WHITEPAPER

The Vital Role of OT-Native Network Visibility and Security Monitoring Amid IT Frameworks

The Dragos Platform: Built for Industrial Control Systems

MARY KORUS | PRINCIPAL PRODUCT MARKETING MANAGER

DRAGOS, INC

JUNE 2024

TABLE OF CONTENTS

TABLE OF CONTENTS (CONTINUED)

Importance of OT-Native Security for Operational Technology Environments

Protecting operational environments and the operational technology (OT) that runs them is difficult. Threats targeting OT environments have become more sophisticated. Since 2021, there has been a 50% increase in the activities of threat groups targeting industrial operations equipment and in ransomware attacks targeting these environments, as highlighted in the **Dragos 2023 OT Cybersecurity Year in Review**. In this paper, we focus on industrial control systems (ICS) network visibility & monitoring and discuss how Dragos's OT-native cybersecurity technology, the Dragos Platform, is purpose-built to address the needs of these critical environments.

FACT: **IT-focused security practices do not seamlessly translate to the unique demands of OT systems, which are specialized and purpose-built to meet high-availability requirements in industrial processes. The use of legacy technology and proprietary protocols complicates the implementation of OT-focused security controls.**

There are many frameworks that address OT cybersecurity specifically. The scope, scale, and complexity of those frameworks make them hard to implement, especially in an area that has been ignored for so long.

SANS has introduced the 5 Critical Controls for ICS Cybersecurity, a strategic framework specifically developed for OT environments:

5 Critical Controls for ICS Cybersecurity

ICS Incident Response Plan	1	Have an operations-informed incident response plan with a focus on system integrity and recovery capabilities during an attack.
Defensible Architecture	2	Design architectures that support visibility, log collection, asset identification, segmentation, industrial DMZs, and process-communication enforcement.
ICS Network Visibility & Monitoring	3	Enable continuous network security monitoring of the ICS environment using protocol-aware toolsets and system of systems interaction analysis capabilities.
Secure Remote Access	4	Identify all remote access points and allowed destination environments and implement on-demand access and multi-factor authentication (MFA) where possible.
Risk-Based Vulnerability Management	5	Understand the cyber digital controls in place and device operating conditions to make risk-based vulnerability management decisions regarding your OT environment.

Dragos finds these five critical controls to be an incredibly useful distillation, and elements in the these controls have been picked up by more modern regulations in the US, Australia, Asia, Europe, and the Middle East.

Unique Challenges in Monitoring OT Environments

How OT Systems & Protocols Differ from IT

Monitoring ICS and OT environments is challenging, and quite different than information technology (IT). If you look at IT network tools, you will see massive amounts of HTTP and HTTPS (web protocol), DNS (domain lookup), RPC, and numerous other application protocols that pin together IT devices and communications.

Of course, you do see web traffic in OT environments, but typically it is much less and much less important. You also have commonalities between IT and OT network protocols – ARP, STP, 802.1Q, NTP, SSH, RDP, VNC. Networking is networking, and there are common protocols for communications and virtual desktops.

However, in industrial automation applications and OT environments, there are hundreds of systems, each with its own application protocols. Some protocols that are common across vendor systems like are Modbus, BACnet, OPCUA, CodeSys, and CIP (Common Industrial Protocol), and each vendor system uses its own protocol - CDA, ASCII, CNIP, CDA, DOP – and the list goes on.

Understanding the different protocols is critical. In these protocols are the system commands that run the equipment. Attempting to retrofit traditional IT monitoring tools for OT purposes often results in visibility gaps, as these tools do not accommodate the unique protocols and processes of OT systems. That information is key to analyzing activities and spot cyber threats.

Rising Threats & Advanced Attack Techniques in OT Environments.

As the value of targeting operational technology environments becomes increasingly apparent to cyber adversaries, their tactics and tools are becoming more sophisticated and specialized. Among these emerging threats, sophisticated obfuscation techniques such as “living off the land” (LOTL) have become particularly effective. These tactics involve blending malicious activities seamlessly with normal network operations, making them incredibly difficult to detect without advanced monitoring tools.

To effectively counter the sophisticated cyber threats in OT environments, organizations must enhance their threat detection capabilities tailored to OT threats. This enhancement involves not only recognizing anomalies but also identifying indicators of compromise (IOCs) and discerning the tactics, techniques, and procedures (TTPs) employed by the attackers.

Complexity in OT Environments – Monitoring OT, IT, IoT & IIOT Devices

The complexity of monitoring in OT environments is further compounded by the multitude of devices present. OT systems, such as PLCs, SCADA, and HMIs, form the backbone of industrial operations. Beyond traditional OT systems, the rapidly growing number of IoT/IIoT devices adds to the complexity. While these devices enhance automation and efficiency, such as smart sensors, barcode scanners, and special-purpose visual cameras, they introduce specific cybersecurity risks due to their connectivity and potential vulnerabilities.

Effectively monitoring and securing IoT/IIoT devices in OT environments requires solutions that can automatically identify and catalogue catalog these devices, monitor and track their communications, map vulnerabilities, and analyze communications for threats. Traditional IT security solutions are not designed to handle these specific needs in OT networks. Specialized monitoring tools developed for OT systems are essential to provide the visibility and analysis required to protect these diverse devices.

Availability Requirements for OT Environments

In OT environments, the main priorities are keeping operations running smoothly, ensuring the stability of physical processes, and maintaining system safety and reliability. For industrial companies, OT environments need to operate to generate revenue, pay employees, and build value for stockholders. When systems are down, electricity does not flow, oil does not get refined, gas does not move, and goods do not get manufactured. The goal is 100 percent uptime, with maintenance windows carefully planned in advance. This is the standard.

So, when an IT security team member calls and wants to install a network device into the tightly controlled OT operations environment, it often doesn't go over well, and with good reason. Or when they receive a service ticket that says, "patch that OPCUA server," it can cause frustration, as the next maintenance window might be months away.

Given the emphasis on availability, OT environments need tools for practical vulnerability management that provide alternatives to immediate patching.

Value Of OT-Native Monitoring for Operations Networks & Technology

In the following section, we break down the seven key principles of OT network security monitoring. These principles are essential for robust protection and operational efficiency.

Do No Harm: Preserve Uptime with Non-Evasive Monitoring

OT-native monitoring prioritizes non-intrusive oversight to avoid impacting industrial operations and maintaining 100% uptime. Many IT tools that catalog devices on a network can be aggressive, pinging equipment or flooding segments with traffic. Operational environments are sensitive to excess traffic or data messages that don't conform to system standards.

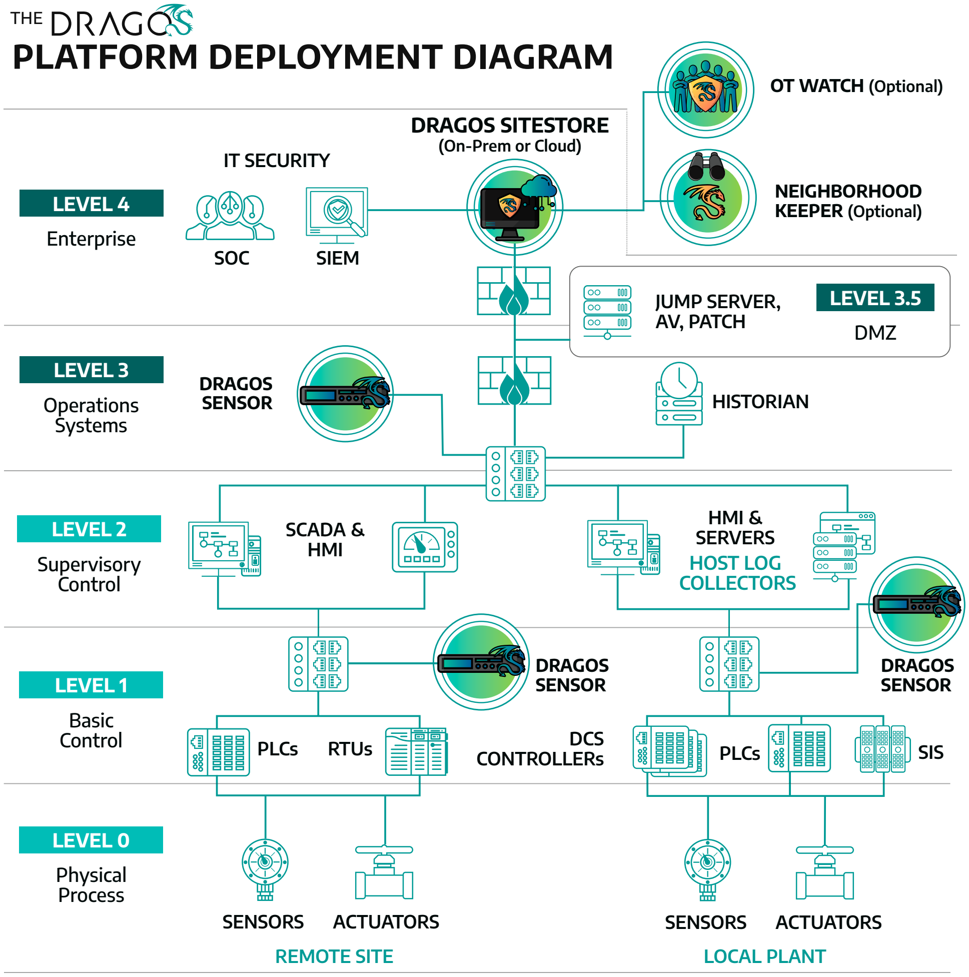
OT-native solutions operate primarily in a passive mode, capturing network data without interfering with operations. Active monitoring can be powerful when designed and trusted specifically for OT environments. These methods should be applied in a highly controlled manner and be purpose-built for these environments. This balanced "do no harm" approach ensures comprehensive monitoring and security without compromising network integrity and performance.

Get a Comprehensive Asset Inventory: OT/IT/IoT Devices Across All Levels of OT

OT-native technology specializes in finding assets within the OT environment, encompassing all device types (OT, IT, IIoT, and IoT assets being used in the OT environment.). It also means operating in the guts of within the OT environment, at Levels 1, 2, 3, and 3.5 (interface of OT/IT) of the Purdue model. IT tools that sit at the border of IT and OT can't see the most critical assets nor the most critical traffic and data to spot problems.

Dig Deep for Insights: Detailed Network Visibility of OT System Traffic

Industrial automation systems run various protocols that may be common across several vendors or proprietary to their system. The network traffic carries the commands to change settings, configure equipment, and conduct other changes to systems. Attackers can leverage those commands to manipulate equipment.


THE DRAGOS PLATFORM DEPLOYMENT DIAGRAM

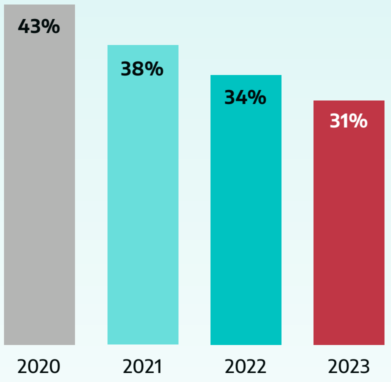
OT-native technology understands industrial network protocols, the system commands, and logging that activity. That data, when paired with accurate and timely OT Cyber Threat Intelligence (CTI), is critical to finding cyber threats. It can also be used to investigate production line issues to optimize equipment and process efficiency.

Deliver Practical OT Vulnerability Management

Vulnerabilities happen. In IT, the typical response is "patch that device." In the world of operations and OT, you can't shut down a substation or a production line to patch a RTU. OT native means understanding the actual potential impact of a vulnerability, defining priority of which needs to be addressed and when, and offering alternative mitigation strategies that allows the process to continue to run safely until a maintenance window can provide a patch if necessary.

According to the Dragos 2023 OT Cybersecurity Year in Review, 31% of 531 vulnerabilities analyzed had errors. Errors can cause asset owners and operators to waste resources on low-risk vulnerabilities over secure ones.

Errors Could Cause Asset Owners And Operators To Waste Resources On Low-Risk Vulnerabilities Over More Severe Ones



Dragos analyzed **531 advisories**
31% had incorrect data.

Detect OT-Focused Cyber Adversaries & Threats

There are more than 20 OT-focused threat groups that directly target operational technology and industrial systems are currently active. They have specialized tactics, techniques, and procedures (TTPs). PIPEDREAM is one example of a highly sophisticated toolset built by the threat group CHERNOVITE, targeting key software components common to hundreds of OT systems, impacting millions of devices. This is one of many attack techniques and toolsets that target OT systems. Effective OT-native threat detection involves utilizing OT-specific IOCs and behavioral threat detection. Many IT visibility tools use general anomaly detection techniques that create a lot of alerts, overwhelming response responses, and missing critical issues. OT native means detecting the threats that target OT and providing context to what needs to be mitigated.

Deliver Value to Operations: Process Insights & Root Cause Analysis

Cyber threats are not the only disruptor of industrial operations. Teams must also respond to networking issues, system misconfiguration, faults, or errors. Detailed monitoring, logging, and analysis across OT systems fill a key gap in many OT environments. The forensic data is used to identify misconfigurations and find root causes of operational problems. The Dragos Platform monitors networks without disruption, mitigates vulnerabilities without system shutdown, and responds too the complexities of the environment to drive tangible value for the operations teams.

Integrate Into IT Security Operations

To effectively manage risks, it is crucial to have a deep understanding of OT systems and environments. Integrating a complete IT/OT ecosystem of technologies within security operations workflows, including those in industrial settings, is essential for a complete cybersecurity program. Together, this approach ensures comprehensive visibility across the organization, provides contextualized vulnerability mitigation, enables intelligence-driven threat detection and response, and enforces protection and segmentation.

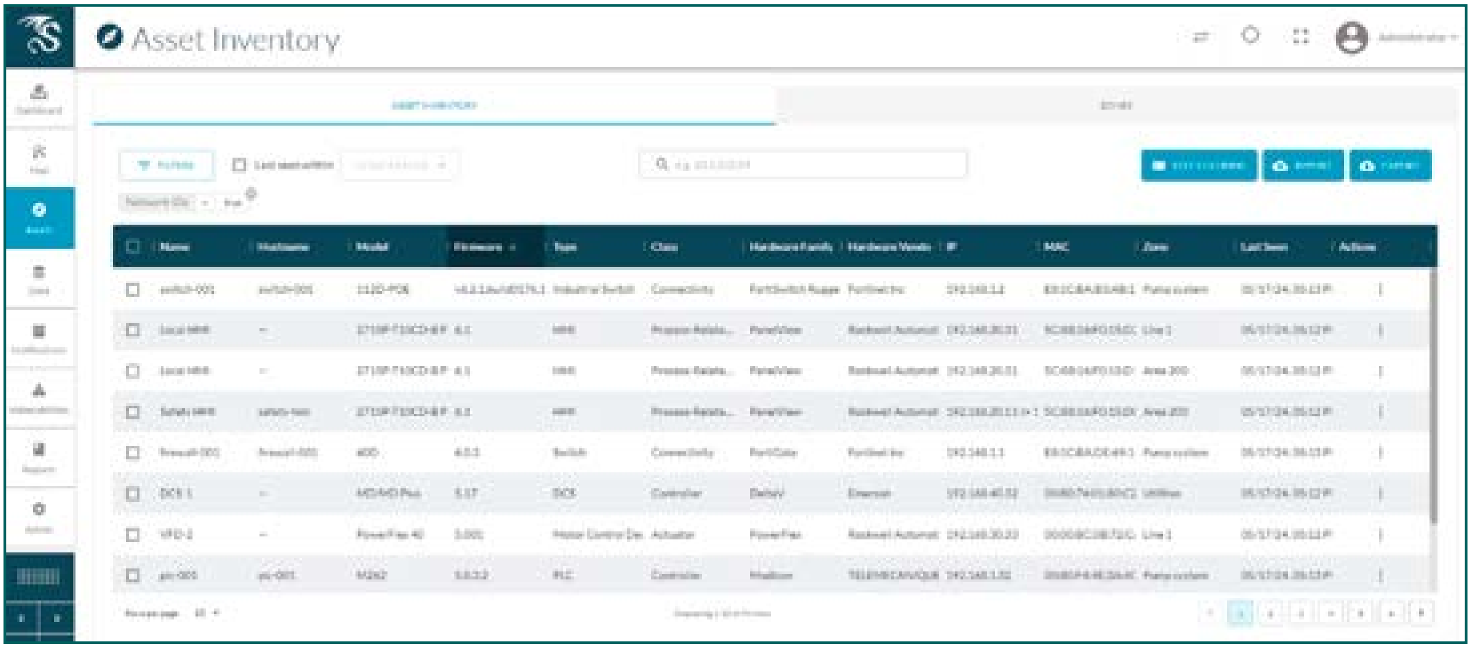
Technology integrations with SIEMs (security information and event management), Firewall, EDR (endpoint detection and response), and service ticketing help lay the foundation of a defensible architecture that OT security can leverage. OT-native visibility and monitoring functionality should integrate into with those tools to build a more effective defense and streamline security operations.

Dragos Platform: Asset Inventory

Identify & Track OT, IT, IoT & IIOT Devices In OT Environments

Creating a comprehensive asset inventory is the first step toward effective security of industrial environments. This involves identifying and cataloging devices—OT systems, IT infrastructure, IoT, and IIoT devices—preferably through automated asset discovery. In OT environments, passive collection methods are the preferred options as they are less disruptive and do not impact performance. When necessary, active monitoring can be employed to gather additional details, such as querying devices for configuration information or software version details.

The Dragos Platform automatically discovers devices on the network and creates an asset inventory. This feature allows for real-time tracking of each device, noting when it was first and last seen on the network. This data is crucial for maintaining an up-to-date and accurate inventory of all network assets.



Name	Hostname	Model	Firmware	Type	Class	Hardware Family	Hardware Vendor	IP	MAC	Zone	Last Seen	Actions
switch-001	switch-001	1120-POE	v6.2.14a/d0176.1	Industrial Switch	Connectivity	FortiSwitch Rugge	Fortinet Inc	192.168.1.2	E8:1C:BA:E1:48:1	Pump system	05/17/24, 05:12 P	⋮
Local HMI	--	2711P-T10CD-B P	6.1	HMI	Process Relate...	PanelView	Rockwell Automat	192.168.20.31	5C:88:16:F0:15:D	Line 1	05/17/24, 05:12 P	⋮
Local HMI	--	2711P-T10CD-B P	4.1	HMI	Process Relate...	PanelView	Rockwell Automat	192.168.20.11	5C:88:16:F0:15:D	Area 200	05/17/24, 05:12 P	⋮
Safety HMI	safety-hmi	2711P-T10CD-B P	6.1	HMI	Process Relate...	PanelView	Rockwell Automat	192.168.20.11 (+1	5C:88:16:F0:15:D	Area 200	05/17/24, 05:12 P	⋮
firewall-001	firewall-001	400	4.0.1	Switch	Connectivity	FortiGate	Fortinet Inc	192.168.1.1	E8:1C:BA:DE:49:1	Pump system	05/17/24, 05:12 P	⋮
DCS 1	--	MD/MD Plus	5.17	DCS	Controller	DeltaV	Emerson	192.168.40.32	00:80:7A:01:80:C	Utilities	05/17/24, 05:12 P	⋮
VFD-2	--	PowerFlex 40	3.001	Motor Control De	Actuator	PowerFlex	Rockwell Automat	192.168.20.22	00:00:BC:3B:72:C	Line 1	05/17/24, 05:12 P	⋮
plc-001	plc-001	M262	5.0.2.2	PLC	Controller	Modicon	TELEMECANIQUE	192.168.1.32	00:80:F4:4E:26:4C	Pump system	05/17/24, 05:12 P	⋮

To enable security teams to see changes to the network over time, the Platform includes a timeline analysis feature. This tool provides a chronological view of network activity, making it easier to identify patterns, spot anomalies, and investigate potential security incidents.

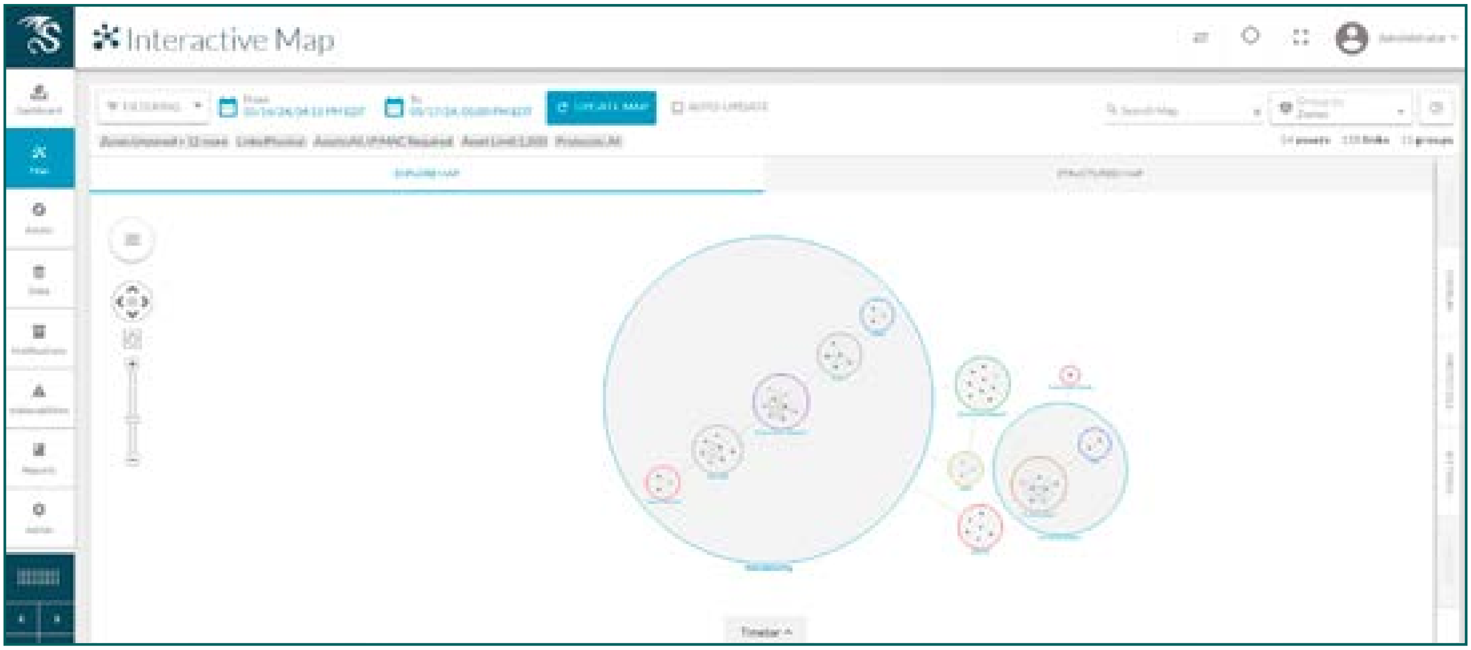
Manage Asset Profiles & Organization

The Dragos Platform uses passive fingerprinting and Deep Packet Inspection (DPI) to detect and track vendor information for common industrial devices. This goes beyond simply identifying the MAC address of each device. It also includes details about the asset's operating system and firmware, providing a more comprehensive view of each device.

In addition to single-interface devices, the system can also handle multi-homed devices, which have multiple network interfaces. If a device has not shown any activity for a user-selectable set time, it will be removed from the baseline devices list. This helps to keep the network map clean and focused on active devices.

The Platform also simplifies the task of assigning assets to their roles for both OT and IT. For OT, this could include roles like master, Human-Machine Interface (HMI), Programmable Logic Controller (PLC), historian, etc. For IT, roles could include Network Time Protocol (NTP) server, web server, Domain Name System (DNS), database, etc.

Finally, the Platform organizes the network visually into zones. This makes it easier for users to understand the layout of the network and the relationships between different devices and areas. This visual organization can be a valuable tool for both network management and security analysis.



Dragos Platform: OT Network Visibility & Monitoring

Analyze OT Network Traffic for Insights Into Cybersecurity & Operational Issues

Comprehensive network visibility goes beyond just listing assets. It means understanding how these assets communicate and operate. This involves monitoring and logging OEM system commands for operational insights. Deep Packet Inspection (DPI) methods cover hundreds of unique protocols to gather detailed information about each asset, such as make, model, firmware version, and configuration. This thorough approach ensures security teams know not only what assets exist but also how they interact and where vulnerabilities might be, what may have caused a disruption, and allows for analysis of where threats may be hiding.

The Dragos Platform is designed with a comprehensive set of features to ensure robust monitoring and security of industrial control systems (ICS). It has the capability to see OSI Layer 2 through 7 ICS protocols based on the data format. This allows for a deep understanding of network traffic and interactions between different devices.

The Platform performs Deep Packet Inspection (DPI) protocol analysis on key ICS applications. This helps in identifying potential security threats and anomalies in network traffic. It logs key activity for variables and function codes for monitored protocols, providing a detailed record of network operations.

One of the key features of the Platform is its ability to monitor, visualize, and alert variables and function codes for monitored protocols. It can monitor and alert on layer 2 and 3, including IP-based traffic for all connected and observable devices. This ensures that any unusual activity or potential security threat is promptly identified and addressed.

Visualize and Baseline Network Traffic, Devices & Key Events

The system provides visualization of ICS/OT asset communications, threat behaviors, vulnerabilities, and anomalies. It displays the communication path as device to device (end-to-end), zone to zone, as well as routed paths. This gives a clear picture of the network topology and the interactions between different devices and zones.

The system baselines devices and communication patterns and allows for the creation of a user-defined allow list and deny list of events. This helps in identifying deviations from normal behavior and potential security threats. It also provides a network event and communication attribute correlation engine able to detect and alert on a combination of anomalies in traffic.

The system can create custom rules and alerts when specific events are detected, facilitating analysis and troubleshooting. Users can make queries on all the collected data and export the results in common formats for further analysis with external tools. The system also provides the ability to create additional reports and dashboards, offering a comprehensive view of the network status and security.

Dragos OT Cyber Threat Intelligence & Intelligence Sharing

Discovery and Sharing of Current OT Threats & Vulnerabilities

New adversaries, tools, vulnerabilities, and threat campaigns emerge on a nearly continuous basis. Being aware of the external threats directed to OT and critical infrastructure is a challenge. That's why Dragos fields the largest civilian threat intelligence operation focused on operational technology.

The Dragos OT Cyber Threat Intelligence teams work diligently to compile and update information on new and emerging OT cyber threats and vulnerabilities, including OT, IT and IoT systems. This constant updating of threat behaviors and vulnerabilities ensures that the organization stays ahead of potential security risks.

Dragos adversary hunters research threat groups that target OT, their campaigns, and their tactics, techniques, and procedures (TTPs). This is compiled into Dragos Platform detections, formulating one of the key differentiators with the Dragos Platform, its ability to find threat behaviors, deliver high fidelity notifications, and minimize the noise that can overwhelm security teams.

In addition, vulnerability researchers conduct primary analysis of OT systems to identify vulnerabilities. These are issued under the Dragos Certified Numbering Authority (CNA). Dragos analysts review CVEs (Common Vulnerabilities & Exposure) from multiple third-party sources to assess their impact and add OT risk & impact analysis. These vulnerabilities are compiled into the Dragos Platform vulnerability database to match your asset inventory, giving you clear impacts and mitigation alternatives to keep your OT safe.

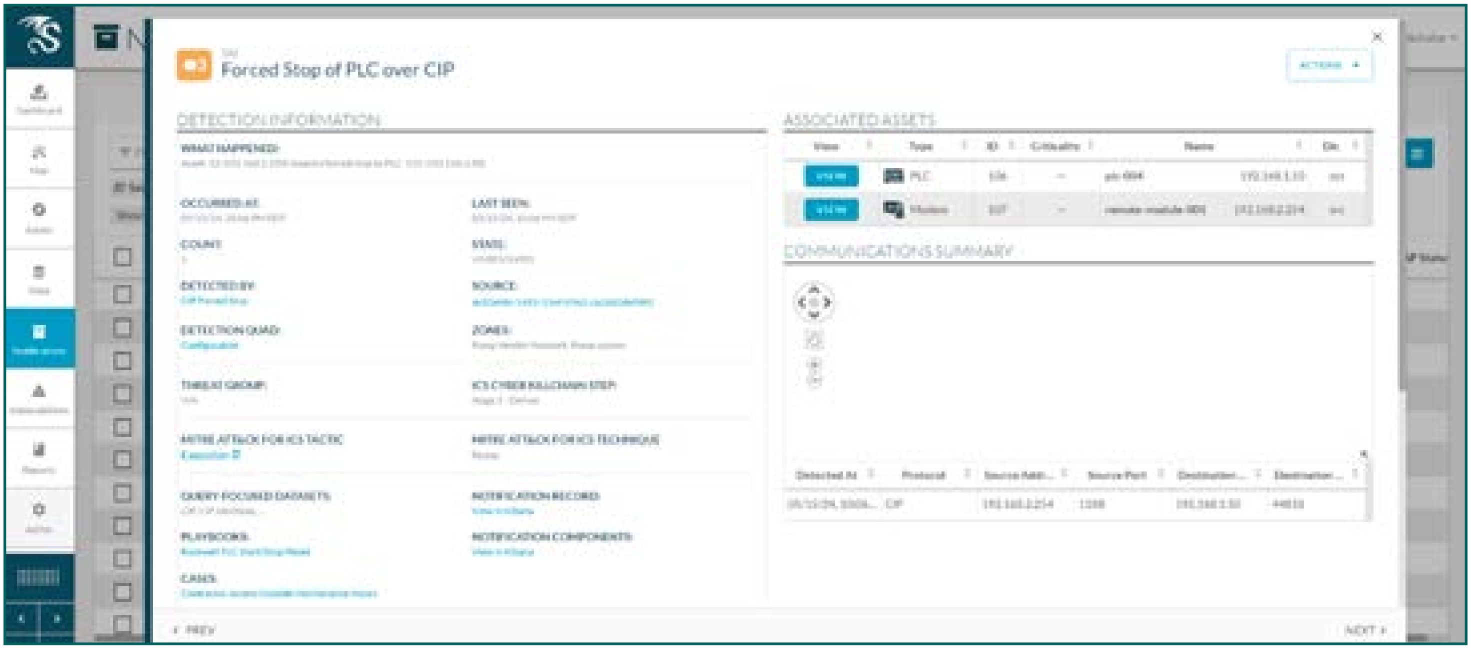
In addition to integration of threat detections and vulnerability data in the Dragos Platform, our threat intelligence is published in full via Dragos WorldView threat intelligence reports, available by subscription.

Dragos Platform: Risk-Based Vulnerability Management

Identify & Manage Vulnerabilities While Maintaining Continuous Operations

Establishing effective vulnerability management is vital for OT cybersecurity because unaddressed vulnerabilities can lead to exploitation and potential compliance issues. A "patch-first" mentality isn't feasible due to operational and safety constraints. Yet, this strategy is still often directed. In fact, the Dragos 2023 OT Cybersecurity Year in Review notes that while 72% of vulnerability advisories included a patch, applying them in OT environments is often impractical. Additionally, 73% of advisories offer no viable mitigation options.

The vulnerability management capability of the Dragos Platform is comprehensive, covering various states such as new, open, closed, risk accepted, and reopened. It provides the ability to prioritize vulnerabilities based on risk and operational impact.



Forced Stop of PLC over CIP

DETECTION INFORMATION

WHAT HAPPENED: [illegible]

OCCURRED AT: [illegible]

LAST SEEN: [illegible]

COUNT: [illegible]

STATE: [illegible]

DETECTED BY: [illegible]

SOURCE: [illegible]

DETECTION QUAD: Configuration

ZONES: [illegible]

THREAT GROUP: [illegible]

ICS CYBER KILLCHAIN STEP: [illegible]

MITRE ATT&CK FOR ICS TACTIC: Execution

MITRE ATT&CK FOR ICS TECHNIQUE: [illegible]

QUERY-FOCUSED DATASETS: [illegible]

NOTIFICATION RECORD: [illegible]

PLAYBOOKS: [illegible]

NOTIFICATION COMPONENTS: [illegible]

CASES: [illegible]

ASSOCIATED ASSETS

View	Type	ID	Criticality	Name		Dir.
VIEW	PLC	[illegible]	–	[illegible]	[illegible]	[illegible]
VIEW	[illegible]	[illegible]	–	[illegible]	[illegible]	[illegible]

COMMUNICATIONS SUMMARY

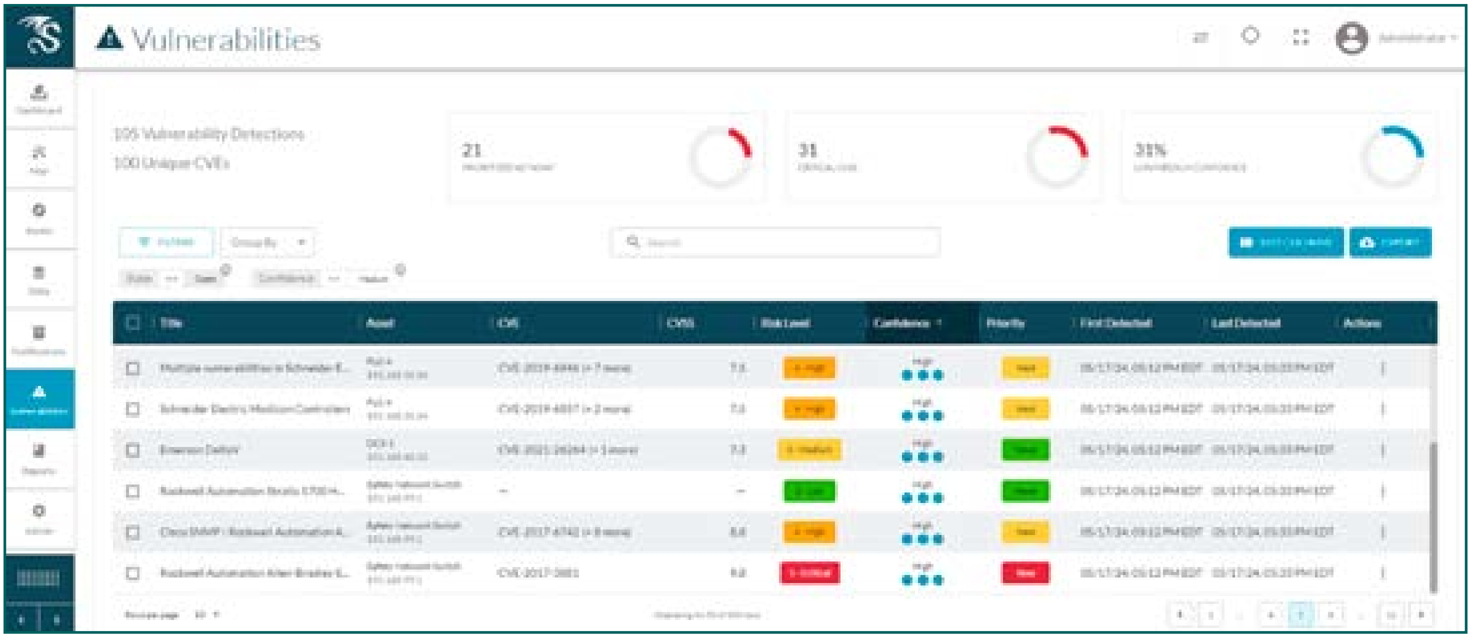
Detected At	Protocol	Source Addr...	Source Port	Destination...	Destination...
[illegible]	CIP	[illegible]	[illegible]	[illegible]	[illegible]

One of the key features of the Dragos Platform is its ability to provide vulnerabilities for the imported assets and not just the assets discovered by the solution. This ensures comprehensive coverage of all assets in the network, enhancing the overall security posture.

Providing IT-Focused CVSS Scoring with OT Context

It is standard to map vulnerabilities to assets and provide a CVS score. However, most scores are aligned to IT impacts. This is where an OT context is invaluable. For example, a vulnerability with a low CVSS score in IT could knock a factory floor offline in the OT environment. Conversely, a "blazing" vulnerability in OT might be "insecure by design" with no risk to operations and thus irrelevant to these environments and closed out. Practical vulnerability management is about grasping the real-world implications of vulnerabilities — how they can disrupt not just individual assets but the intricate systems and processes they support.

Dragos OT Cyber Threat Intelligence analyzes third party CVEs, evaluates the impact, analyzes the true risk, and corrects the CVSS. That information is then compiled and delivered to the Dragos Platform.



Vulnerabilities

105 Vulnerability Detections
100 Unique CVEs

21 PRIORITIZED AS "NOW"

31 CRITICAL CVSS

31% UNKNOWN/LOW CONFIDENCE

	Title	Asset	CVE	CVSS	Risk Level	Confidence	Priority	First Detected	Last Detected	Actions
□	Multiple vulnerabilities in Schneider E...	PLC-[illegible]	CVE-2019-6846 (+7 more)	7.5	4 - High	High ●●●	Next	05/17/24 05:12 PM EDT	05/17/24 05:33 PM EDT	⋮
□	Schneider Electric Modicon Controllers	PLC-[illegible]	CVE-2019-6857 (+2 more)	7.5	4 - High	High ●●●	Next	05/17/24 05:12 PM EDT	05/17/24 05:33 PM EDT	⋮
□	Emerson DeltaV	DCS-1	CVE-2021-26264 (+1 more)	7.3	3 - Medium	High ●●●	Never	05/17/24 05:12 PM EDT	05/17/24 05:33 PM EDT	⋮
□	Rockwell Automation Stratix 5700 H...	Safety Network Switch	–	–	2 - Low	High ●●●	Never	05/17/24 05:12 PM EDT	05/17/24 05:33 PM EDT	⋮
□	Cisco SNMP / Rockwell Automation A...	Safety Network Switch	CVE-2017-6742 (+8 more)	8.8	4 - High	High ●●●	Next	05/17/24 05:12 PM EDT	05/17/24 05:33 PM EDT	⋮
□	Rockwell Automation Allen-Bradley S...	Safety Network Switch	CVE-2017-3881	9.8	5 - Critical	High ●●●	Now	05/17/24 05:12 PM EDT	05/17/24 05:33 PM EDT	⋮

OT-Practical Risk Mitigation Alternatives to Patching

OT cybersecurity teams are often overwhelmed by the sheer volume of potential vulnerabilities that require remediation. Without simple, OT-accurate, and prioritized guidance, it is challenging to address the most critical vulnerabilities effectively, leading to operational risks and non-compliance with regulatory standards and best practices.

Utilizing the enriched risk scoring from our OT CTI team, the Dragos Platform delivers prioritized "Now, Next, Never" guidance. This critical feature enables teams to focus on the most pressing vulnerabilities, effectively mitigating risk and minimizing downtime.

Only Some Vulnerabilities Need Immediate Action

From Dragos 2023 Year In Review: Analysis of ICS/OT Vulnerabilities

3%

of ICS/OT Vulnerabilities Needed To Be Addressed

NOW

68%

Are Network Exploitable With No Direct Operational Impact

These Need To Be Addressed

NEXT

Mitigate Through Network Monitoring, Segementation & MFA

29%

NEVER

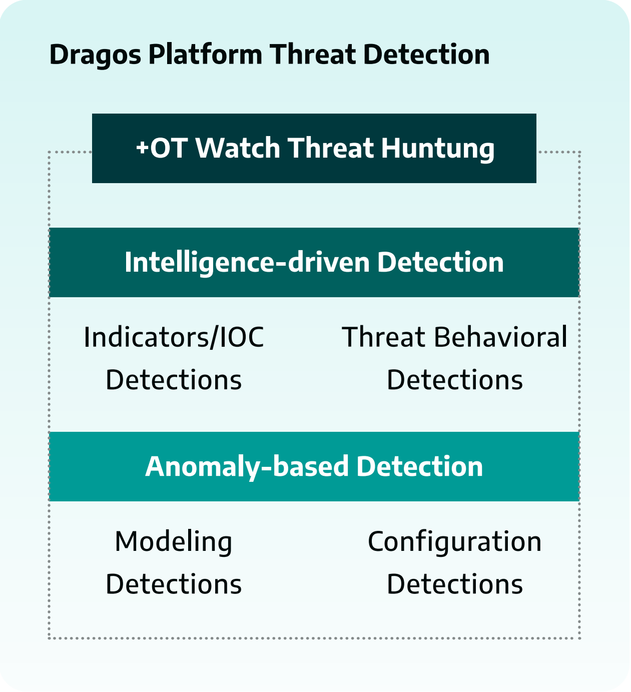
Monitor These For Signs Of Exploitation

Dragos Platform + OT Watch: Intelligence-Driven Threat Detection

There is an imperative: Move beyond the asset inventory stage that many organizations dwell in and get to threat detection. But that means more than "ticking the box." Too many companies adopt a simple anomaly-based approach that results in high levels of alerts that fatigue investigators. As a result, the tools are never effectively used to detect threats.

Many organizations lack the people with the skills and experience to find elusive threats in their environment. Dragos combines high-fidelity detections with a skilled team of hunters to deliver the most effective solution to find OT cyber threats.

For example, in the energy sector, an anomaly in power consumption could be part of routine operations, whereas threat behaviors identified by researched TTPs might indicate a more sophisticated intrusion tailored to energy control systems.



Dragos Platform Threat Detection

+OT Watch Threat Huntung

Intelligence-driven Detection

Indicators/IOC Detections

Threat Behavioral Detections

Anomaly-based Detection

Modeling Detections

Configuration Detections

Get High Fidelity, Low Noise Threat Detection

Dragos uses four methodologies for detecting threats:

Modeling Detection

a type of anomaly detection, is a mathematical approach to detecting threats by defining "normal" and measuring deviations from the definition.

Configuration Detection

a second type of anomaly detection that looks for deviations from a known architecture

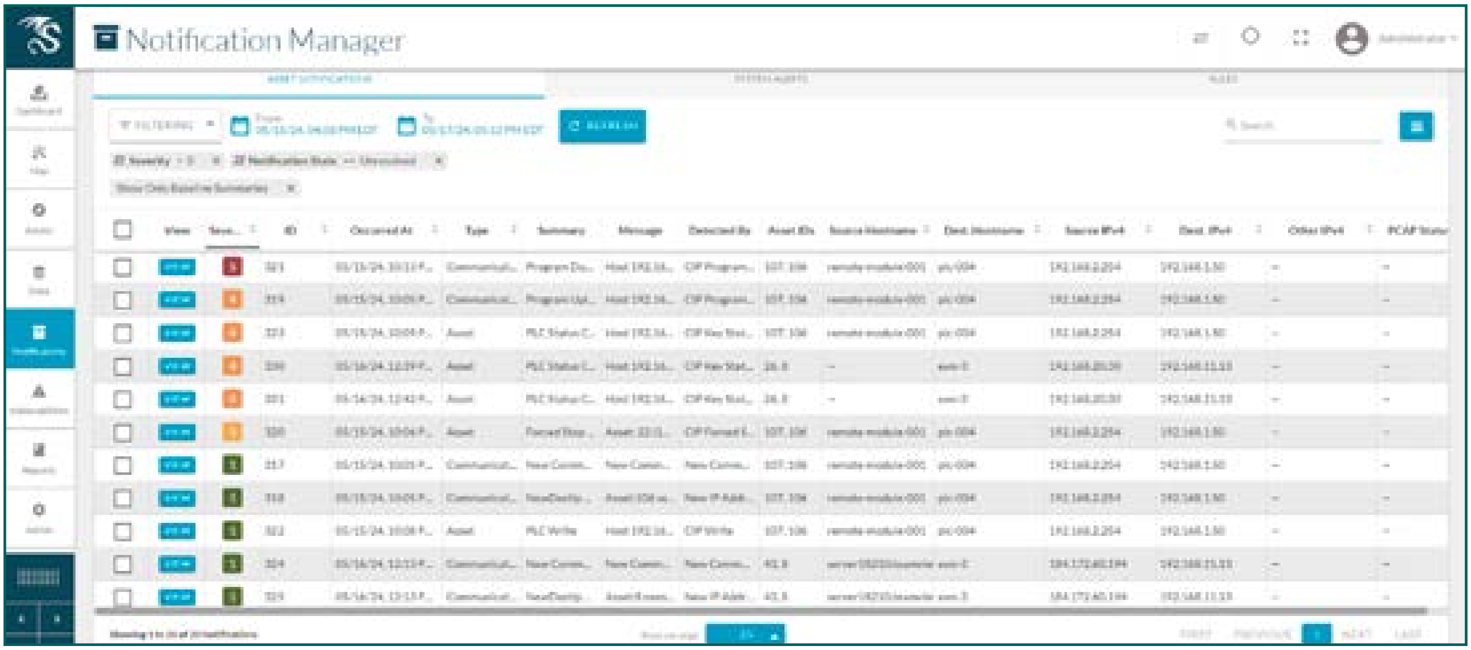
Indicators/IOC Detections

which are elements of information that identify a particular state and context. There are both "good" and "bad" indicators. A bad indicator may be a specific URL associated with a ransomware gang. Sometimes known as Indicators of Compromise or IOCs

Behavioral Threat Detection

codifies malicious adversary tradecraft for detection regardless of specific indicators such as capability or infrastructure. These relate to tactics, techniques, and procedures (TTPs) identified with specific threat activity groups or toolsets.

By integrating IOCs and TTPs into threat detection processes and tailoring them to the specific environments and operations of OT systems, organizations can significantly reduce the incidence of false positives and enhance the accuracy of threat detection. This OT-aligned approach is crucial for ensuring that when alerts do arise, they receive the attention and resources necessary to respond effectively and maintain the security and continuity of critical operations.



Notification Manager

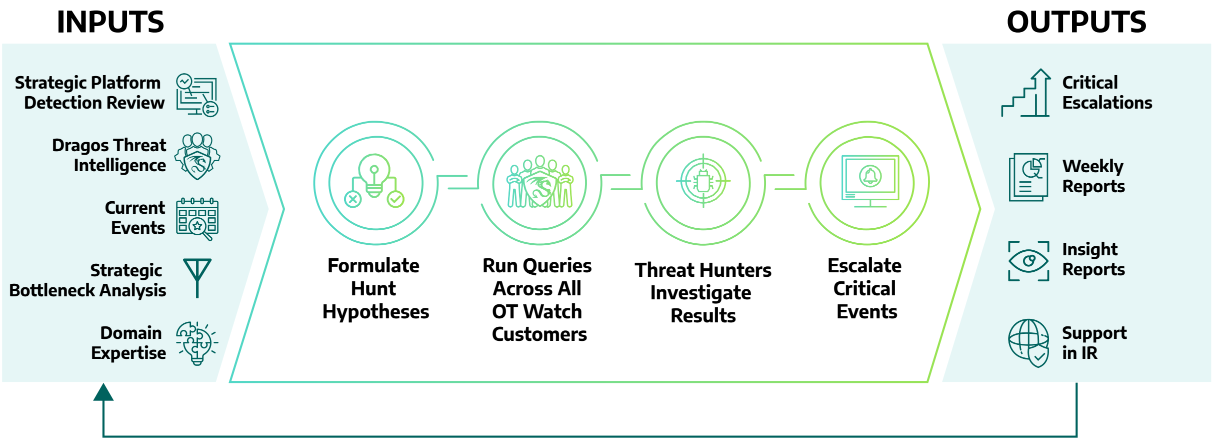
	View	Seve…	ID	Occurred At	Type	Summary	Message	Detected By	Asset IDs	Source Hostname	Dest. Hostname	Source IPv4	Dest. IPv4	Other IPv4	PCAP Status
□	VIEW	5	321	05/15/24 10:13 P…	Communicati…	Program Do…	Host 192.16…	CIP Program…	107, 104	remote-module-001	plc-004	192.168.2.254	192.168.1.50	–	–
□	VIEW	4	319	05/15/24 10:09 P…	Communicati…	Program Up…	Host 192.16…	CIP Program…	107, 104	remote-module-001	plc-004	192.168.2.254	192.168.1.50	–	–
□	VIEW	4	323	05/15/24 10:09 P…	Asset	PLC Status C…	Host 192.16…	CIP Key Swi…	107, 104	remote-module-001	plc-004	192.168.2.254	192.168.1.50	–	–
□	VIEW	4	330	05/16/24 12:39 P…	Asset	PLC Status C…	Host 192.16…	CIP Key Swi…	26, 8	–	evm-3	192.168.20.30	192.168.11.13	–	–
□	VIEW	4	331	05/16/24 12:42 P…	Asset	PLC Status C…	Host 192.16…	CIP Key Swi…	26, 8	–	evm-3	192.168.20.30	192.168.11.13	–	–
□	VIEW	3	320	05/15/24 10:04 P…	Asset	Forced Stat…	Asset 22 (1…	CIP Forced I…	107, 104	remote-module-001	plc-004	192.168.2.254	192.168.1.50	–	–
□	VIEW	1	317	05/15/24 10:01 P…	Communicati…	New Comm…	New Comm…	New Comm…	107, 106	remote-module-001	plc-004	192.168.2.254	192.168.1.50	–	–
□	VIEW	1	318	05/15/24 10:01 P…	Communicati…	New Dev/Ip…	Asset 106 w…	New IP Addr…	107, 104	remote-module-001	plc-004	192.168.2.254	192.168.1.50	–	–
□	VIEW	1	322	05/15/24 10:08 P…	Asset	PLC Write	Host 192.16…	CIP Write	107, 106	remote-module-001	plc-004	192.168.2.254	192.168.1.50	–	–
□	VIEW	1	324	05/16/24 12:13 P…	Communicati…	New Comm…	New Comm…	New Comm…	42, 8	server-08210.example	evm-3	184.172.60.194	192.168.11.13	–	–
□	VIEW	1	325	05/16/24 13:13 P…	Communicati…	New Dev/Ip…	Asset 8 was…	New IP Addr…	43, 8	server-08210.example	evm-3	184.172.60.194	192.168.11.13	–	–

Threat Hunting Finds Highly Elusive Adversaries & Tools

The Dragos Platform is the best in the world at detecting threats to OT, as validated by MITRE ATT&CK for ICS. But, detecting sophisticated tactics of human threat actors remains a challenge. To address this, organizations are encouraged to integrate the human element of security. This involves merging advanced cybersecurity technology with proactive threat hunting, which aids in identifying advanced tools and escalating them for further investigation.

The Dragos OT Watch team of threat hunters develops hunting leads from various key inputs. These include strategic reviews of detections on the Dragos Platform, proprietary OT Cyber Threat Intelligence (CTI), and insights from external sources and current events. The team hunts for critical steps or "bottlenecks" that an attacker must navigate to install their tools, gain and propagate access, and achieve their objectives. By leveraging WorldView OT CTI and the expertise of hunters, OT Watch can tailor targeted hunts to address specific security risks in industrial environments.

Dragos OT Watch Threat Hunting Process


INPUTS
Strategic Platform Detection Review
Dragos Threat Intelligence
Current Events
Strategic Bottleneck Analysis
Domain Expertise
Formulate Hunt Hypotheses
Run Queries Across All OT Watch Customers
Threat Hunters Investigate Results
Escalate Critical Events
OUTPUTS
Critical Escalations
Weekly Reports
Insight Reports
Support in IR

Hunting queries are disseminated across the OT Watch customer fleet. When these hunts yield results, the OT Watch team delves into deeper investigation and validation. The team also conducts exploratory hunting to devise new methods of detecting adversaries. Upon completion, significant findings and security events are escalated, enabling customers to take swift and effective prioritized action.

To further optimize Dragos Platform performance, Technical Account Managers (TAMs) conduct platform-tuning support cadence calls. During hunting operations, OT Watch often uncovers misconfigurations in networks, systems, and applications, thereby enhancing the security posture and reducing attack exposure.

OT Watch also provides support to the customer's incident response (IR) team during an event, ensuring a coordinated and effective response to any threats. To maintain a pulse on the system's performance and security status, weekly and quarterly insight reporting is also conducted.

Dragos Platform: Investigation & Response

Get Detailed Forensics to Streamline Investigations

The Dragos Platform enhances an organization's response plan to speed up forensics and enable quick resolution with embedded case management and integrated response playbooks developed by OT security experts. Forensics are abstracted and well organized, and users can easily create cases to initiate investigations, accessing relevant activity logs and timeline views. This comprehensive approach ensures thorough and efficient incident investigations.

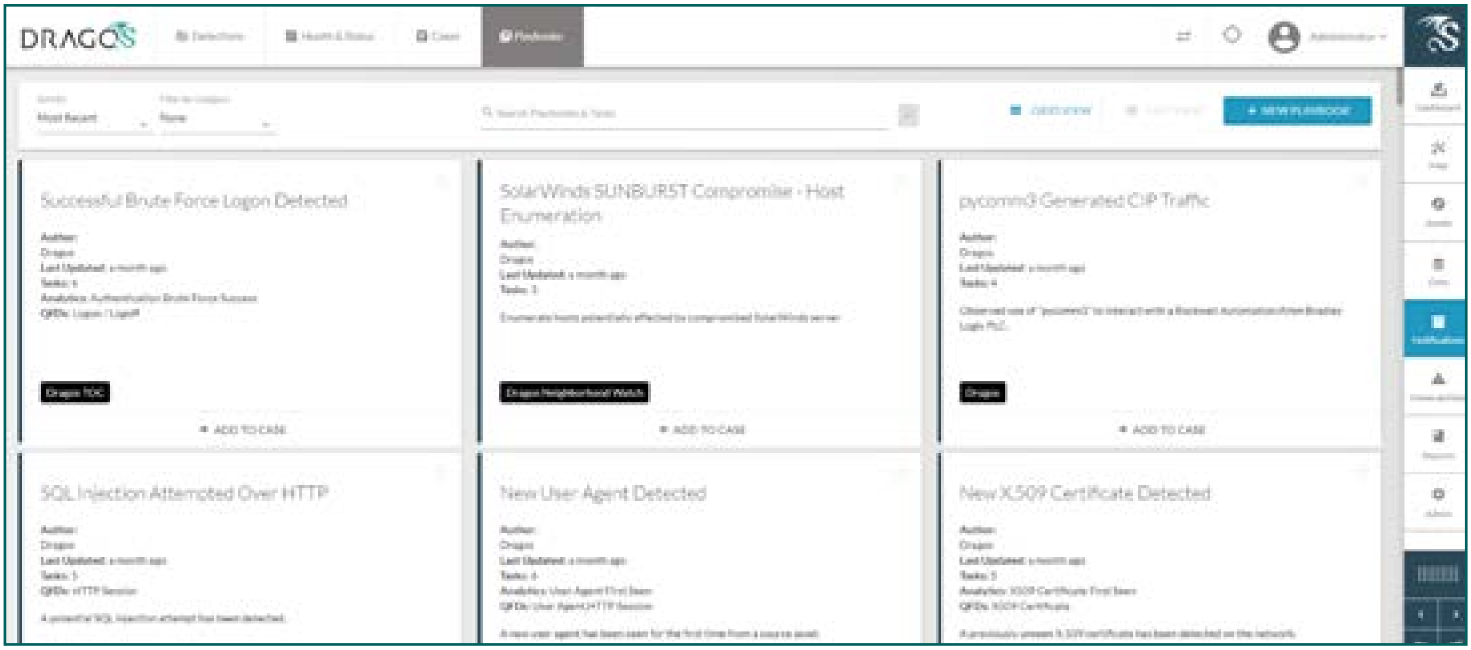
The system visually presents timeline analysis on structured maps, aiding investigations and providing a comprehensive view of events. This is facilitated by an analyst workbench, which has the capability to perform investigations natively in the technology without the need for additional integrations.

To streamline the investigation process, predefined queries are available. These provide responders with immediate access to the data they need, eliminating the need to search for specific data such as Logon/Logoff events, PLC state changes, and DNS queries. This feature is complemented by Query Focused Datasets, pre-defined queries that enable rapid analysis and investigation of alert information.

The system allows users to make queries on all the collected data and to export the results in common formats. This feature facilitates further analysis with external tools. Additionally, the system can perform and store network capture files (pcap or pcapng) for replay and post-event forensic analysis.

Expert-Authored Response Playbooks Provide Leverage from Experienced Responders

Case management is another key feature of the Dragos Platform. It automatically associates relevant playbooks to the identified notifications, streamlining the response process. The system Platform comes with pre-configured focusedquery-focused datasets and relevant behaviors TTPs in the playbooks to improve investigation and response time.



Successful Brute Force Logon Detected
Author:
Dragos
Last Updated: a month ago
Tasks: [illegible]
Analytics: Authentication Brute Force Success
QFDs: Logon / Logoff
Dragos SOC
ADD TO CASE

SolarWinds SUNBURST Compromise - Host Enumeration
Author:
Dragos
Last Updated: a month ago
Tasks: 3
Enumerate hosts potentially affected by compromised SolarWinds server
Dragos Neighborhood Watch
ADD TO CASE

pycomm3 Generated CIP Traffic
Author:
Dragos
Last Updated: a month ago
Tasks: 4
Observed use of "pycomm3" to interact with a Rockwell Automation Allen Bradley Logix PLC.
Dragos
ADD TO CASE

SQL Injection Attempted Over HTTP
Author:
Dragos
Last Updated: a month ago
Tasks: 5
QFDs: HTTP Session
A potential SQL Injection attempt has been detected.

New User Agent Detected
Author:
Dragos
Last Updated: a month ago
Tasks: 4
Analytics: User Agent First Seen
QFDs: User Agent,HTTP Session
A new user agent has been seen for the first time from a source asset.

New X.509 Certificate Detected
Author:
Dragos
Last Updated: a month ago
Tasks: 3
Analytics: X509 Certificate First Seen
QFDs: X509 Certificate
A previously unseen X.509 certificate has been detected on the network.

The case management capability also includes the ability to attach evidence and relevant notifications identified by the solution to the created cases. It supports owner assignment, ensuring accountability and efficient management of cases. The Dragos Platform is equipped with case management functionality and investigation playbooks to respond to common ICS threat scenarios. Furthermore, the playbooks can be customized to match the requirements of the incidents, providing a flexible and adaptable solution for incident response.

Platform Deployment: OT Visibility & Monitoring

Where to Monitor: IT/OT Boundary & Deep Into Operations

The Dragos Platform can safely monitor deep into OT environments, deploying at key points in the Purdue Model. The Purdue Model is a model for the segmentation of physical processes, sensors, supervisory controls, operations, and logistics. The Dragos Platform enables OT network visibility from level 1 – level 3 of the Purdue model and at the IT/OT network boundary with multiple methods of data capture to assure environment availability and comprehensive coverages.

Passive First

The primary method is via Dragos Sensors, passive devices deployed at key aggregation points using network spans, port mirroring, or traffic aggregators to direct copies of network traffic to the Dragos Sensors.

As the sensor sees traffic, it builds asset inventories, logs key activities, and analyzes the data. This results in threat detections dashboard, vulnerability dashboard, asset inventory and communications visualization, along with other views on the OT system and network activity.

Sensors connect to SiteStores, which aggregate information across all connected sensors. SiteStore operates either on-premises or in the cloud. Both sensors and SiteStores can be deployed virtually on your approved hardware models via ESXi and HyperV; they are also delivered on Dragos hardware platforms, with multiple options to meet capacity, form factor, and environmental needs.

Dragos also offers other passive collection methods to enrich data. The Platform supports ingested data logs, utilizes local collection and integrates with third-party tools to feed data into the Platform to ensure comprehensive visibility while maintaining minimal impacts to operations.

Active Monitoring to Fill the Gaps

Active techniques are utilized to fill visibility gaps, extend asset attributes, and verify information that passive methods have not yet been identified. Dragos' extended the ability to actively discover and query assets, supporting inventory and monitoring use cases. These features are purpose-built for OT environments, providing read-only access to the systems being monitored while prioritizing non-intrusive methods of asset identification. It is recommended to conduct active query during scheduled maintenance or downtime to minimize the risk to production systems.

Platform Integration with IT Security Operations

Security Operations – Integrate OT Monitoring Into SIEM & Service Ticketing

Security Information and Event Management (SIEM) systems play a pivotal role in cybersecurity operations. They serve as the central hub for security-related activities, providing real-time analysis of security alerts generated by applications and network hardware. Key tasks performed by SIEMs include data aggregation, correlation, alerting, threat detection, and forensics.

The Dragos Platform feeds contextualized data and prioritized notifications into SIEMs like Splunk, Fortinet and CrowdStrike, so defenders have maximum visibility across both IT and OT networks, improving overall threat detection, response, and post-incident mitigation when time is of the essence.

Service Management systems like ServiceNow allow users to manage digital workflows for enterprise operations like asset and vulnerability management, along with security operations to manage incident response cases and service desk tickets. Through an integration with ServiceNow, ServiceNow users can utilize the comprehensive asset discovery available in the Dragos Platform to reveal critical enterprise assets such as industrial controllers (Programmable Logic Controllers - PLCs, Distributed Control Systems - DCSs), helping drive a more accurate asset inventory. The additional knowledge of OT assets, along with prioritization on vulnerabilities and associated alternative mitigation options, allows ServiceNow users to make better-informed workflow decisions based on the asset type, locations, and function, resulting in improved overall efficiency.

Infrastructure – Add OT-Native Intelligence Into IT Firewalls & Endpoint

Dragos integrates its ICS/OT intelligence into both Firewalls and EDR (Endpoint detection and response). This approach allows for a more tailored security posture, with firewall policies created specifically for different device groups within the industrial environment. For instance, the Dragos Platform provides asset inventories to firewalls to create policies. Policies can be set to block remote access connections to certain systems or device groups, thereby strengthening the network's defense against unauthorized access.

In addition to device inventory management for policy creation, the Dragos Platform offers intelligence-derived network-based threat detections that work with firewall isolation capabilities. When the Platform identifies a potential threat within the network, it can trigger a firewall policy for an administrator to isolate or block the affected devices, preventing the spread of any malicious activity. Furthermore, the Dragos Platform plays a crucial role in validating firewall policies, providing monitoring of the environment to identify potential drift from expected policies.

Extending comprehensive visibility, detection, and response capabilities across IT and OT Networks, EDR integrations like CrowdStrike, enrich the Dragos Platform with additional threat telemetry to accelerate the detection, investigation, and response of cyber incidents across the enterprise.

OT Incident Response Services Augment Your IR Capability

Cyber incidents happen. The volume of ransomware events targeting industrial companies continues to increase every year. While many companies have an IT cyber incident response (IR) plan in place, to few have IR plans for the Operations environments. And let's be clear – incidents impacting power plants, substations, pipelines, processing facilities, refineries, and manufacturing floors have unique requirements.

Those are among the many reasons that SANS #1 ICS critical control is the creation of an ICS Incident Response Plan – to proactively prepare for an incident – so have the people, systems, and required resources identified and contracted to help on those worst days that we hope never to see.

Dragos OT Incident Response teams are experienced in industrial cyber events, there to help our investigate and resolve incidents as quickly as possible. That experience and expertise is available to our customers to help your teams in times of crisis.

Conclusion

The evolving landscape of cybersecurity threats targeting OT environments demands a specialized approach to network visibility and monitoring. The recommendation of SANS Critical Control #3, which emphasizes the criticality of ICS network visibility and monitoring, provides a clear and actionable framework for organizations. Implementing this control involves adopting OT-native solutions that integrate seamlessly with existing IT security operations, enhancing both security and operational efficiency.

Monitoring diverse OT, IT, IoT, and IIoT devices is complex, and the increasing sophistication of OT-focused adversaries highlights the need for OT-native solutions. These solutions provide deep insights into network traffic, practical vulnerability management, and high-fidelity threat detection with minimal false positives. Integrating OT cybersecurity measures into broader IT security frameworks is essential for effective risk management.

The Dragos Platform is vital for organizations aiming to protect their critical infrastructure. Its capabilities in network visibility, vulnerability management, and threat response help maintain the security and resilience of industrial operations. As the threat landscape evolves, leveraging specialized OT cybersecurity solutions like the Dragos Platform will be crucial for maintaining the safety, reliability, and efficiency of industrial processes.

About Dragos, Inc.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. 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.

Learn more about our technology, services, and threat intelligence offerings:

Request a Demo   Contact Us