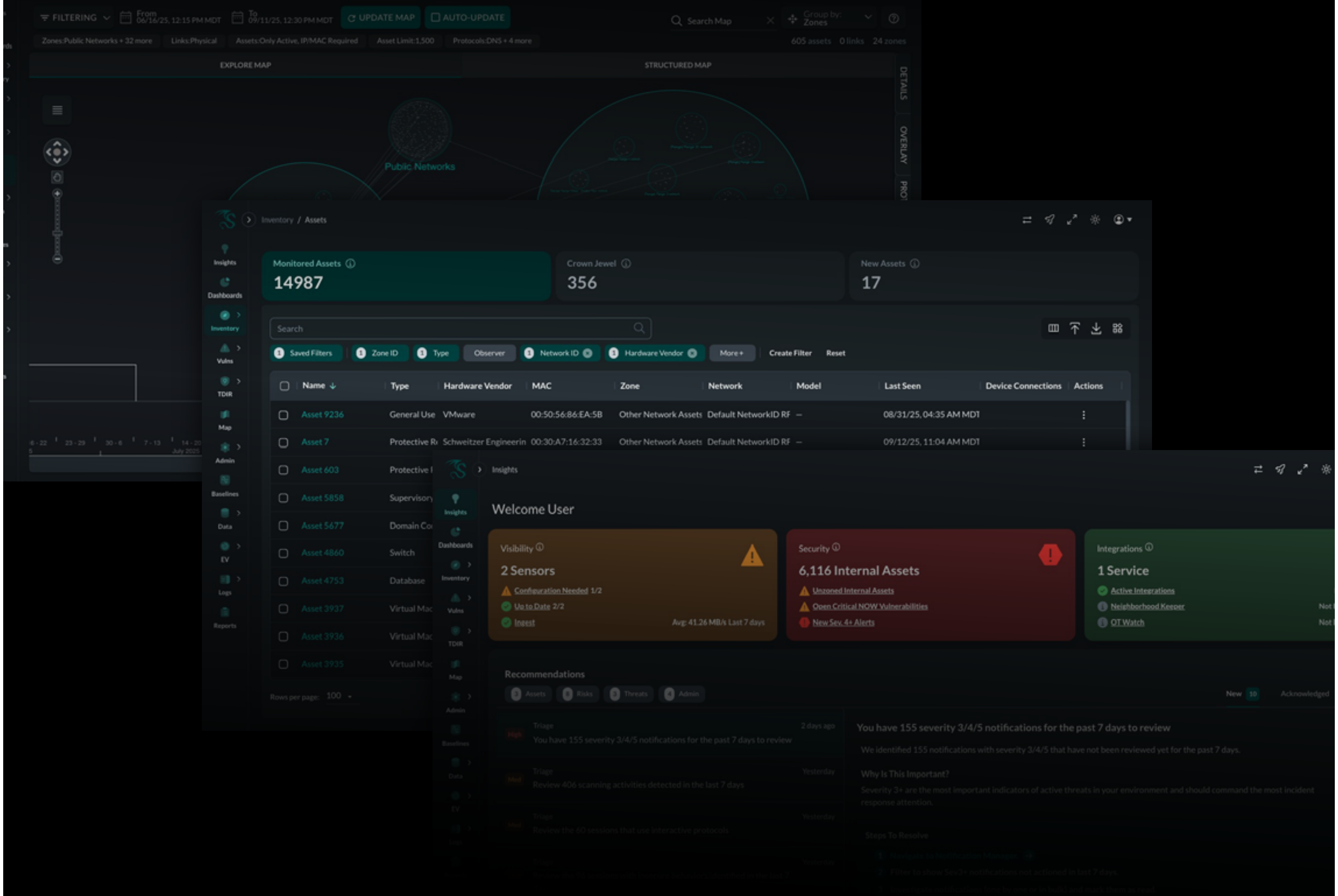
BROCHURE



Inventory / Assets

Monitored Assets 14987

Crown Jewel 356

New Assets 17

Search

1 Saved Filters · 1 Zone ID · 1 Type · Observer · 1 Network ID · 1 Hardware Vendor · More + · Create Filter · Reset

Name	Type	Hardware Vendor	MAC	Zone	Network	Model	Last Seen	Device Connections	Actions
Asset 9236	General Use	VMware	00:50:56:86:EA:5B	Other Network Assets	Default NetworkID RF	–	08/31/25, 04:35 AM MDT		⋮
Asset 7	Protective R	Schweitzer Engineerin	00:30:A7:16:32:33	Other Network Assets	Default NetworkID RF	–	09/12/25, 11:04 AM MDT		⋮
Asset 603	Protective I								
Asset 5858	Supervisory								
Asset 5677	Domain Co								
Asset 4860	Switch								
Asset 4753	Database								
Asset 3937	Virtual Mac								
Asset 3936	Virtual Mac								
Asset 3935	Virtual Mac								

Rows per page: 100

Insights

Welcome User

Visibility
2 Sensors
Configuration Needed 1/2
Up to Date 2/2
Ingest
Avg: 41.26 MB/s Last 7 days

Security
6,116 Internal Assets
Unzoned Internal Assets
Open Critical NOW Vulnerabilities
New Sev. 4+ Alerts

Integrations
1 Service
Active Integrations
Neighborhood Keeper
OT Watch

Recommendations

3 Assets · 8 Risks · 3 Threats · 4 Admin · New 10 · Acknowledged

High · Triage · 2 days ago
You have 155 severity 3/4/5 notifications for the past 7 days to review

Med · Triage · Yesterday
Review 406 scanning activities detected in the last 7 days

Med · Triage · Yesterday
Review the 60 sessions that use interactive protocols

You have 155 severity 3/4/5 notifications for the past 7 days to review

We identified 155 notifications with severity 3/4/5 that have not been reviewed yet for the past 7 days.

Why Is This Important?

Severity 3+ are the most important indicators of active threats in your environment and should command the most incident response attention.

Steps To Resolve

The Dragos Platform

A Cybersecurity Platform Built for OT Environments

The Dragos Platform delivers network security monitoring, asset visibility and inventory, risk-based vulnerability management, intelligence-driven threat detection, and comprehensive investigation and response capabilities across operational technology (OT) environments—including OT systems, IT, IoT, IIoT, and cyber-physical systems (CPS). Powered by industry-leading OT cyber threat intelligence and built by defenders for defenders, the Dragos Platform provides actionable insights to protect critical industrial infrastructure from emerging cyber threats.

THE CHALLENGE

Cyber adversaries are increasingly targeting industrial infrastructure because of the high-impact potential to disrupt essential functions. Given the unique requirements within the OT environments, specialized solutions that are purpose-built to monitor and secure OT systems are vital.

THE SOLUTION

The Dragos Platform enhances the cybersecurity posture in these critical environments through comprehensive OT and IOT asset and network visibility, threat detection, vulnerability management, and investigation and response capabilities.

KEY CAPABILITIES

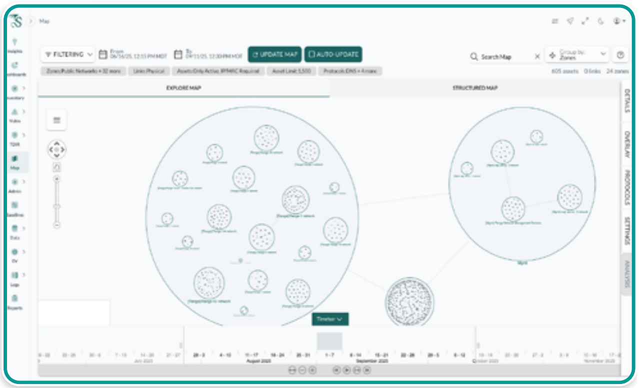
- Asset Visibility and Inventory
- OT Network Monitoring and Deep Packet Inspection
- Risk-Based Vulnerability Management
- Intelligence-Driven Threat Detection
- Investigation and Response
- Segmentation Policy Validation

WHY THE DRAGOS PLATFORM

- ✓ **OT-Native Platform** - Purpose-built specifically for OT and industrial control systems (ICS) environments.
- ✓ **Recognized Industry Leader** - Named a Leader in Gartner® Magic Quadrant™ for CPS Protection Platforms (2025).
- ✓ **Comprehensive Threat Intelligence** - Industry-leading OT cyber threat intelligence injected directly into the Platform.
- ✓ **Neighborhood Keeper Collective Defense** - Enables anonymous threat intelligence sharing across the OT community.
- ✓ **Monitoring & Visibility with OT Watch –** 24/7 platform coverage, with expert threat hunting, tuning, and hardening, led by Dragos.
- ✓ **Commitment to Customer Success** - Dedicated professional services and ongoing support ensure measurable cybersecurity outcomes.

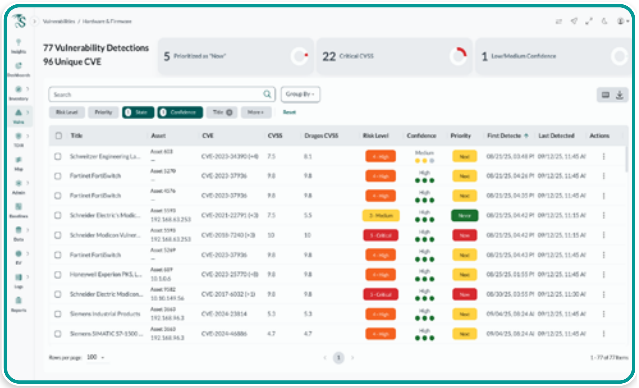
Key Features

OT Network Monitoring



Monitors network traffic to enable both cybersecurity and operations. The Platform performs deep packet inspection (DPI) to establish baselines and identify communication patterns. This enables a comprehensive understanding of the environment and allows users to visualize communications over time to provide a clear network topology.

Risk-Based Vulnerability Management



77 Vulnerability Detections
96 Unique CVE

5 Prioritized as "Now"

22 Critical CVSS

1 Low/Medium Confidence

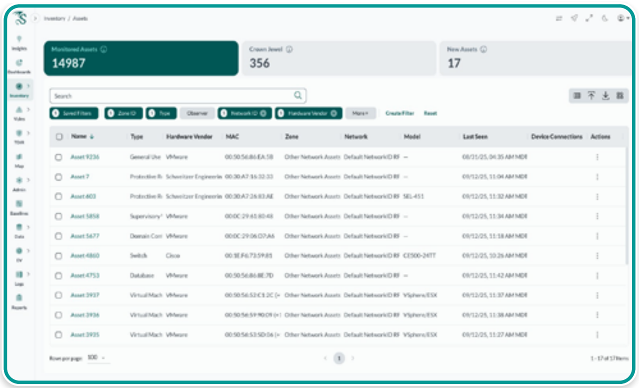
Title	Asset	CVE	CVSS	Dragos CVSS	Risk Level	Confidence	Priority	First Detecte	Last Detected	Actions
Schweitzer Engineering La...	Asset 603 –	CVE-2023-34390 (+8)	7.5	8.1	4 - High	Medium	Next	08/21/25, 03:48 PI	09/12/25, 11:45 A!	⋮
Fortinet FortiSwitch	Asset 1279 –	CVE-2023-37936	9.8	9.8	4 - High	High	Next	08/21/25, 04:26 PI	09/12/25, 11:45 A!	⋮
Fortinet FortiSwitch	Asset 4576	CVE-2023-37936	9.8	9.8	4 - High	High	Next	08/21/25, 04:35 PI	09/12/25, 11:45 A!	⋮
Schneider Electric's Modic...	Asset 5593 192.168.63.253	CVE-2021-22791 (+3)	7.5	5.5	3 - Medium	High	Never	08/21/25, 04:42 PI	09/12/25, 11:15 A!	⋮
Schneider Modicon Vulner...	Asset 5593 192.168.63.253	CVE-2018-7240 (+3)	10	10	5 - Critical	High	Now	08/21/25, 04:42 PI	09/12/25, 11:15 A!	⋮
Fortinet FortiSwitch	Asset 5269 –	CVE-2023-37936	9.8	9.8	4 - High	High	Next	08/21/25, 04:43 PI	09/12/25, 11:45 A!	⋮
Honeywell Experion PKS, L...	Asset 609 10.1.0.6	CVE-2023-25770 (+8)	9.8	9.8	4 - High	High	Next	08/25/25, 01:55 PI	09/12/25, 11:45 A!	⋮
Schneider Electric Modicon...	Asset 9582 10.10.149.56	CVE-2017-6032 (+1)	9.8	9.8	5 - Critical	High	Now	08/30/25, 03:55 PI	09/12/25, 11:30 A!	⋮
Siemens Industrial Products	Asset 2663 192.168.96.3	CVE-2024-23814	5.3	5.3	4 - High	High	Next	09/04/25, 08:24 A!	09/12/25, 11:45 A!	⋮
Siemens SIMATIC S7-1500 ...	Asset 2663 192.168.96.3	CVE-2024-46886	4.7	4.7	4 - High	High	Next	09/04/25, 08:24 A!	09/12/25, 11:45 A!	⋮

Rows per page: 100

1 - 77 of 77 items

Provides corrected, enriched, prioritized guidance that allows you to manage the full lifecycle of hardware, software, and OS vulnerabilities in your environment. With "Now, Next, Never" mitigation guidance, teams can prioritize resources, minimize downtime and mitigate risks. Guidance authored and updated by Dragos vulnerability analysts and incorporated back into the Platform to keep up with the changing threat landscape.

Asset Inventory



Monitored Assets
14987

Crown Jewel
356

New Assets
17

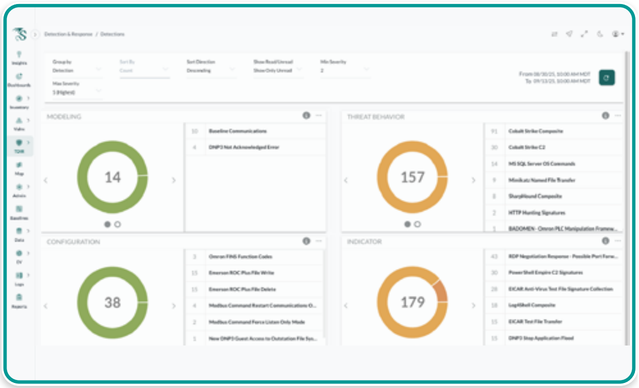
Name	Type	Hardware Vendor	MAC	Zone	Network	Model	Last Seen	Device Connections	Actions
Asset 9236	General Use	VMware	00:50:56:86:EA:5B	Other Network Assets	Default NetworkID RF	–	08/31/25, 04:35 AM MDT		⋮
Asset 7	Protective R	Schweitzer Engineerin	00:30:A7:16:32:33	Other Network Assets	Default NetworkID RF	–	09/12/25, 11:04 AM MDT		⋮
Asset 603	Protective R	Schweitzer Engineerin	00:30:A7:26:83:AE	Other Network Assets	Default NetworkID RF	SEL-451	09/12/25, 11:32 AM MDT		⋮
Asset 5858	Supervisory	VMware	00:0C:29:61:80:48	Other Network Assets	Default NetworkID RF	–	09/12/25, 11:34 AM MDT		⋮
Asset 5677	Domain Con	VMware	00:0C:29:06:D7:A6	Other Network Assets	Default NetworkID RF	–	09/12/25, 11:18 AM MDT		⋮
Asset 4860	Switch	Cisco	00:1E:F6:73:59:85	Other Network Assets	Default NetworkID RF	CE500-24TT	09/12/25, 10:26 AM MDT		⋮
Asset 4753	Database	VMware	00:50:56:86:8E:7D	Other Network Assets	Default NetworkID RF	–	09/12/25, 11:42 AM MDT		⋮
Asset 3937	Virtual Mach	VMware	00:50:56:52:C1:2C (+	Other Network Assets	Default NetworkID RF	VSphere/ESX	09/12/25, 11:37 AM MDT		⋮
Asset 3936	Virtual Mach	VMware	00:50:56:59:90:09 (+	Other Network Assets	Default NetworkID RF	VSphere/ESX	09/12/25, 11:38 AM MDT		⋮
Asset 3935	Virtual Mach	VMware	00:50:56:53:5D:06 (+	Other Network Assets	Default NetworkID RF	VSphere/ESX	09/12/25, 11:27 AM MDT		⋮

Rows per page: 100

1 - 17 of 17 items

Build a strong foundation with a complete, continuously updated OT asset inventory. The Dragos Platform delivers passive-first discovery, safe active collection when needed, and deep protocol analysis to build accurate visibility south of the firewall.

Intelligence-Driven Threat Detection



Group by: Detection
Sort By: Count
Sort Direction: Descending
Show Read/Unread: Show Only Unread
Min Severity: 2
Max Severity: 1 (Highest)

From 08/30/25, 10:00 AM MDT
To 09/13/25, 10:00 AM MDT

MODELING: 14

10	Baseline Communications
4	DNP3 Not Acknowledged Error

THREAT BEHAVIOR: 157

91	Cobalt Strike Composite
30	Cobalt Strike C2
14	MS SQL Server OS Commands
9	Mimikatz Named File Transfer
8	SharpHound Composite
2	HTTP Hunting Signatures
1	BADOMEN - Omron PLC Manipulation Framew...

CONFIGURATION: 38

3	Omron FINS Function Codes
15	Emerson ROC Plus File Write
15	Emerson ROC Plus File Delete
4	Modbus Command Restart Communications O...
2	Modbus Command Force Listen Only Mode
1	New DNP3 Guest Access to Outstation File Sys...

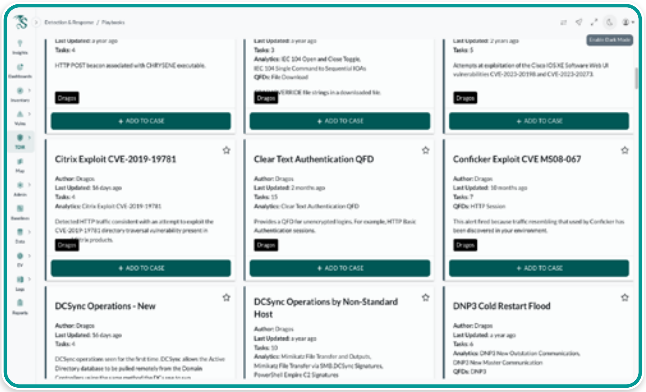
INDICATOR: 179

43	RDP Negotiation Response - Possible Port Forw...
30	PowerShell Empire C2 Signatures
28	EICAR Anti-Virus Test File Signature Collection
18	Log4Shell Composite
15	EICAR Test File Transfer
15	DNP3 Stop Application Flood

The Dragos Platform offers the leading threat detection capability in the industry. Rapidly pinpoint malicious activity with four types of threat detection – modeling, configuration, indicators, and behavioral detections. Dragos incorporates cyber threat intelligence continuously, enabling up-to-date and contextualized analytics to provide deeper detection of threats.

Key Features (cont.)

Investigation and Response



Last Updated: a year ago
Tasks: 4
HTTP POST beacon associated with CHRYSENE executable.
Dragos
+ ADD TO CASE

Last Updated: a year ago
Tasks: 3
Analytics: IEC 104 Open and Close Toggle, IEC 104 Single Command to Sequential IOAs
QFDs: File Download
VERRIDE file strings in a downloaded file.
Dragos
+ ADD TO CASE

Last Updated: 2 years ago
Tasks: 5
Attempts at exploitation of the Cisco IOS XE Software Web UI vulnerabilities CVE-2023-20198 and CVE-2023-20273.
Dragos
+ ADD TO CASE

Citrix Exploit CVE-2019-19781
Author: Dragos
Last Updated: 56 days ago
Tasks: 4
Analytics: Citrix Exploit CVE-2019-19781
Detected HTTP traffic consistent with an attempt to exploit the CVE-2019-19781 directory traversal vulnerability present in Citrix products.
Dragos
+ ADD TO CASE

Clear Text Authentication QFD
Author: Dragos
Last Updated: 2 months ago
Tasks: 15
Analytics: Clear Text Authentication QFD
Provides a QFD for unencrypted logins. For example, HTTP Basic Authentication sessions.
Dragos
+ ADD TO CASE

Conficker Exploit CVE MS08-067
Author: Dragos
Last Updated: 10 months ago
Tasks: 7
QFDs: HTTP Session
This alert fired because traffic resembling that used by Conficker has been discovered in your environment.
Dragos
+ ADD TO CASE

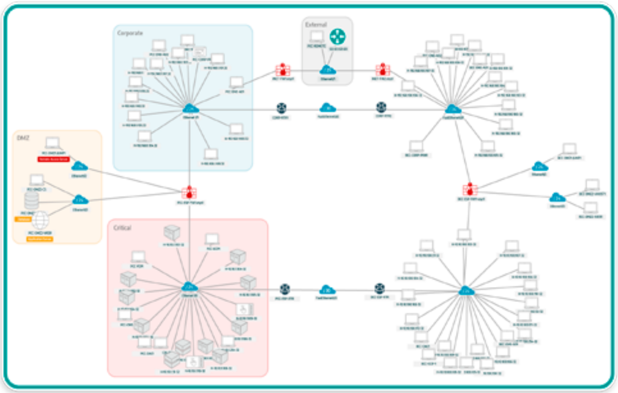
DCSync Operations - New
Author: Dragos
Last Updated: 56 days ago
Tasks: 4
DCSync operations seen for the first time. DCSync allows the Active Directory database to be pulled remotely from the Domain Controllers using the same method the DC's use to syn

DCSync Operations by Non-Standard Host
Author: Dragos
Last Updated: a year ago
Tasks: 10
Analytics: Mimikatz File Transfer and Outputs, Mimikatz File Transfer via SMB, DCSync Signatures, PowerShell Empire C2 Signatures

DNP3 Cold Restart Flood
Author: Dragos
Last Updated: a year ago
Tasks: 6
Analytics: DNP3 New Outstation Communication, DNP3 New Master Communication
QFDs: DNP3

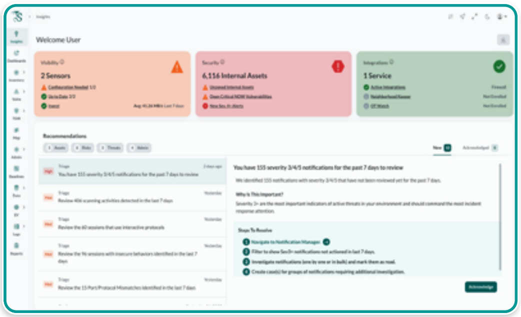
Dragos Platform users can easily create cases to initiate investigations by pulling in relevant activity logs, forensic data, threat intelligence reports, timeline views, and reference response playbooks written by Dragos experts for a comprehensive approach to investigating incidents and reducing crucial time to response.

Segmentation and Policy Validation



Dragos NP-View analyzes configuration of firewalls, switches, and routers to validate segmentation policies, map topologies and access routes, and evaluate firewall policies to streamline compliance reporting and improve cybersecurity posture.

INSIGHTS HUB



Welcome User

Visibility
2 Sensors
Configuration Needed 1/2
Up to Date 1/2
Ingest — Avg 45.26 MB/s Last 7 days

Security
6,116 Internal Assets
Unzoned Internal Assets
Open Critical NOW Vulnerabilities
New Sev. 4+ Alerts

Integrations
1 Service
Active Integrations — Firewall
Neighborhood Keeper — Not Enrolled
OT Watch — Not Enrolled

Recommendations
Assets · Risks · Threats · Admin — New · Acknowledged

High — Triage — 2 days ago — You have 155 severity 3/4/5 notifications for the past 7 days to review
Med — Triage — Yesterday — Review 406 scanning activities detected in the last 7 days
Med — Triage — Yesterday — Review the 60 sessions that use interactive protocols
Med — Triage — Yesterday — Review the 96 sessions with insecure behaviors identified in the last 7 days
Med — Triage — Yesterday — Review the 15 Port/Protocol Mismatches identified in the last 7 days

You have 155 severity 3/4/5 notifications for the past 7 days to review

We identified 155 notifications with severity 3/4/5 that have not been reviewed yet for the past 7 days.

Why Is This Important?

Severity 3+ are the most important indicators of active threats in your environment and should command the most incident response attention.

Steps To Resolve

1. Navigate to Notification Manager
2. Filter to show Sev3+ notifications not actioned in last 7 days.
3. Investigate notifications (one by one or in bulk) and mark them as read.
4. Create case(s) for groups of notifications requiring additional investigation.

Acknowledge

Your Central OT Security Dashboard

Unifies alerts, vulnerabilities, asset insights, operational status, and analyst guidance in one dashboard—your starting point to see what matters, prioritize exposures, accelerate investigations, and reduce risk.

KNOWLEDGE PACKS

Dragos pushes regular content updates to the Dragos Platform content via Knowledge Packs including:

- ✓ Detections and threat analytics for new and evolving threats to include threat activity groups, ransomware, malware, and targeted exploits.
- ✓ Vulnerability advisories, detections, and guidance to the industry's largest vulnerability database.
- ✓ Protocol characterizations including updated ICS, equipment, and vendor protocols to expand dissection.
- ✓ Playbooks to guide cyber analysts to enable response and threat hunting efforts.

THE DRAGOS PLATFORM OFFERS FLEXIBLE MONITORING TO ADDRESS CUSTOMER REQUIREMENTS

DRAGOS PLATFORM INPUTS

Sensor and Virtual Appliances:
Comprehensive passive monitoring via physical sensor appliances and virtual sensors, ensuring extensive coverage, minimal network disruption, and flexible deployments across diverse environments.

Active Collection with Dragos Agent:
Lightweight, purpose-built software executable deployed directly on Windows-based devices for active data collection. Discovers isolated or low-traffic assets, enriches asset inventories, and software and OS vulnerabilities matching.

Containerized Traffic Forwarding:
Lightweight Collector (LWC) deployed in containerized and edge computing environments captures east-west traffic locally, then deduplicates, filters, compresses, and forwards data to sensors.

Data and Project File Import
Import and enrich asset inventories from existing data sources, vendor files, and third-party tools.

INTEGRATIONS

Seamlessly integrates with leading firewall vendors such as Fortinet, Cisco, CheckPoint, Palo Alto Networks, SIEM systems like Microsoft Sentinel, endpoint solutions including CrowdStrike, and CMDB systems like ServiceNow, enhancing asset enrichment, threat detection, and response capabilities.

SITESTORE

Aggregates Dragos Sensor asset, vulnerability, and threat information across connected sensors, including key workflows.

CENTRALSTORE

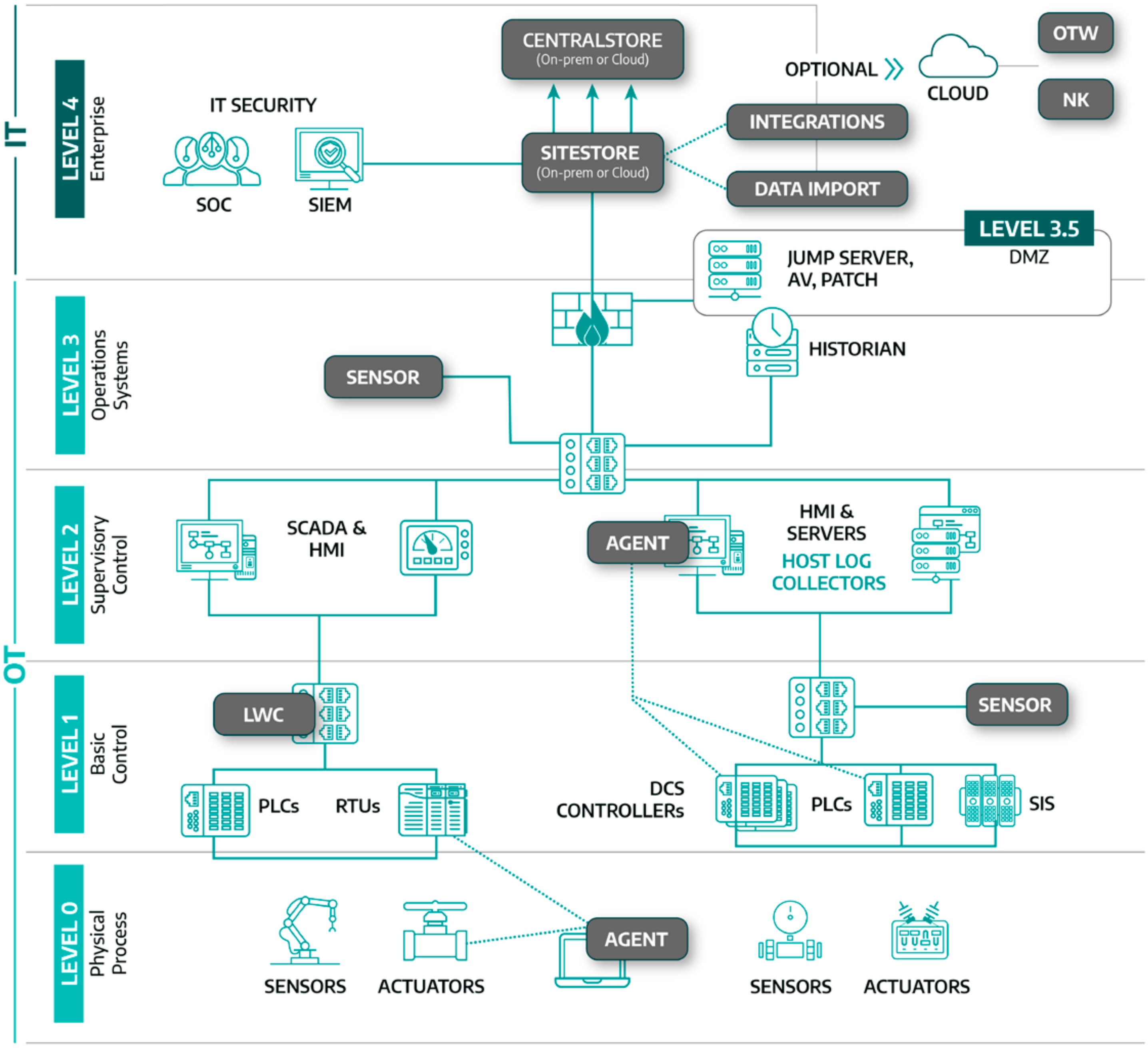
Optional component that offers SiteStore management enabling a central location for multi-enterprise aggregation, central dashboards, searching, and reporting.

DEPLOYMENT OPTIONS

Gain Visibility Through Flexible Monitoring

Preserve operational uptime with a "Do No Harm" monitoring approach. Industrial organizations need to monitor deep within the OT environment, at Levels 1, 2, 3, & 3.5 (the interface of OT/IT) of the Purdue Model.

THE DRAGOS PLATFORM DEPLOYMENT DIAGRAM



The Power of the Dragos Ecosystem

The Dragos Platform is supported by industry-leading expertise, meeting our customers where they are in their OT cybersecurity journey.

OT Watch

We put Dragos experts behind your Platform. Offered as scheduled threat hunts or as 24/7 managed platform coverage with OT Watch Complete, you get an OT security program that overcomes staffing constraints and delivers measurable outcomes sooner.

Neighborhood Keeper

An opt-in collective intelligence data network that enables Dragos Platform users to benefit from anonymously shared intelligence Neighborhood Keeper aggregates data and intelligence across organizations providing a view of threat activity and trends.

WorldView

Dragos fields the largest civilian OT-focused cyber threat intelligence operation. Adversary hunters research threat groups, their campaigns, and tactics. Vulnerability researchers conduct primary OT vulnerability discovery and analyze third-party vulnerabilities, providing OT risk and impact analysis. All findings are reported in Dragos WorldView and integrated into the Dragos Platform.

Supporting Services

Dragos offers critical services to operationalize an effective OT cyber defense. From technical account managers that help customers operationalize key platform use cases, to experienced OT incident responders, to consultants that help you assess your broader OT cyber defense architectures – we focus on helping you achieve your key OT cybersecurity outcomes.

Integrating with Security Operations

The Dragos Platform integrates with a wide variety of complementary technologies to enable customers to expand visibility and reduce time to response and recover across OT and IT environments while achieving maximum value from the investments made in their existing ecosystem including leading SIEMs, Firewalls, EDR and more.

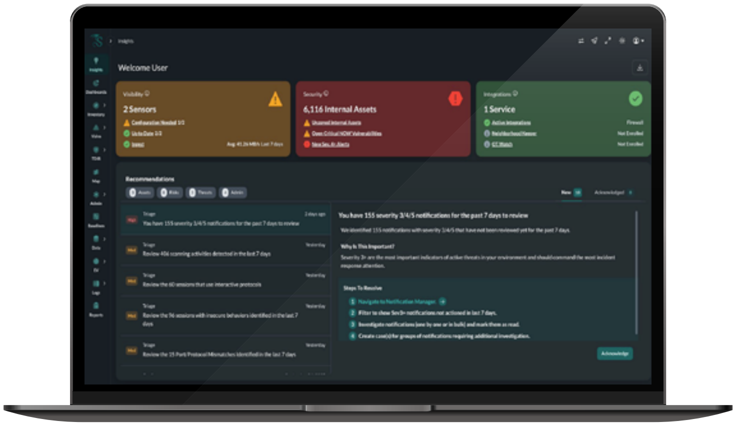
Industrial OEM Partnerships

Dragos partners with industrial OEMs to validate interoperability of the Dragos Platform within industrial environments and help with development of new content to improve visibility and detections. Furthermore, our industrial OEM partners provide additional value to customers by providing an option to procure from, deliver, and support Dragos Platform into their OT operations.

See the full list of Dragos Partners:
www.dragos.com/partners/

SEE THE POWER OF THE DRAGOS ECOSYSTEM

Get a Demo ↓



You have 155 severity 3/4/5 notifications for the past 7 days to review

Review 406 scanning activities detected in the last 7 days

Review the 60 sessions that use interactive protocols

Review the 96 sessions with insecure behaviors identified in the last 7 days

Review the 15 Port/Protocol Mismatches identified in the last 7 days

You have 155 severity 3/4/5 notifications for the past 7 days to review

We identified 155 notifications with severity 3/4/5 that have not been reviewed yet for the past 7 days.

Why Is This Important?

Severity 3+ are the most important indicators of active threats in your environment and should command the most incident response attention.

Steps To Resolve

1. Navigate to Notification Manager.
2. Filter to show Sev3+ notifications not actioned in last 7 days.
3. Investigate notifications (one by one or in bulk) and mark them as read.
4. Create case(s) for groups of notifications requiring additional investigation.

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