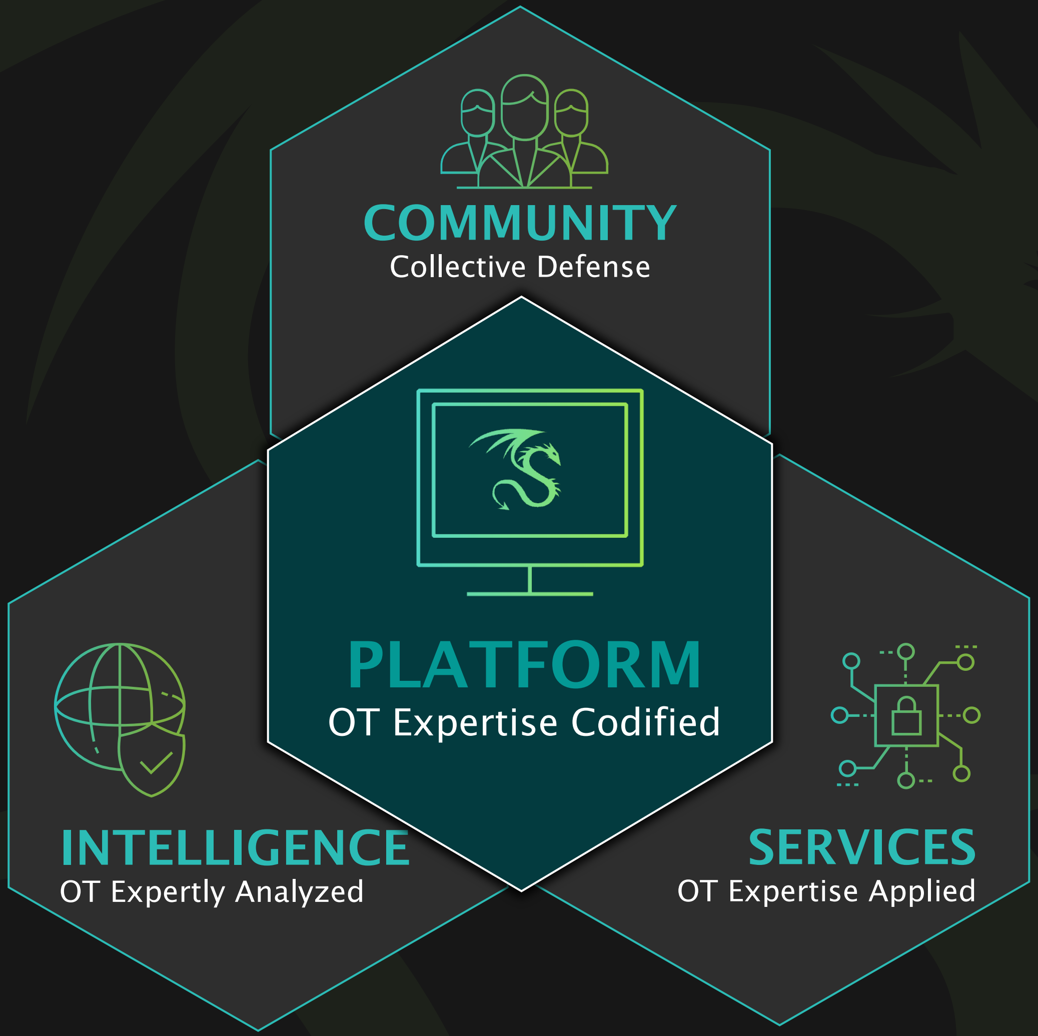
DRAGOS

Dragos Platform

Improving OT Threat Visibility on CHERNOVITE's PIPEDREAM

Sam Wilson
Kimberly Graham
John Burns



COMMUNITY
Collective Defense

PLATFORM
OT Expertise Codified

INTELLIGENCE
OT Expertly Analyzed

SERVICES
OT Expertise Applied

DRAGOS

Safeguarding Civilization

The Most Effective OT Security Tech Platform
The speed, scale, & codified expertise to reduce your OT risk.

Expert OT Intelligence & Service resources
Help to build & maintain an effective OT security program.

A Community-Focused Mission
Building relationships between operators & practitioners.

CHERNOVITE PIPEDREAM SUMMARY

PIPEDREAM is identified in early 2022 before it was employed.

▼

Dragos begins analysis of PIPEDREAM's modular capabilities.

▼

WorldView Threat Intel customers receive several advisories.

▼

Knowledge Packs tested & released to Dragos Platform customers.

▼

WorldView customers receive further detailed technical guidance.

CHERNOVITE
Unique Tool Development

ICS IMPACT
Loss of Safety,
Availability,
and Control;
Manipulation
of Control

ICS Kill Chain Stage 2
Develop;
Install/Modify;
Execute ICS Attack

Impacted Technology

Schneider Electric OMRON

ICS protocols used in 100s of devices:
CODESYS, Schneider Discovery (NetManage),
Modbus, Omron FINS, OPC-UA

PIPEDREAM Modules

EVILSCHOLAR
Designed to discover, access, manipulate, and disable Schneider Electric PLCs. Can target other PLCs via the CODESYS library.

BADOMEN
Designed to scan, identify, and interact with Omron software and PLCs.

MOUSEHOLE
Tool to interact with OPC-UA servers. Designed to read/write, enumerate, and brute force credentials.

DUSTTUNNEL
Remote operational implant to perform host reconnaissance and command-and-control.

LAZYCARGO
User-mode Windows executable that drops and exploits a vulnerable ASRock driver.

dragos.com/pipedream

Dragos Platform Overview

Kimberly Graham
Director Product Management

PLATFORM USE CASES

COMPREHENSIVE ICS/OT CYBER TECHNOLOGY

ASSET VISIBILITY

- Identify crown jewel assets to protect
- Create asset inventory & zone maps
- See unauthorized IT-OT traffic

VULNERABILITY MANAGEMENT

- Simplify fulfillment regulatory requirements
- Identify highest priority vulnerabilities
- Maximize scarce remediation resources

THREAT DETECTION

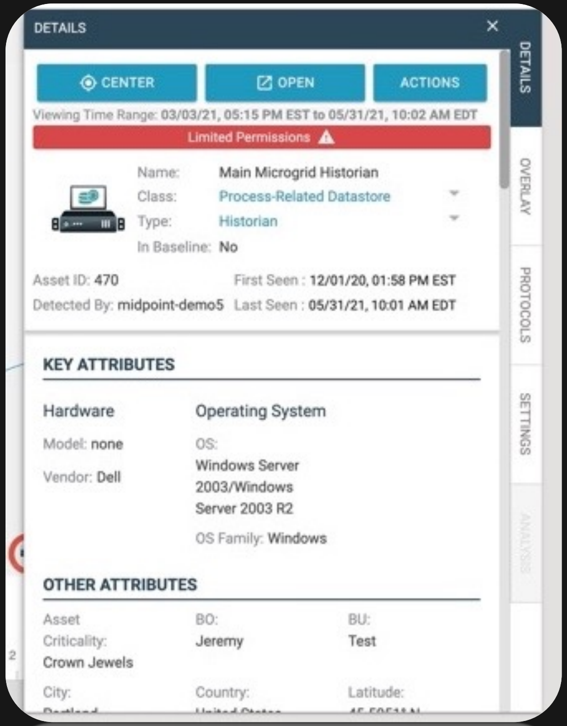
- Evaluate unusual changes & commands
- See malicious file transfers
- Spot adversary activity

INCIDENT RESPONSE

- Organize analyst case assignments
- Efficiently manage response and recovery
- Equip defenders with prescriptive playbooks

ASSET VISIBILITY

A comprehensive inventory is essential for any monitoring, threat correlation and effective vulnerability management



Viewing Time Range: 03/03/21, 05:15 PM EST to 05/31/21, 10:02 AM EDT

Limited Permissions ⚠

Name: Main Microgrid Historian
Class: Process-Related Datastore
Type: Historian
In Baseline: No

Asset ID: 470
First Seen : 12/01/20, 01:58 PM EST
Detected By: midpoint-demo5
Last Seen : 05/31/21, 10:01 AM EDT

KEY ATTRIBUTES

Hardware
Model: none
Vendor: Dell

Operating System
OS: Windows Server 2003/Windows Server 2003 R2
OS Family: Windows

OTHER ATTRIBUTES

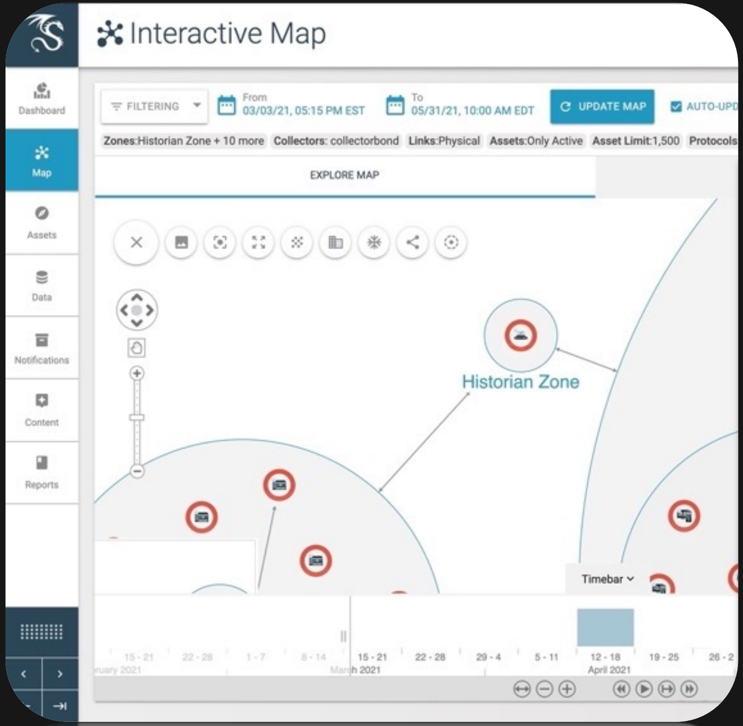
Asset Criticality: Crown Jewels
BO: Jeremy
BU: Test
City:
Country:
Latitude:

Build asset inventory depth through “operations safe” passive collection and device level detail

- Establish asset profile baselines for connected integrations with firewall and CMDB systems
- Group assets in a visual map with customizable zones for easier cyber-ops management
- See historical changes with timeline views to spot unexpected activity

ICS PROTOCOL & TRAFFIC ANALYSIS

Proper traffic dissection and inspection requires in depth protocol coverage – assets and threats remain hidden until their communications are exposed


From 03/03/21, 05:15 PM EST

To 05/31/21, 10:00 AM EDT

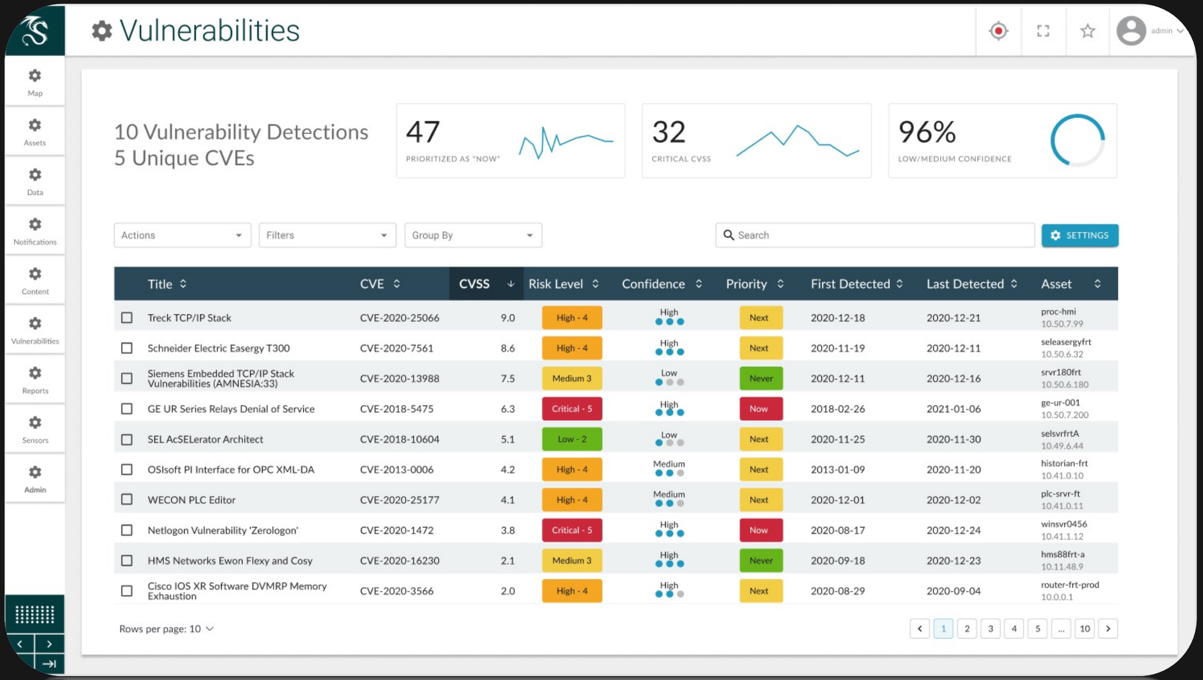
Zones:Historian Zone + 10 more Collectors: collectorbond Links:Physical Assets:Only Active Asset Limit:1,500 Protocols

Improve the accuracy and understanding of devices in your environment

- Full support across most industrial vendors, equipment, and protocols
- Capture, analyze, and investigate device communications
- Monitor for remote connections, search historical activity

VULNERABILITY MANAGEMENT

OT cyber teams face impossible numbers of potential vulnerabilities to remediate – without simple, accurate, prioritized guidance they become overwhelmed



10 Vulnerability Detections
5 Unique CVEs

47 PRIORITIZED AS "NOW"

32 CRITICAL CVSS

96% LOW/MEDIUM CONFIDENCE

	Title	CVE	CVSS	Risk Level	Confidence	Priority	First Detected	Last Detected	Asset
□	Treck TCP/IP Stack	CVE-2020-25066	9.0	High - 4	High	Next	2020-12-18	2020-12-21	proc-hmi 10.50.7.99
□	Schneider Electric Easergy T300	CVE-2020-7561	8.6	High - 4	High	Next	2020-11-19	2020-12-11	seleasergyfrt 10.50.6.32
□	Siemens Embedded TCP/IP Stack Vulnerabilities (AMNESIA:33)	CVE-2020-13988	7.5	Medium 3	Low	Never	2020-12-11	2020-12-16	srvr180frt 10.50.6.180
□	GE UR Series Relays Denial of Service	CVE-2018-5475	6.3	Critical - 5	High	Now	2018-02-26	2021-01-06	ge-ur-001 10.50.7.200
□	SEL AcSELerator Architect	CVE-2018-10604	5.1	Low - 2	Low	Next	2020-11-25	2020-11-30	selsvrfrtA 10.49.6.44
□	OSIsoft PI Interface for OPC XML-DA	CVE-2013-0006	4.2	High - 4	Medium	Next	2013-01-09	2020-11-20	historian-frt 10.41.0.10
□	WECON PLC Editor	CVE-2020-25177	4.1	High - 4	Medium	Next	2020-12-01	2020-12-02	plc-srvr-ft 10.41.0.11
□	Netlogon Vulnerability 'Zerologon'	CVE-2020-1472	3.8	Critical - 5	High	Now	2020-08-17	2020-12-24	winsvr0456 10.41.1.12
□	HMS Networks Ewon Flexy and Cosy	CVE-2020-16230	2.1	Medium 3	High	Never	2020-09-18	2020-12-23	hms88frt-a 10.11.48.9
□	Cisco IOS XR Software DVMRP Memory Exhaustion	CVE-2020-3566	2.0	High - 4	High	Next	2020-08-29	2020-09-04	router-frt-prod 10.0.0.1

Rows per page: 10

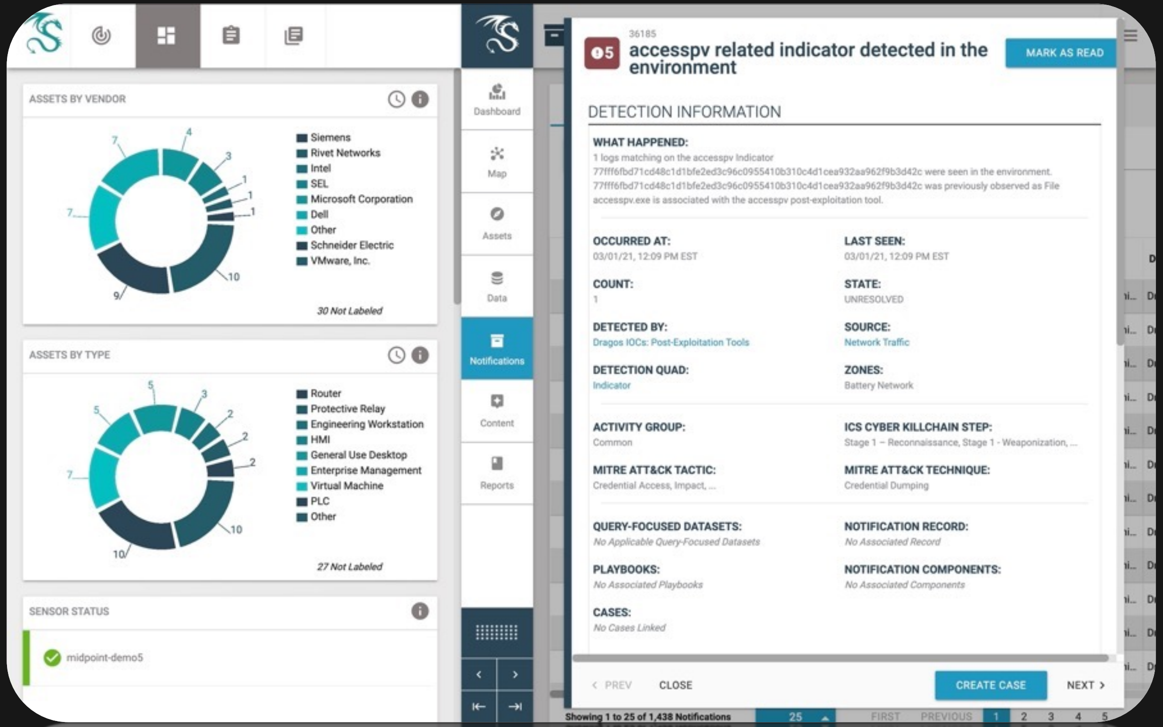
‹ 1 2 3 4 5 ... 10 ›

Practical OT vulnerability intelligence and mitigation strategies

- Industry specific analysis, correction, and enrichment of known vulns
- Alternative mitigation advice, prioritized with “*Now, Next, Never*” guidance
- Disposition tracking for full lifecycle management and to simplify audits

THREAT DETECTION

Adversaries evolve their Tactics, Techniques, and Procedures (TTPs) with subtle behaviors lost in the noise without AI (Actual Intelligence) – creating alert fatigue



36185

5 accesspv related indicator detected in the environment

DETECTION INFORMATION

WHAT HAPPENED:
1 logs matching on the accesspv Indicator 77fff6fbd71cd48c1d1bfe2ed3c96c0955410b310c4d1cea932aa962f9b3d42c were seen in the environment. 77fff6fbd71cd48c1d1bfe2ed3c96c0955410b310c4d1cea932aa962f9b3d42c was previously observed as File accesspv.exe is associated with the accesspv post-exploitation tool.

OCCURRED AT: 03/01/21, 12:09 PM EST

LAST SEEN: 03/01/21, 12:09 PM EST

COUNT: 1

STATE: UNRESOLVED

DETECTED BY: Dragos IOCs: Post-Exploitation Tools

SOURCE: Network Traffic

DETECTION QUAD: Indicator

ZONES: Battery Network

ACTIVITY GROUP: Common

ICS CYBER KILLCHAIN STEP: Stage 1 – Reconnaissance, Stage 1 - Weaponization, ...

MITRE ATT&CK TACTIC: Credential Access, Impact, ...

MITRE ATT&CK TECHNIQUE: Credential Dumping

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

NOTIFICATION RECORD: *No Associated Record*

PLAYBOOKS: *No Associated Playbooks*

NOTIFICATION COMPONENTS: *No Associated Components*

CASES: *No Cases Linked*

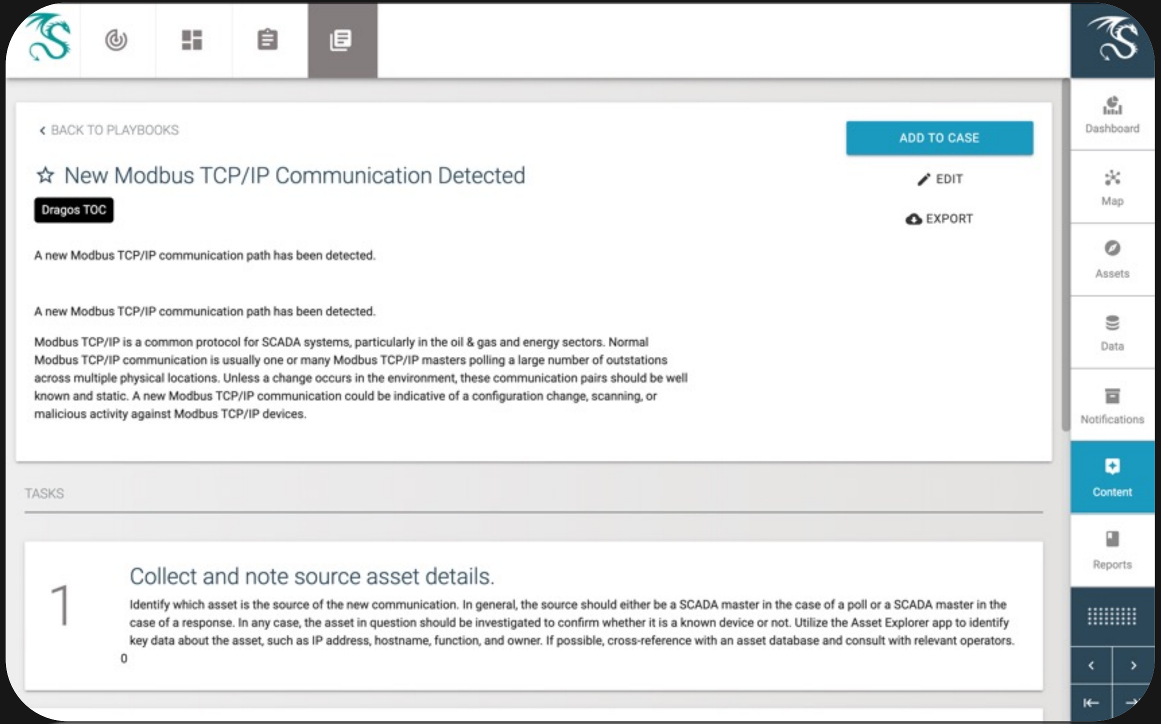
Showing 1 to 25 of 1,438 Notifications 25

High signal, low noise intelligence-based detections mapped against MITRE ATT&CK for ICS :

- Curated Indicators of Compromise (IOCs), malicious IPs, domains, and hashes from Dragos Intelligence
- Anomalous traffic patterns and baseline deviation alerts
- Composite detections from TTP analysis of threat groups and attacks

RESPONSE

When faced with a potential incident, clear and carefully vetted guidance can mean the difference between quickly restoring operations or making the situation worse



☆ New Modbus TCP/IP Communication Detected

A new Modbus TCP/IP communication path has been detected.

A new Modbus TCP/IP communication path has been detected.

Modbus TCP/IP is a common protocol for SCADA systems, particularly in the oil & gas and energy sectors. Normal Modbus TCP/IP communication is usually one or many Modbus TCP/IP masters polling a large number of outstations across multiple physical locations. Unless a change occurs in the environment, these communication pairs should be well known and static. A new Modbus TCP/IP communication could be indicative of a configuration change, scanning, or malicious activity against Modbus TCP/IP devices.

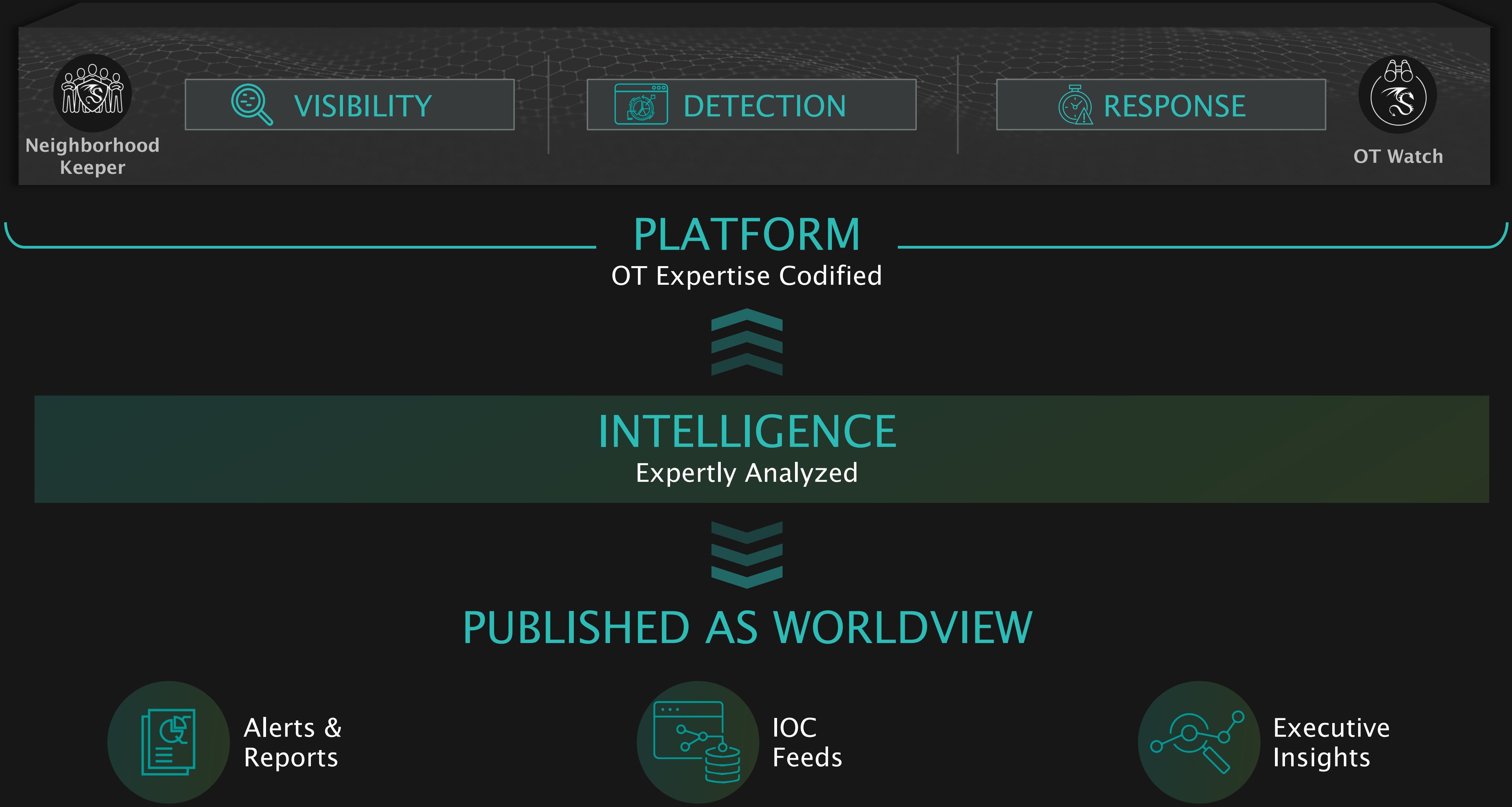
1 Collect and note source asset details.

Identify which asset is the source of the new communication. In general, the source should either be a SCADA master in the case of a poll or a SCADA master in the case of a response. In any case, the asset in question should be investigated to confirm whether it is a known device or not. Utilize the Asset Explorer app to identify key data about the asset, such as IP address, hostname, function, and owner. If possible, cross-reference with an asset database and consult with relevant operators.

0

Provide responders with the tools to triage and investigate potential incidents

- Incident response playbooks with OT-centric guidance from industry experts
- Collect evidence and organize by case in the analyst investigation workbench
- Centralized forensics and timeline views to coordinate across OT and IT teams



Neighborhood Keeper

VISIBILITY

DETECTION

RESPONSE

OT Watch

PLATFORM

OT Expertise Codified

INTELLIGENCE

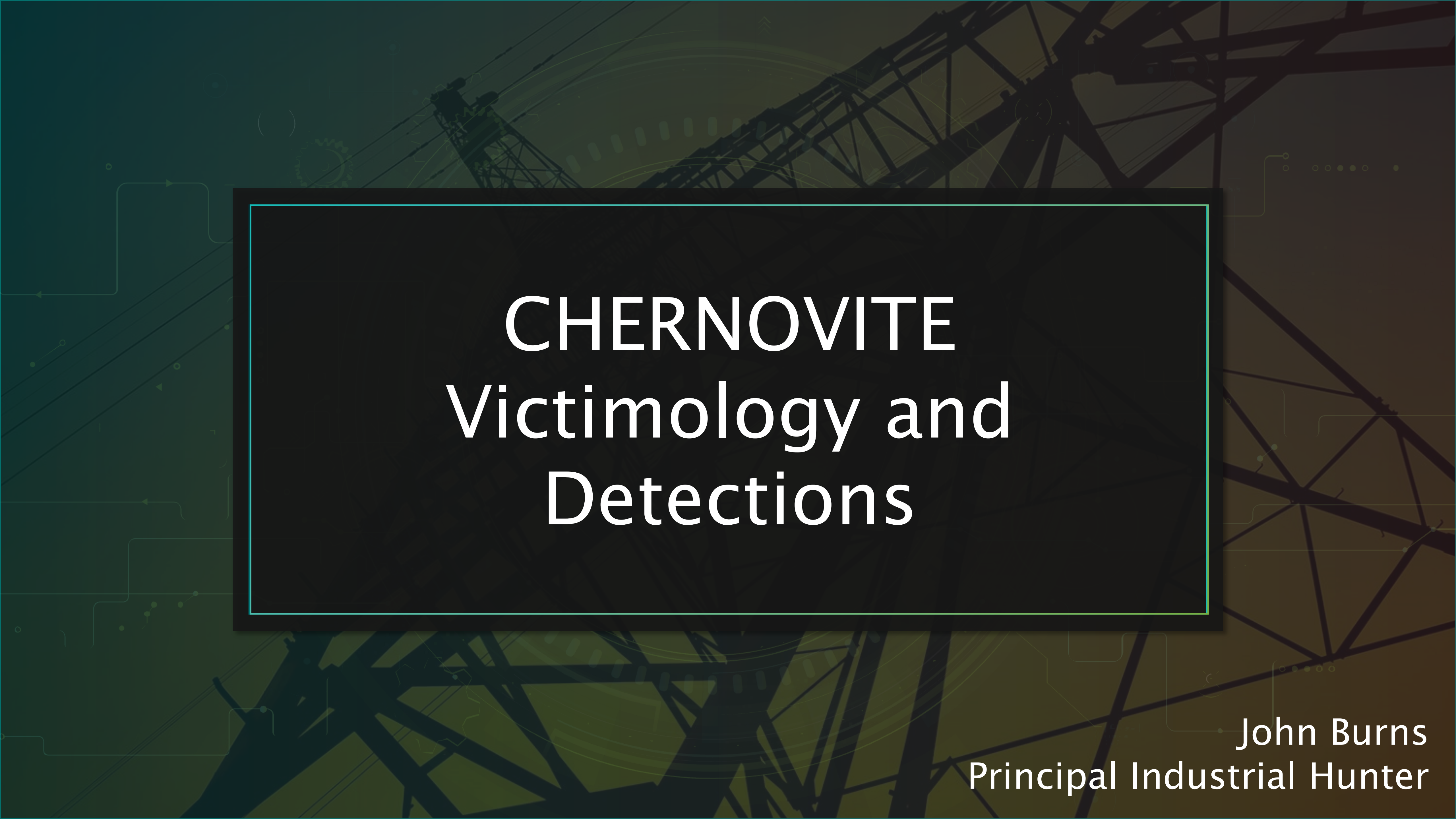
Expertly Analyzed

PUBLISHED AS WORLDVIEW

Alerts & Reports

IOC Feeds

Executive Insights



CHERNOVITE Victimology and Detections

John Burns
Principal Industrial Hunter

CHERNOVITE VICTIMOLOGY

Victim Personas:

Dragos assesses with moderate confidence that CHERNOVITE victimology is likely North American and European ONG, LNG, and Electric.

Victim Assets:

Omron PLCs including:

- NX1P2
- NX-ECC
- NX-EIC202
- NX-SL3300
- NX-ECC203
- NJ501-1300
- S8VK
- R88D-1SN10F-ECT

Schneider Electric PLCs including:

- TM251
- TM241
- TM221
- TM258
- TM238
- LMC058
- LMC078

Omron PLC Control Software including:

- CX-One
- CX-Supervisor
- NX-IO Configurator

Vulnerabilities, Exposures, and Susceptibilities

- CVE-2020-15368
- CVE-2018-7823
- Undisclosed vulnerabilities in Schneider Electric and Omron devices

CHERNOVITE DETECTIONS

Detection Group	Detection Summary
General	Network Transfer of Compiled Python
	Host Download of Compiled Python
	Network Transfer of Uncompiled Python
	Execution of Compiled Python .exe
	Execution of Python Script
DUSTTUNNEL	C2 Backdoor via SSL
	Interrogate Windows System via WMI
OMRON PLC	OMRON PLC CoESDO Read
	HTTP POST ENCRYPTED (XOR or Base64)
	Telnet Access via Hardcoded Username and Password
	HTTP Access via Hardcoded Username
	Get PLC Status
	Activate Telnet
	File Upload
SCHNEIDER ELECTRIC	Password Brute Force
	Denial of Service
	PLC Initial Communication
ASROCK DRIVER	Network File Transfer
	Host File Download
OPC UA	Initial Device Connectivity
	OPC UA protocol over non-standard port
	Composite: Create Connection, Login Attempt, OPC UA Enumeration
	Degrade Server

Dragos Platform CHERNOVITE Demo

John Burns
Principal Industrial Hunter

MITIGATION RECOMMENDATIONS

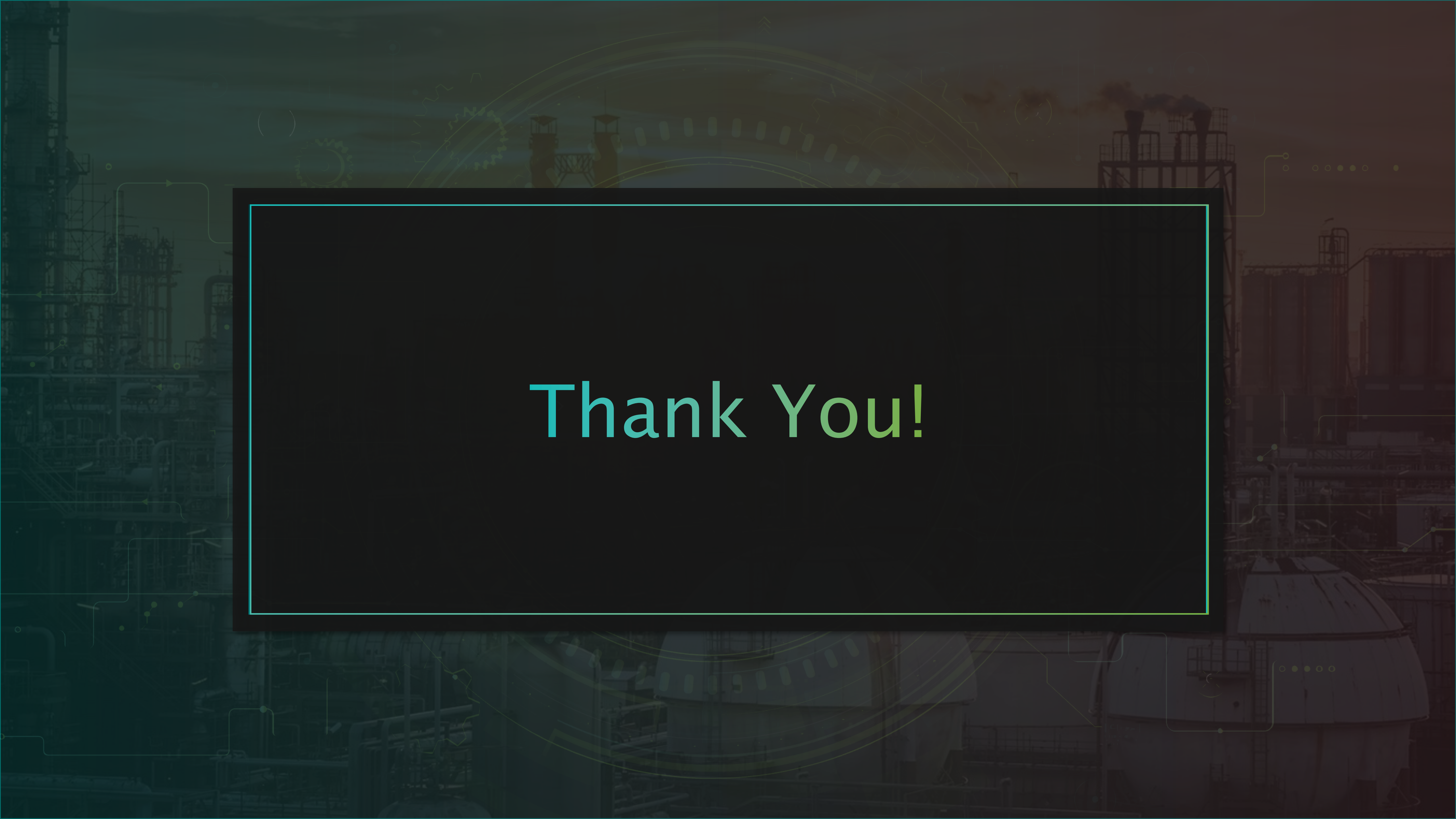
- Monitor industrial environments for all threat behaviors in the MITRE ATT&CK for ICS matrix
- Ensure ICS visibility and threat detection include all ICS North-South and East-West communications
- Maintain knowledge and control of all assets within Operational Technology (OT) environments
- Utilize a fully researched and rehearsed industrial incident response plan

Q&A

QUESTIONS AND ANSWERS

To learn more:

- dragos.com/request-a-demo/
- contact: sales@dragos.com
- dragos.com/pipedream



Thank You!