DRAGOS

How The Dragos Platform's Asset Inventory Fuels Detection and Response

Dillon Lee, Principal Technical Account Manager
Gregory Pollmann, Principal Industrial Threat Hunter
Mary Korus, Product Marketing Manager

Agenda

1. Building an Operational Asset Inventory
2. Prioritizing Vulnerabilities in OT Environments
3. From Intel to Defense Case Study
4. The Power of Proactive Threat Hunting
5. Live Question and Answer

Today's Industrial Systems

Operational Technology (OT)

Massive scale systems built with OT & IOT assets with 100s of specialized system protocols

Connected

Modernization, digital transformation, remote & 3rd party access

Automated

Common software across systems widens target list for given attack method

Threats to OT & Industrial Systems

Unmanaged Risk

Unknown assets, connections, and vulnerabilities

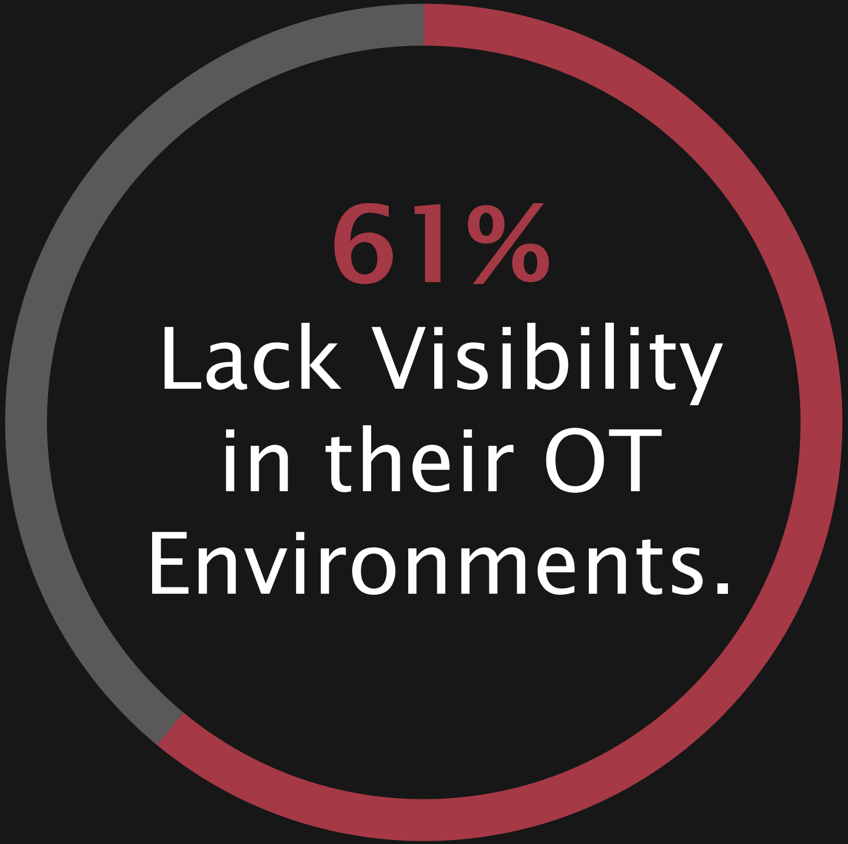
Blind Operations

Inability to identify and troubleshoot operational issues that can lead to outages

Ransomware & Adversary Activity

21 threat groups, 9 malware toolsets, plus active ransomware gangs targeting industrial systems

Building an Asset Inventory is Challenging



61%

Lack Visibility in their OT Environments.

*YIR 2023, Dragos Services Customers

Building an Asset Inventory

1 **Getting the Data:** Sourcing the data to get an accurate asset Inventory without impacting availability

2 **Lacking Standardization:** Inconsistent asset attributes across different vendors, asset types, and inputs

3 **Lacking OT Context:** Inadequate threat and vulnerability context linked to assets for effective decision-making

With Standardization and context, you can ask **questions** of that data:

How many assets are we monitoring at my site?

What are our crown jewels?

How are these assets critical to the operation?

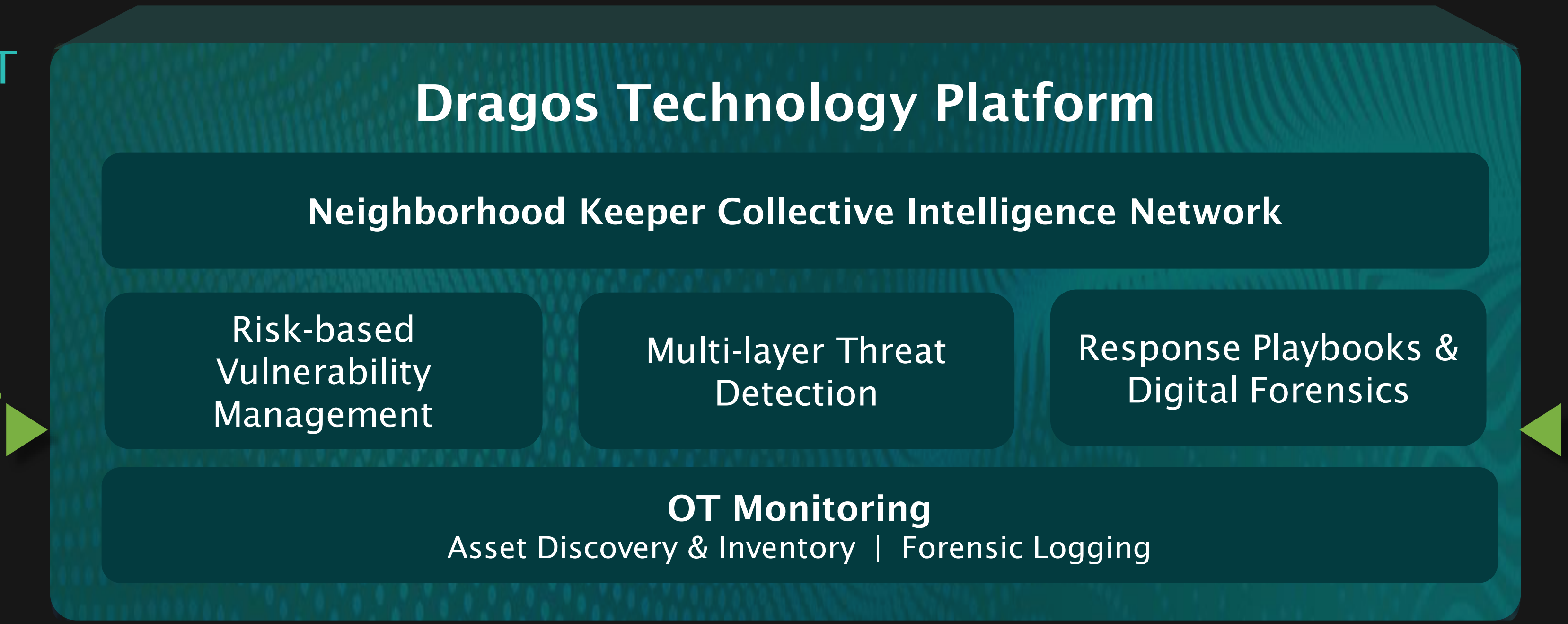
What assets exposed to vulnerabilities?

The Dragos Ecosystem

OT CYBER THREAT INTELLIGENCE

Intelligence Reports,
RFI’s, & Concierge
Analysts

Platform Analytics
Threats &
Vulnerabilities



Dragos Technology Platform

Neighborhood Keeper Collective Intelligence Network

Risk-based Vulnerability Management

Multi-layer Threat Detection

Response Playbooks & Digital Forensics

OT Monitoring
Asset Discovery & Inventory | Forensic Logging

OT CYBER SERVICES

Proactive Assessments,
Threat Hunting,
& Incident Response

Expertise
Help Customers Build
Their OT Defense

How It Works

Level 3

Level 2

Level 1

Collect Data in Levels 1-3 of Purdue Model

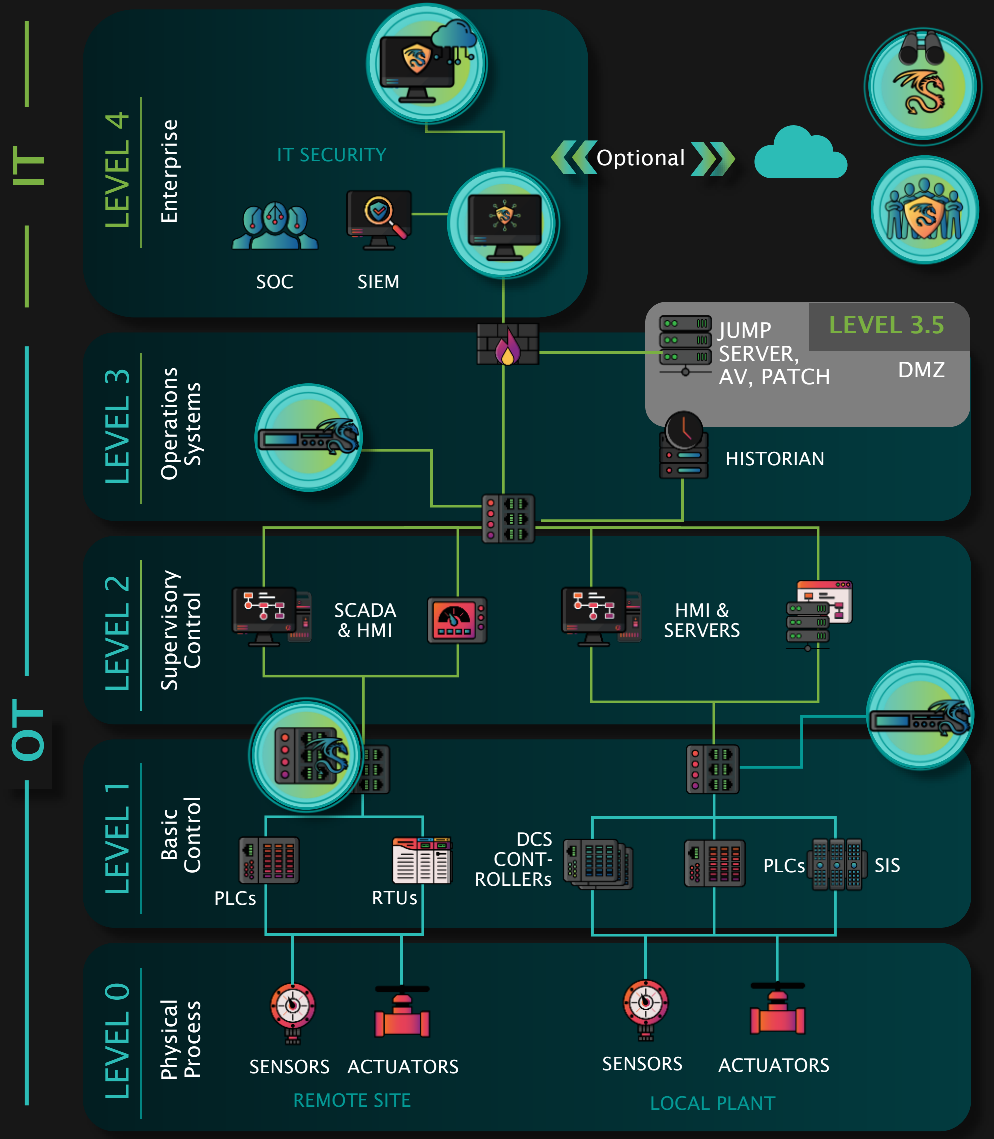
- Dragos network sensors, edge collector, & file ingest
- Analyze North-South & East-West traffic
- Passive-first approach

Monitor Your Environment via SiteStore

- Asset inventories & profiles
- “Now, next, never” prioritized vulnerability lists
- High fidelity threat detections with playbook-based investigation tools

Integrate into Security Processes

- Alerts flow into SIEM & SOC Tools
- Integrate asset groups with firewalls for policy, detections for action
- Vulnerabilities flow into service management tickets



DRAGOS

DEMO

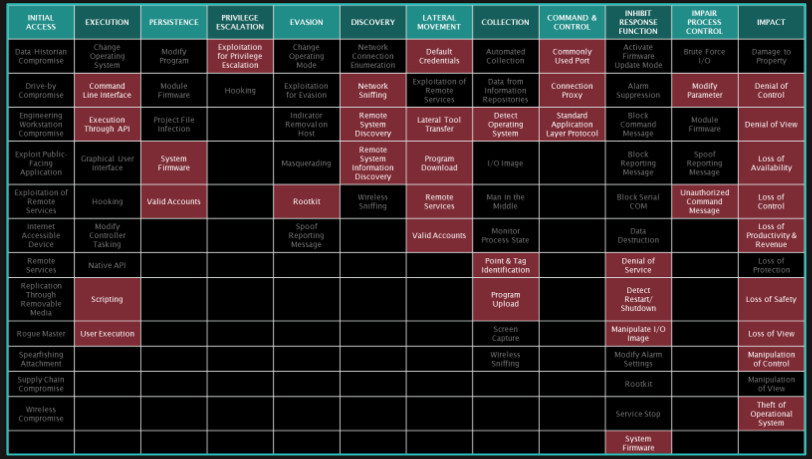
Operational Asset Inventory

Operationalize Threat Intelligence

TRANSFORM THREAT INTEL INTO DETECTIONS

UNDERSTAND THE THREAT

BEHAVIOR, CAPABILITIES, INFRASTRUCTURE, INTENT



INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	EVASION	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND & CONTROL	INHIBIT RESPONSE FUNCTION	IMPAIR PROCESS CONTROL	IMPACT
Data Historian Compromise	Change Operating System	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 System	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
Internet Accessible Device	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity & Revenue
Remote Services	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Replication Through Removable Media	Scripting						Program Upload		Detect Restart/ Shutdown		Loss of Safety
Rogue Master	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Spearfishing Attachment							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Supply Chain Compromise									Rootkit		Manipulation of View
Wireless Compromise									Service Stop		Theft of Operational System
									System Firmware		

DATA SOURCES: DRAGOS THREAT INTELLIGENCE, OSINT RESEARCH, THIRD-PARTY THREAT INTELLIGENCE

OPERATIONAL CONSTRAINTS

PIVOT AGAINST BEHAVIORS & OPERATE WITHIN PLATFORM CAPABILITIES

Type

Indicator
Configuration
Modeling
Threat Behavior

Complexity

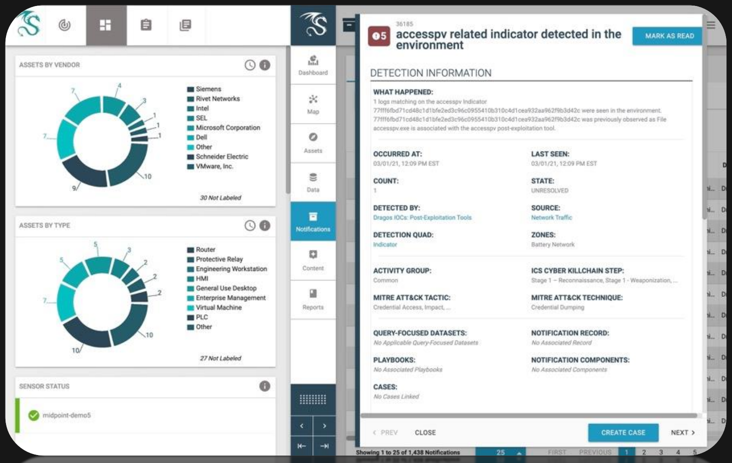
Atomic
Composite

Telemetry

Network Monitoring
Host Logs

DETECTIONS ARE CODIFIED IN THE DRAGOS PLATFORM

KNOWLEDGE PACKS RELEASED REGULARLY WITH NEW THREAT INTELLIGENCE-DRIVEN DETECTIONS



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

NEIGHBORHOOD KEEPER

Free anonymous collective intelligence data network

- Automate KnowledgePack updates – vulns, detections, dashboards, & more
- Receive notifications of emergent vulnerabilities & threats
- Access community wide threat data

OT WATCH

OT cyber threat hunting service by Dragos experts

- Continuous hunting with critical escalations & support during IR
- Alerts on misconfigurations that impact operations efficiency
- Quarterly insights and weekly status reports

FROSTYGOOP ICS MALWARE

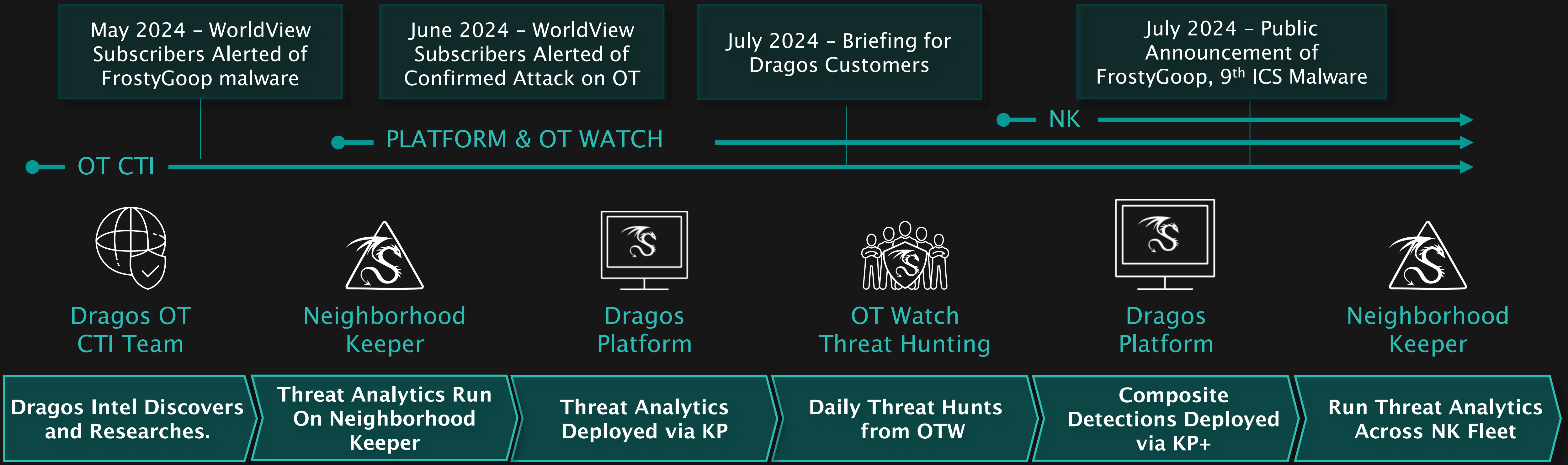
9th
known ICS malware

Dragos discovered FrostyGoop binaries in April 2024.

1st
Modbus ICS malware that causes effects on ICS devices

FrostyGoop interacts directly with industrial control systems (ICS) using Modbus TCP over port 502.

Dragos Ecosystem – Frostygoop Example



May 2024 – WorldView Subscribers Alerted of FrostyGoop malware

June 2024 – WorldView Subscribers Alerted of Confirmed Attack on OT

July 2024 – Briefing for Dragos Customers

July 2024 – Public Announcement of FrostyGoop, 9th ICS Malware

NK

PLATFORM & OT WATCH

OT CTI

Dragos OT CTI Team – **Dragos Intel Discovers and Researches.**

Identify new malware with low confidence after attack, develop IOC & behaviors

Neighborhood Keeper – **Threat Analytics Run On Neighborhood Keeper**

Hunters query data, send Trusted Insight Response if high value analytic seen, all anonymous

Dragos Platform – **Threat Analytics Deployed via KP**

<1 Day from WorldView Alert

OT Watch Threat Hunting – **Daily Threat Hunts from OTW**

FrostyGoop run added to OTWatch daily hunts

Dragos Platform – **Composite Detections Deployed via KP+**

Detect adversarial activity with composite detections + respond with embedded Playbooks

Neighborhood Keeper – **Run Threat Analytics Across NK Fleet**

If found, notification via dashboards

DEMO

Threat and Response Workflow

DEMO

Threat Hunting in OT Environments

Actioning Intelligence

1 **Threat Discovery:** Circumstance or event with the potential to adversely impact organizational operations (NIST)

2 **Threat Intelligence:** Detailed actionable threat information used to prevent and fight cybersecurity threats targeting an organization

3 **Threat Hunting:** Proactively discovering, identifying and investigating known and unknown cyber-threats within a network

4 Putting It All Together

Threat Hunt Hypothesis?

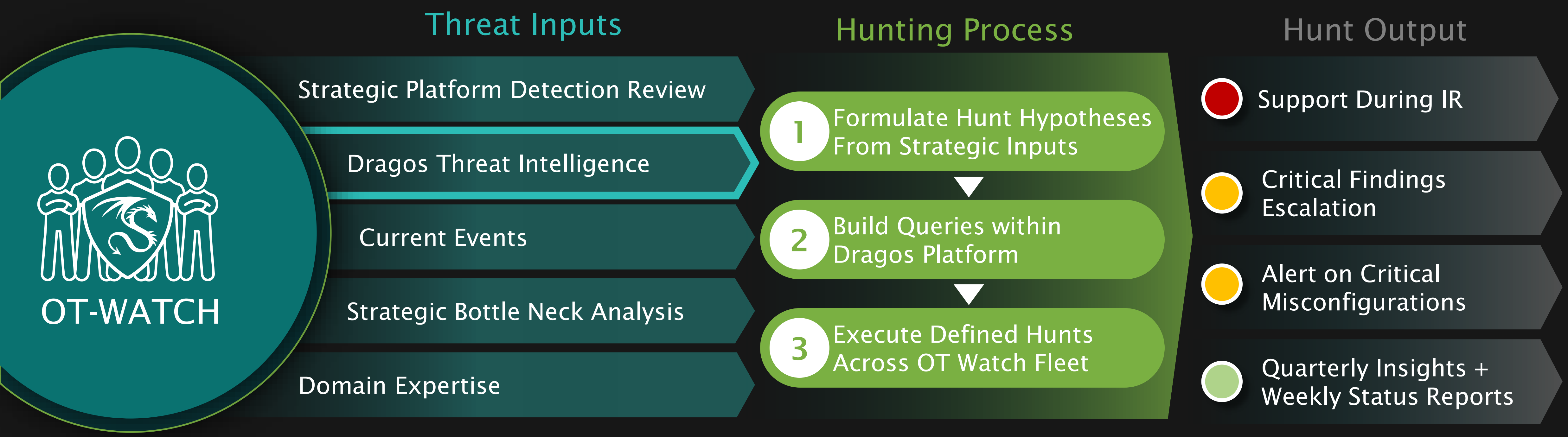
Data Required?

Duration Required?

Access / Visibility Required?

How OT Watch Threat Hunts

Threat-Hunting-as-a-Service – Provides peace of mind by adding a human element to detecting threats



OT-WATCH

Threat Inputs

- Strategic Platform Detection Review
- Dragos Threat Intelligence
- Current Events
- Strategic Bottle Neck Analysis
- Domain Expertise

Hunting Process

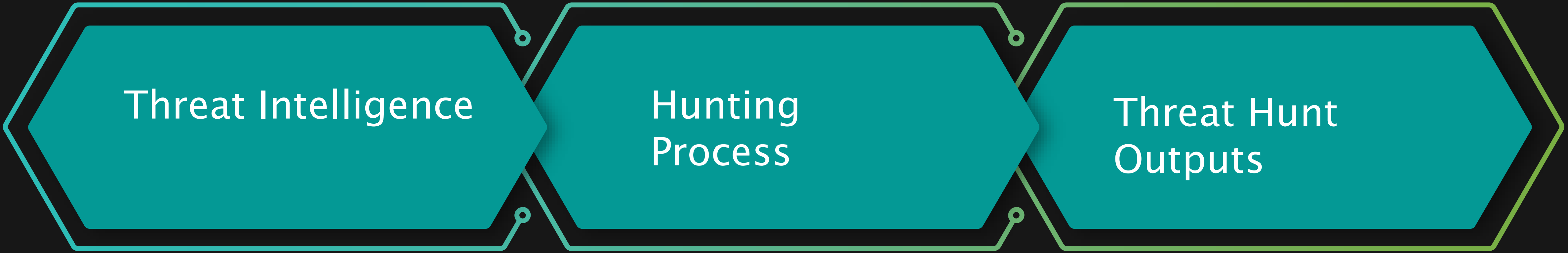
1. Formulate Hunt Hypotheses From Strategic Inputs
2. Build Queries within Dragos Platform
3. Execute Defined Hunts Across OT Watch Fleet

Hunt Output

- ● Support During IR
- ● Critical Findings Escalation
- ● Alert on Critical Misconfigurations
- ● Quarterly Insights + Weekly Status Reports

Threat Hunting Example: Critical Vuln

AA-2024-28: CVE-2024-6242, Rockwell Automation Trusted Slot Bypass Vulnerability



Threat Intelligence

Hunting Process

Threat Hunt Outputs

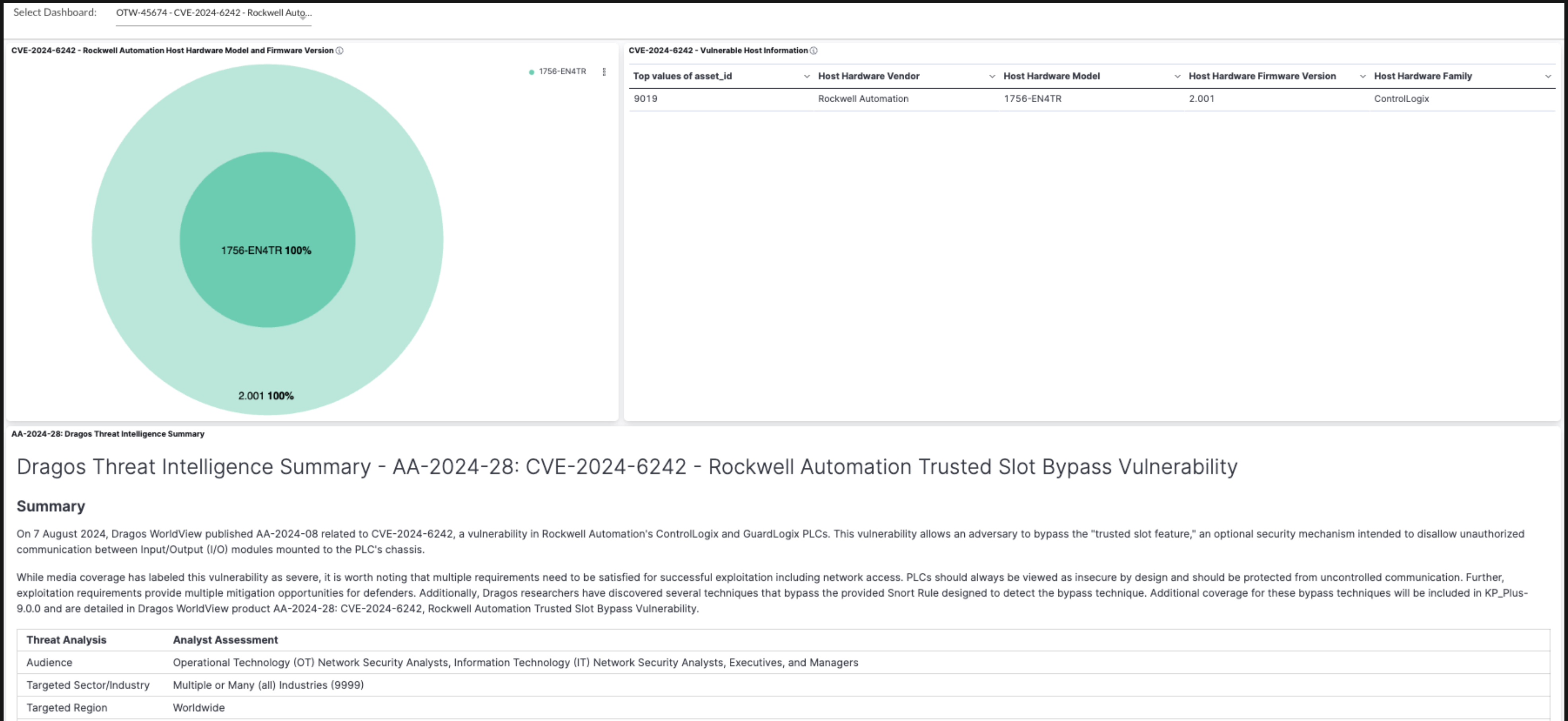
- Chassis restrictions bypass vulnerability
  - 1756-L8z
  - 1756-L8zS
  - 1756-EN2T (A/B/C/D)
  - 1756-EN2F (A/B/C)
  - 1756-EN2TR (A/B/C)
  - 1756-EN3TR (A/B)

- Hypothesis generation
- Data requirements
  - Data fields
  - Query build
- Duration requirements
  - Time / visibility
- Execution

- IR Notification or Support
- Critical Finding Escalation
- Weekly Hunting Reports
- Update to Vulnerability Management Database

Integrated Threat Hunting Results

Platform Dashboards and Threat Summaries



Select Dashboard: OTW-45674 - CVE-2024-6242 - Rockwell Auto...

CVE-2024-6242 - Rockwell Automation Host Hardware Model and Firmware Version

CVE-2024-6242 - Vulnerable Host Information

Top values of asset_id	Host Hardware Vendor	Host Hardware Model	Host Hardware Firmware Version	Host Hardware Family
9019	Rockwell Automation	1756-EN4TR	2.001	ControlLogix

AA-2024-28: Dragos Threat Intelligence Summary

Dragos Threat Intelligence Summary - AA-2024-28: CVE-2024-6242 - Rockwell Automation Trusted Slot Bypass Vulnerability

Summary

On 7 August 2024, Dragos WorldView published AA-2024-08 related to CVE-2024-6242, a vulnerability in Rockwell Automation's ControlLogix and GuardLogix PLCs. This vulnerability allows an adversary to bypass the "trusted slot feature," an optional security mechanism intended to disallow unauthorized communication between Input/Output (I/O) modules mounted to the PLC's chassis.

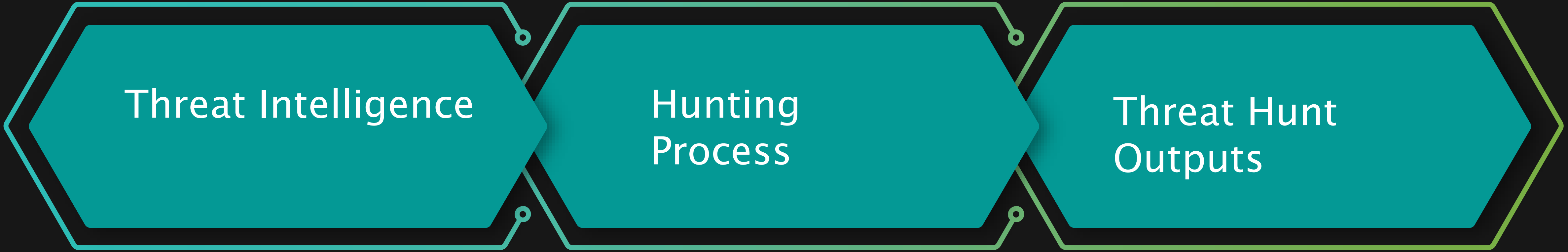
While media coverage has labeled this vulnerability as severe, it is worth noting that multiple requirements need to be satisfied for successful exploitation including network access. PLCs should always be viewed as insecure by design and should be protected from uncontrolled communication. Further, exploitation requirements provide multiple mitigation opportunities for defenders. Additionally, Dragos researchers have discovered several techniques that bypass the provided Snort Rule designed to detect the bypass technique. Additional coverage for these bypass techniques will be included in KP_Plus-9.0.0 and are detailed in Dragos WorldView product AA-2024-28: CVE-2024-6242, Rockwell Automation Trusted Slot Bypass Vulnerability.

Threat Analysis	Analyst Assessment
Audience	Operational Technology (OT) Network Security Analysts, Information Technology (IT) Network Security Analysts, Executives, and Managers
Targeted Sector/Industry	Multiple or Many (all) Industries (9999)
Targeted Region	Worldwide

DRAGOS

Threat Hunting Example: FrostyGoop

AA-2024-23: FrostyGoop Impact on Ukraine Municipal District Energy Company



Threat Intelligence

Hunting Process

Threat Hunt Outputs

- New Network Asset

+ New Modbus Connection TCP over port 502
+ Function codes: 3, 6, 16
+ Specific adversary tradecraft / coding behaviors

- Hypothesis generation
- Data requirements
  - Data fields
  - Query build
- Duration requirements
  - Time / visibility
- Execution

- IR Notification or Support
- Critical Finding Escalation
- Weekly Hunting Reports
- Dashboard Deployment

Engaging Dragos

1 Not sure where to start

SANS 5 CC with Dragos Rapid Response Retainer (RRR)

Start with SANS 5 ICS Critical Controls

Secure Dragos Dragos RRR; burn down with Tabletop Exercise (TTX) to set requirements and Architecture Review (AR) to validate current state.

2 Want to Implement OT Monitoring

Dragos Platform

Implement OT Visibility & Monitoring;
Focus on operationalization

ADD Rapid Response Retainer for IR help and proactive assessments;
ADD OTWatch for expert threat hunting protection

3 Want to implement, but not ready or under resourced

Dragos Platform + OTWatch

Platform + OTWatch provides expert OT threat hunting protection

ADD Deployment Services to streamline rollout

Q&A

QUESTIONS AND ANSWERS