENSIVE TECHNOLOGY
- ✓ UNIQUE THREAT INTELLIGENCE
- ✓ EXPERT-GUIDED SERVICES



THE DRAGOS PLATFORM

ICS/OT cybersecurity technology for comprehensive asset visibility, threat detection, and response



WORLDVIEW THREAT INTELLIGENCE

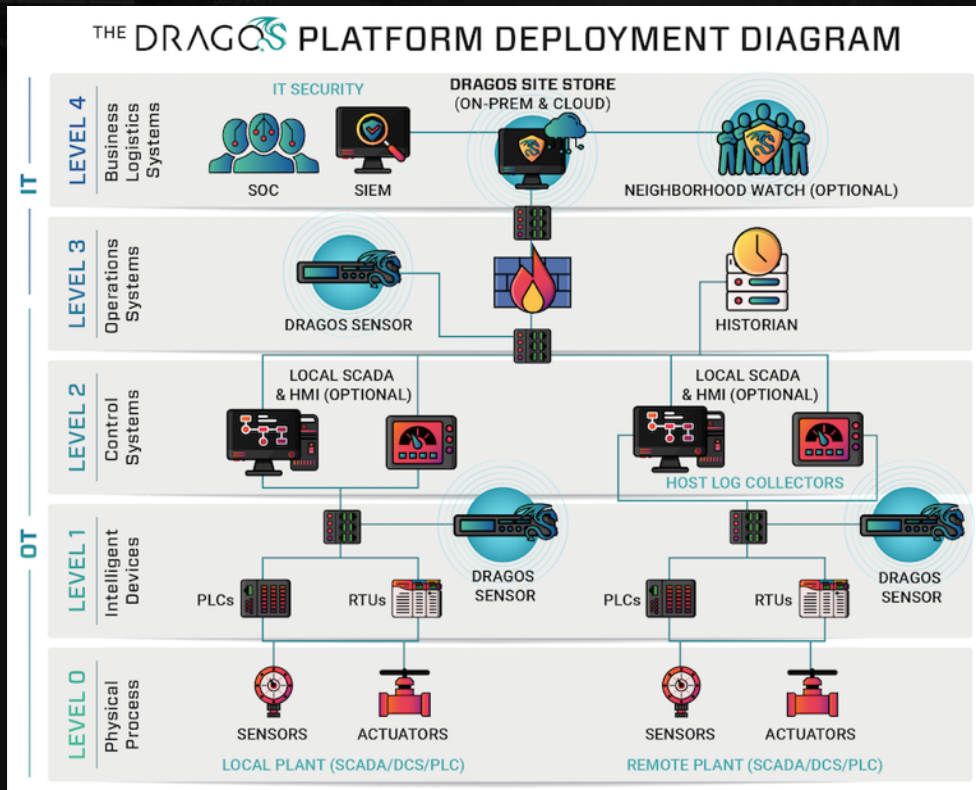
In-depth situational awareness of the threat landscape via actionable insights and intelligence reports



ICS/OT SECURITY SERVICES

Expert guidance to combat and respond to adversaries via incident response, proactive services, and training

DEPLOYMENT STRATEGY



Traffic Collection

Dragos Sensors are primarily deployed via network Span or Tap.

Logs and/or PCAPs

Utilize existing infrastructure; systems, devices, and tools.

API Integrations

Extend visibility and/or enrich data collected

COMMON CHALLENGES

ASSET VISIBILITY



WHAT WE HEAR:

- I need to know what's on my network?
- Do I have misconfigurations and security gaps?
- Are there rogue devices?
- When did changes take place?
- What is happening inside the control protocols?

HOW THE DRAGOS PLATFORM HELPS:

- Network visibility and asset identification
- Deep packet inspection covering a variety of protocols and vendors (e.g., EthernetIP/CIP, DNP3, OPC, ModbusTCP, BACNet, Honeywell, Yokogawa, Rockwell, GE, SEL, etc.)
- Timeline analysis

COMMON CHALLENGES THREAT DETECTION



WHAT WE HEAR:

- Am I under attack?
- How do I focus on the right things and not noise?
- What is the context of this event? (Why do I care?)
- What do I do about it?

HOW THE DRAGOS PLATFORM HELPS:

- Threat analytics mapped to MITRE ICS ATT&CK
- Pre-configured searches (data queries)
- Expert guided Playbooks



The PlantCo Story: XENOTIME ICS CYBER ATTACK

PlantCo Refinery



60,000 BPD Operating Capacity



Complex Processing (DCU, FCCU, HCU)



Sweet & Sour Crude Capable

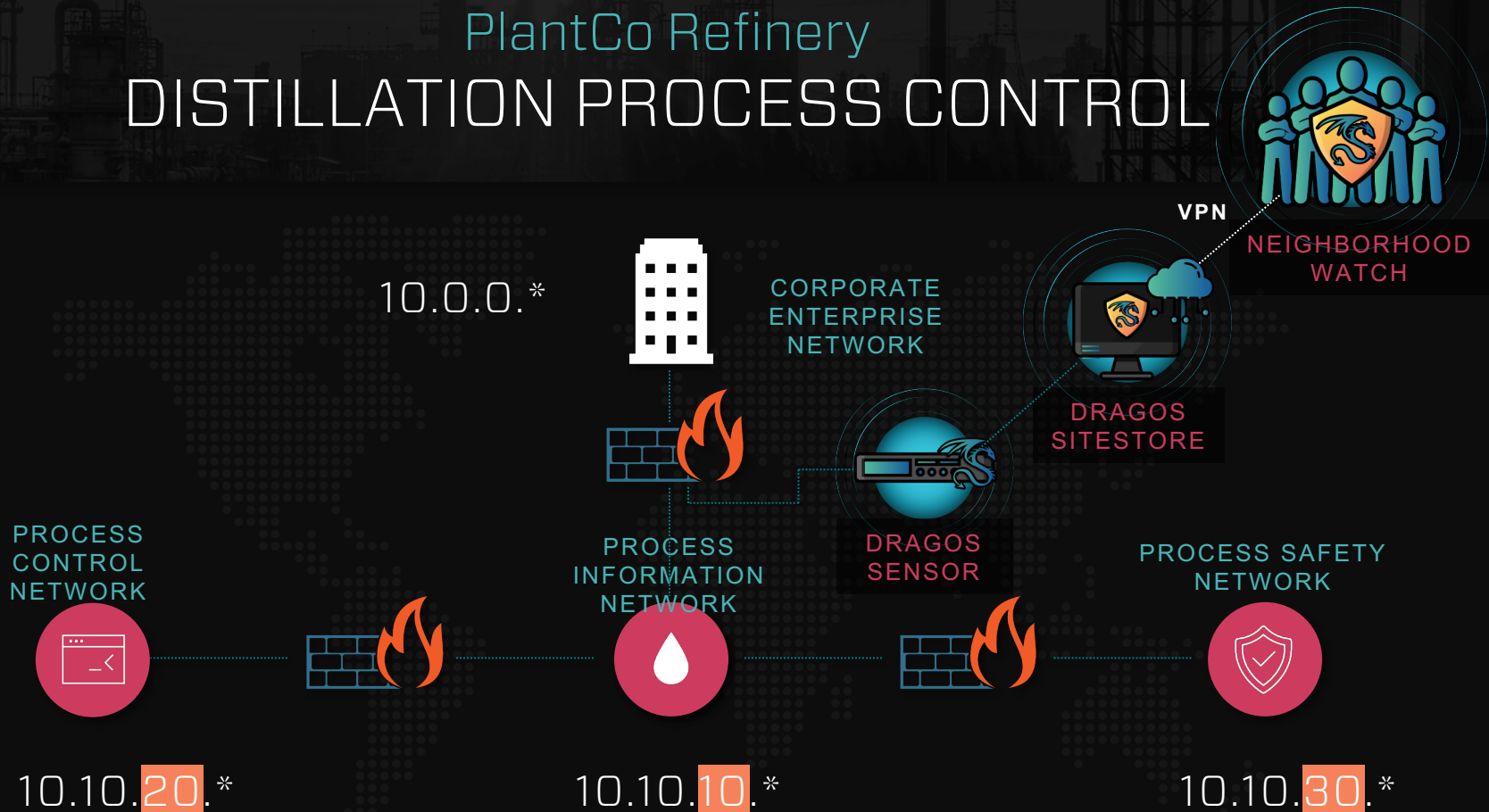


Produces finished fuel products



PlantCo Refinery

DISTILLATION PROCESS CONTROL



ATTACK SCENARIO

PlantCo Refinery



L4
CORPORATE
ENTERPRISE NETWORK



L3.5
PROCESS INFORMATION
NETWORK



L2/3
PROCESS CONTROL
AND SAFETY NETWORKS



L0/1
PROCESS CONTROL
LOGIC



THREAT PROLIFERATION

KNOWN ACTIVITY GROUPS TARGETING ONG

Six activity groups targeting ONG:

➤ **XENOTIME**

➤ **CHRYSENE**

➤ **MAGNALLIUM**

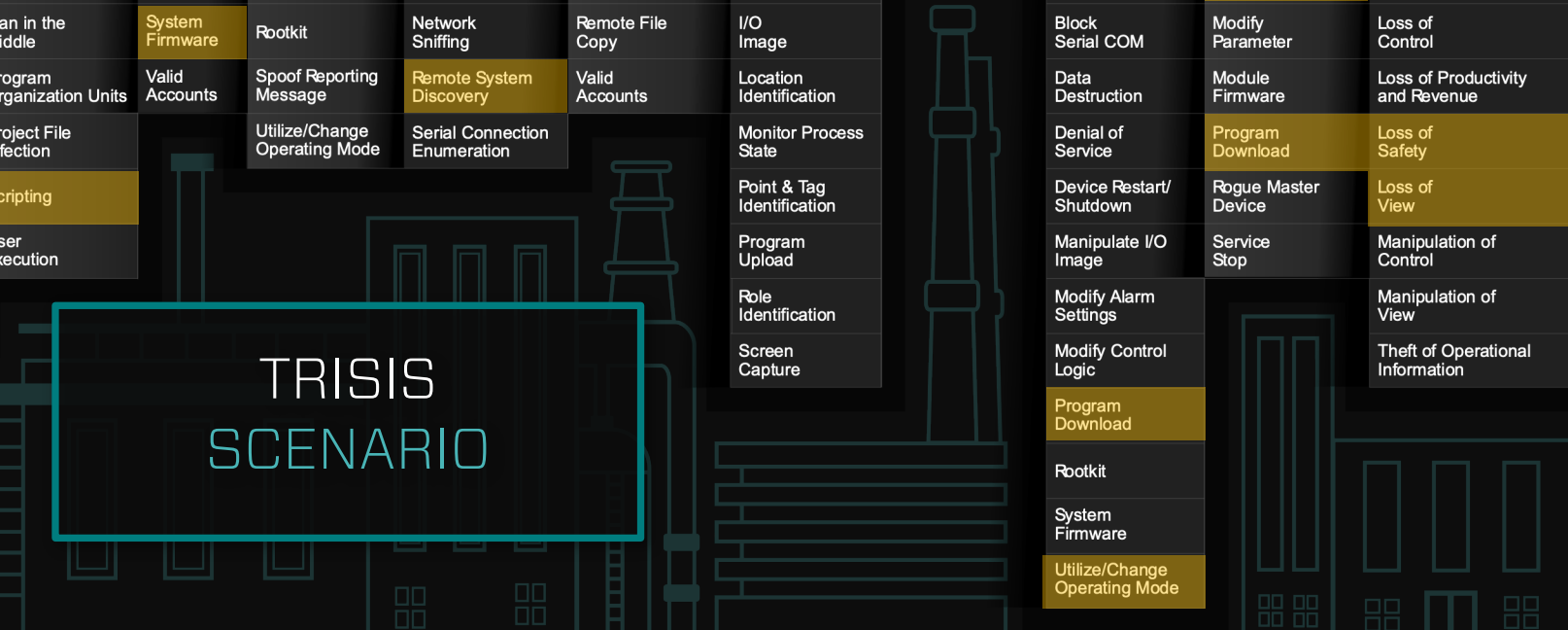
➤ **HEXANE**

➤ **PARISITE***

➤ **WASSONITE**

*New in 2019

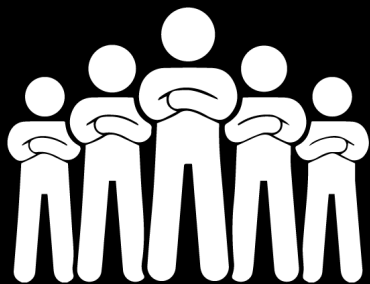


INITIAL ACCESS	EXECUTION	PERSISTENCE	EVASION	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND & CONTROL	INHIBIT RESPONSE FUNCTION	IMPAIR PROCESS CONTROL	IMPACT
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode		Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings		Manipulation of View
						Screen Capture		Modify Control Logic		Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

TRISIS SCENARIO

NEIGHBORHOOD WATCH

OUR TEAM IS YOUR TEAM



Industrial Hunters

EXPERT ICS SECURITY ANALYSTS

+



Platform

VISIBILITY + DETECTION + RESPONSE

Regular Asset Reporting

Receive curated reports of what exists in your environment so you can understand at a glance

Proactive Threat Hunting

Continuous threat hunting based on Dragos threat intelligence and Dragos adversary hunting expertise

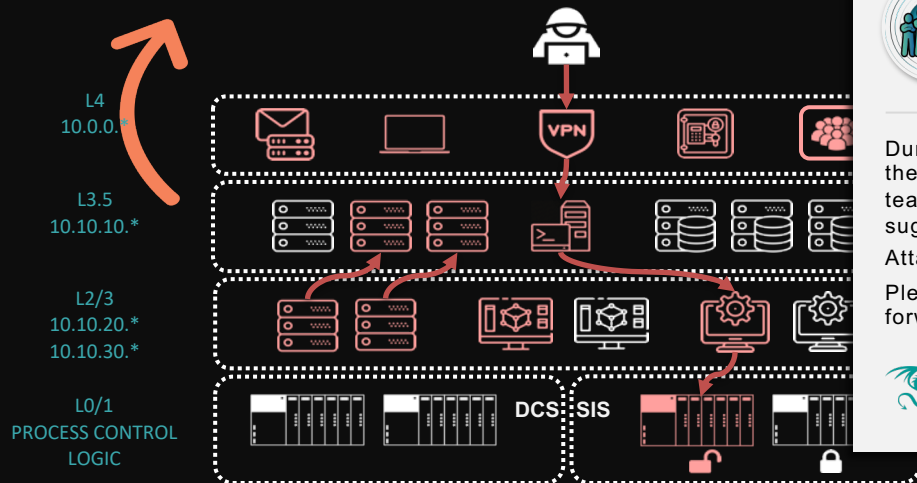
Critical Incident Support

Rapid support for severe threats with in-depth context and best-practice defensive recommendations

NEIGHBORHOOD WATCH

DRAGOS'S TEAM IS YOUR TEAM

1 | DETECTION OF SSH REVERSE TUNNELING



NEIGHBORHOOD WATCH

RFI – PlantCo Refinery – 20200920 SSH Reverse Tunneling detected
To: PlantCo Refinery

During the course of triaging the Severity 3 Detection: SSH Reverse Tunneling in the PlantCo Refinery instance of the Dragos Platform the Neighborhood Watch team developed some questions around the legitimacy of this network traffic and suggested next steps.

Attached is the RFI that was developed around this detection.

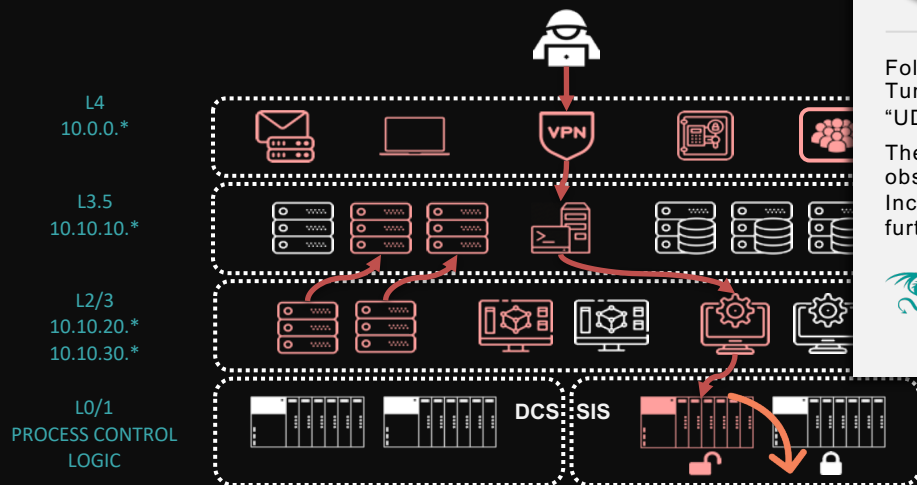
Please respond back to this RFI at your earliest convenience so we can move forward with triaging this detection.



Thank you,
Dragos Neighborhood Watch

NEIGHBORHOOD WATCH

DRAGOS'S TEAM IS YOUR TEAM



NEIGHBORHOOD WATCH

Immediate Action Required – Potentially Malicious Behavior
To: PlantCo Refinery

Following the earlier RFI regarding a Severity 4 Detection: "SSH Reverse Tunneling", the Neighborhood Watch team was alerted on a Severity 4 Detection: "UDP Broadcast Packet over Port 52 on 09/22/21 @ 07:02 UTC."

The Neighborhood Watch team recommends immediate action based on the observed behavior. The team has forwarded all related information to our Incident Response team in preparation and will wait for the decision to escalate further.



Thank you,
Dragos Neighborhood Watch

**2 | CONTROL DEVICE
IDENTIFICATION
DETECTED**

1

MS SQL Server OS Commands

1

Metasploit Bind Shell and Reverse Bind Shell

CONFIGURATION

...

8

New Source IP Address Detection

5

New Destination Ethernet Address Detection

5

New Source Ethernet Address Detection

4

New Destination IP Address Detection

1

New Tristation Device Detection

INDICATOR

...

136

Snort Community Rules

6

Nmap Signatures

4

Metasploit Login Detection

4

MS 17-010 Signatures

1

Dragos IOCs: TR-2019-33

Map

Assets

Data

Notifications

Content

Baselines

Reports

Sensors

21093

0

Detected 43 NewTristationCommunication between 2020-09-30T04:11:49.000Z and 2020-09-30T04:14:33.000Z

MARK AS READ

DETECTION INFORMATION

WHAT HAPPENED:

Sample NewTristationCommunication values include: src_asset_id: 1199, 1396, 1198, 1196, 1197; dst_asset_id: 1243, 1259, 1199, 1226, 1208, 1214, 1262, 1287, 1200, 19; tcm_type: COMMAND REPLY; tristation_dir: 1, 0; tristation_cid: 00; tristation_cmd: GetModuleVersions, UploadProgram, UploadFunction, HaltProgram, GetCPStatusResponse, GetSymbolTable, RunProgram, MPDiagnosticRequest, CancelDownloadChange; tristation_key_status: , PROGRAM; tristation_run_status: , HALT; tristation_cpstatus_version: , 0x00030004; tristation_cpstatus_downloadtime: , Jan 14, 2019 19:21:43.000000000 , Jan 14, 2019 19:21:31.000000000 , Jan 14, 2019 19:21:55.000000000 , Jan 14, 2019 19:22:32.000000000 , Jan 14, 2019 19:22:20.000000000 ; uuid: 733921cd-9b1a-4b07-bd18-f93dbb0ed171, 2cfccd9c-61ce-4c17-bde3-993422081f55, 6a087b73-9b7a-4b30-bb31-2321702721a9, d6258212-d867-4bad-8512-08f808269448, 4de3931a-682e-482f-83d2-b99499e4bb2c, 761bfd2b-6873-4b77-afab-dcb43bdabc07, 2d86c882-7c05-4f82-b175-0031fba6a665, 962f421b-fc20-4688-b08a-4be7c7d03a68, 85e6f8ff-be95-4ec7-84a7-c55454ee52b0, 5470505a-22da-476c-9cf5-f8b47f8811e8;

OCCURRED AT:

09/30/20, 04:14 AM UTC

DETECTED BY:

New Tristation Device Detection

SOURCE:

733921cd-9b1a-4b07-bd18-f93dbb0ed171, 2cfccd9c-61ce-4c17-bde3-993422081f55, 6a087b73-9b7a-4b30-bb31-2321702721a9, d6258212-d867-4bad-8512-08f808269448, 4de3931a-682e-482f-83d2-b99499e4bb2c, 761bfd2b-6873-4b77-afab-dcb43bdabc07, 2d86c882-7c05-4f82-b175-0031fba6a665, 962f421b-fc20-4688-b08a-4be7c7d03a68, 85e6f8ff-be95-4ec7-84a7-c55454ee52b0, 5470505a-22da-476c-9cf5-f8b47f8811e8

DETECTION QUAD:

Configuration

ZONES:

RFC1918

< PREV

CLOSE

CREATE A RULE

CREATE CASE

NEXT >

snort rule set not current rule bank

snort rule set not current rule bank (1) nnnnn

[< BACK TO PLAYBOOKS](#)[ADD TO CASE](#)

☆ New Tristation Communication

[Dragos TOC](#)[✎ EDIT](#)[📄 EXPORT](#)

New Tristation Communication

TRISTATION is a communication protocol that is leveraged for communications with Schneider Electric (SE) Safety Integrated Systems (SIS) controllers. The communications mostly originate between Engineering Workstations running the TRISTATION software and SE Tricon controllers, or between Tricon controllers for redundancy and data replication. Communication flows are generally static, in that associated hosts do not change frequently. Any new communications observed leveraging the protocol should be investigated for validity and authenticity.

TASKS

1

Check for Tristation Broadcast

Prior to the initiation of the program upload, the malicious program triggers a broadcast to poll for controller information. This command is used to enumerate devices that the payload will be able to impact after the code is injected. An abnormal spike in broadcast connections, broadcasts outside of the cyclical pattern, or broadcasts outside of normal maintenance windows should be analyzed for historical variability.

1 QFDS

Tristation

Shows unique Tristation communications in the environment

2

Analyze for Controller Keystates

Controllers are required to be in specific keystates in order to receive commands or programs. "Program" states allow controller reconfiguration while "Run" states execute the uploaded code. Changing of keystates prior to the upload can be an indication of threat behavior but can also correlate to maintenance activities. Record the keystate changes to confirm the logs present in the Tristation EWS software with operators.



QFD Details



admin



Map



Assets



Data



Notifications



Content



Baselines



Reports



Sensors



< BACK

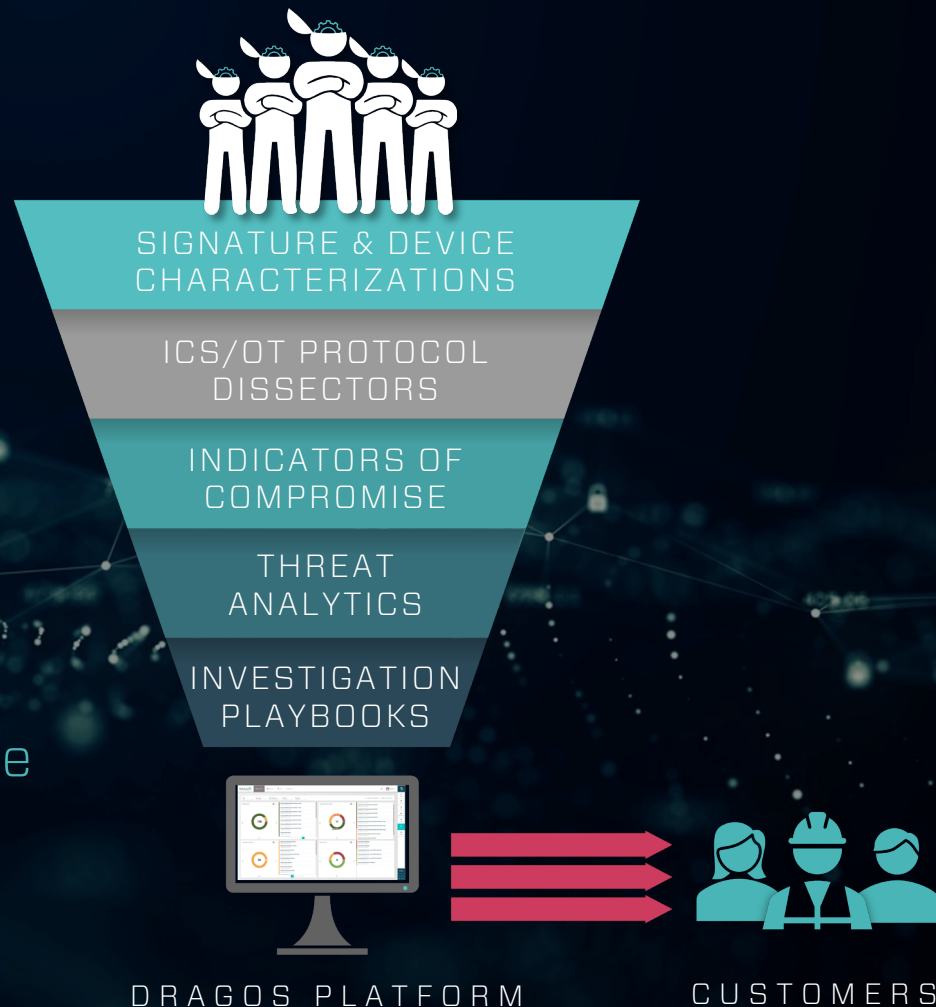
REPLY

▶	September 30th 2020, 04:14:33.000	1196	1199	COMMAND REPLY	00	MPDiagnosticRequest	0			
▶	September 30th 2020, 04:14:33.000	1196	1199	COMMAND REPLY	00	UploadFunction	0			
▶	September 30th 2020, 04:14:33.000	1196	1200	COMMAND REPLY	00	HaltProgram	0			
▶	September 30th 2020, 04:14:33.000	1196	1200	COMMAND REPLY	00	MPDiagnosticRequest	0			
▶	September 30th 2020, 04:14:33.000	1196	1200	CONNECT REQUEST						
▶	September 30th 2020, 04:14:33.000	1197	1196	COMMAND REPLY	00	GetCPStatusResponse	1	PROGRAM	HALT	0x00030004
▶	September 30th 2020, 04:14:33.000	1197	1196	COMMAND REPLY	00	GetCPStatusResponse	1	PROGRAM	HALT	0x00030004
▶	September 30th 2020, 04:14:33.000	1198	1196	COMMAND REPLY	00	GetCPStatusResponse	1	PROGRAM	HALT	0x00030004
▶	September 30th 2020, 04:14:33.000	1198	1196	COMMAND REPLY	00	GetCPStatusResponse	1	PROGRAM	HALT	0x00030004
▶	September 30th 2020, 04:14:33.000	1198	1196	CONNECT REPLY						
▶	September 30th 2020, 04:14:33.000	1199	1196	COMMAND REPLY	00	GetCPStatusResponse	1	PROGRAM	HALT	0x00030004
▶	September 30th 2020, 04:11:49.000	1196	1207	CONNECT REQUEST						

DRAGOS KNOWLEDGE PACKS

Keeping you one step
ahead of adversaries

Monthly updates of industrial
adversarial information and device
data, plus the latest expert
prescriptive guidance to investigate
and respond to threats



Getting Started

- Where do I start?
- What is my timeline?

Where Do I Start?

- Understand your business
- Start with a vision
 - Mission Statement
 - Follow through with the strategy

Strategy Roadmap follows Vision

ICS Security Roadmap - Year 1

PRACTICAL STEPS TO EFFECTIVE ICS SECURITY



Thank you!

More amazing content and
resources:

<https://www.dragos.com/resources/>

sam@dragos.com

[linkedin.com/in/svanryder](https://www.linkedin.com/in/svanryder)

