BROCHURE

DRAGOS®

PLATFORM

OT-Native Network Visibility & Security Monitoring

The Dragos Platform is the leading solution for securing industrial environments, engineered specifically for operational technology (OT) and industrial control systems (ICS). It provides comprehensive network visibility and security monitoring for OT environments, including OT systems, IT, IoT, and IIoT. The Dragos Platform supports operational continuity and resilience against cyber threats, safeguarding industrial infrastructure.

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 asset and network visibility, threat detection, vulnerability management, and investigation and response capabilities.

KEY ADVANTAGES

Asset Inventory and Network Monitoring

- Automate asset inventory in OT environments, including IT, IoT, and IIOT.
- Gain detailed network visibility and preserve uptime with non-invasive monitoring.

Vulnerability Management

- Corrected, enriched, prioritized guidance for managing the full lifecycle of vulnerabilities.
- "Now, Next, Never" guidance to reduce risk, minimize downtime, and prioritize resources.

Threat Detection and Response

- Detect cyber adversaries effectively with leading threat detection capabilities.
- Simplify investigations with proprietary CTI, forensic data, and expert-authored playbooks.
- Proactively detect threats and misconfigurations with Dragos OT Watch threat-hunting-as-a-service.

Services and Integrations

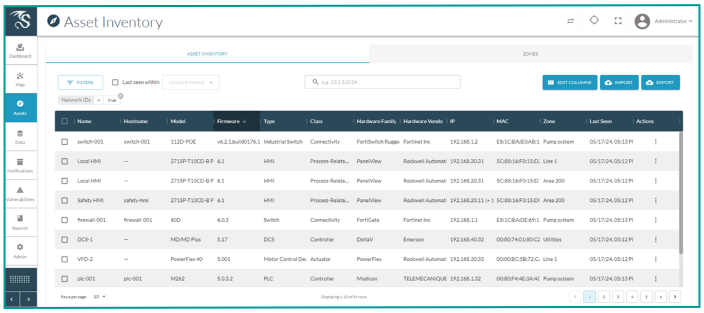
- Largest civilian OT CTI with Dragos WorldView providing in-depth threat analysis and reporting.
- Gain anonymized shared intelligence with Dragos Neighborhood Keeper.
- Comprehensive services to support the overall OT Security Program.
- Improve enterprise cybersecurity with extensive IT integrations.

DRAGOS PLATFORM DIFFERENTIATORS

- ✓ **Built for Industrial Environments**
- ✓ **OT-Enriched Vulnerability Management**
- ✓ **Industry-Leading Threat Detection**
- ✓ **Simplified Investigations**
- ✓ **Threat-Hunting-as-a-Service**
- ✓ **OT-CTI Research and Analytics Anonymized Shared Intelligence Access**

Key Features

Asset Inventory



□ Last seen within NO DATE RANGE

e.g. 10.1.5.0/24

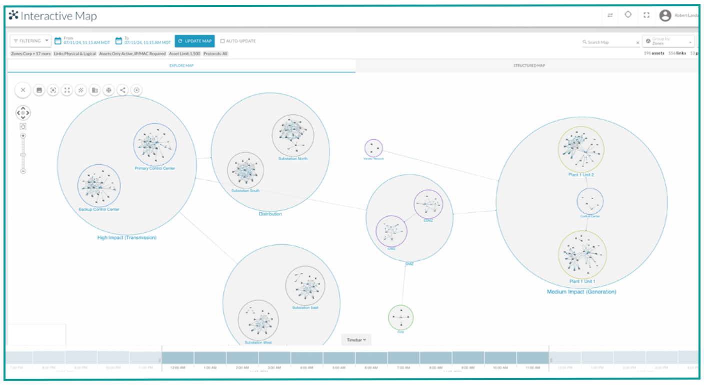
Network IDs = true

□	Name	Hostname	Model	Firmware ↓	Type	Class	Hardware Family	Hardware Vendo	IP	MAC	Zone	Last Seen	Actions
□	switch-001	switch-001	112D-POE	v6.2.1,build0176,1	Industrial Switch	Connectivity	FortiSwitch Rugge	Fortinet Inc	192.168.1.2	E8:1C:BA:B3:AB:1	Pump system	05/17/24, 05:13 PI	⋮
□	Local HMI	–	2715P-T10CD-B P	6.1	HMI	Process-Relate...	PanelView	Rockwell Automati	192.168.30.31	5C:88:16:F0:15:D:	Line 1	05/17/24, 05:12 PI	⋮
□	Local HMI	–	2715P-T10CD-B P	6.1	HMI	Process-Relate...	PanelView	Rockwell Automati	192.168.20.31	5C:88:16:F0:15:D:	Area 200	05/17/24, 05:12 PI	⋮
□	Safety HMI	safety-hmi	2715P-T10CD-B P	6.1	HMI	Process-Relate...	PanelView	Rockwell Automati	192.168.20.11 (+ 1	5C:88:16:F0:15:D(	Area 200	05/17/24, 05:12 PI	⋮
□	firewall-001	firewall-001	60D	6.0.3	Switch	Connectivity	FortiGate	Fortinet Inc	192.168.1.1	E8:1C:BA:DE:69:1	Pump system	05/17/24, 05:13 PI	⋮
□	DCS-1	–	MD/MD Plus	5.17	DCS	Controller	DeltaV	Emerson	192.168.40.32	00:80:74:01:80:C2	Utilities	05/17/24, 05:12 PI	⋮
□	VFD-2	–	PowerFlex 40	5.001	Motor Control De\	Actuator	PowerFlex	Rockwell Automati	192.168.30.33	00:00:BC:5B:72:C.	Line 1	05/17/24, 05:12 PI	⋮
□	plc-001	plc-001	M262	5.0.3.2	PLC	Controller	Modicon	TELEMECANIQUE	192.168.1.32	00:80:F4:4E:3A:4(	Pump system	05/17/24, 05:13 PI	⋮

Rows per page: 10 Displaying 1-10 of 54 rows

Automates discovery, management, and inventory across all assets within the OT environment (OT, IT, IoT, and IIoT). The Platform utilizes insights from hundreds of protocols, network data, and logs, laying a foundation for an effective OT cybersecurity program.

OT Network Visibility and Monitoring



From 07/11/24, 11:15 AM MDT To 07/15/24, 11:15 AM MDT

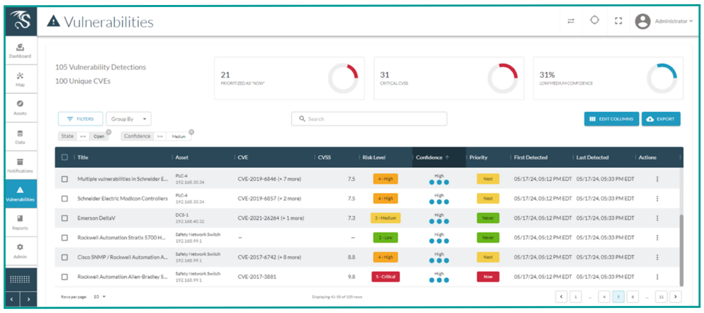
Zones:Corp + 17 more Links:Physical & Logical Assets:Only Active, IP/MAC Required Asset Limit:1,500 Protocols: All

Group by: Zones

196 assets 556 links

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



105 Vulnerability Detections
100 Unique CVEs

21 PRIORITIZED AS "NOW"

31 CRITICAL CVSS

31% LOW/MEDIUM CONFIDENCE

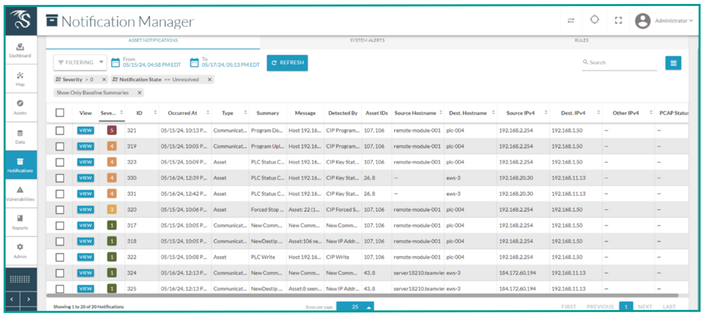
State == Open Confidence >= Medium

□	Title	Asset	CVE	CVSS	Risk Level	Confidence ↑	Priority	First Detected	Last Detected	Actions
□	Multiple vulnerabilities in Schneider E...	PLC-4 192.168.30.34	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-4 192.168.30.34	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-1 192.168.40.32	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 192.168.99.1	–	–	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 192.168.99.1	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 192.168.99.1	CVE-2017-3881	9.8	5 - Critical	High ●●●	Now	05/17/24, 05:12 PM EDT	05/17/24, 05:33 PM EDT	⋮

Rows per page: 10 Displaying 41-50 of 105 rows

Provides corrected, enriched, prioritized guidance that allows you to manage the full lifecycle of vulnerabilities in your environment, with "now, next, never" mitigation guidance to reduce risk, minimize downtime, and prioritize cybersecurity resources. Guidance is consistently updated by Dragos CTI team and incorporated back into the Platform to keep up with the changing threat landscape.

Intelligence-Driven Threat Detection



From 05/15/24, 04:58 PM EDT To 05/17/24, 05:13 PM EDT

Severity > 0 Notification State == Unresolved

Show Only Baseline Summaries

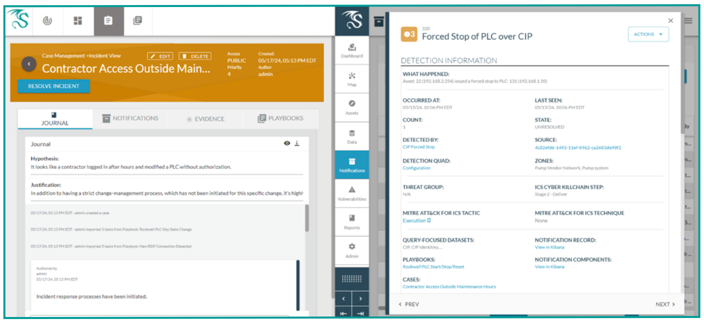
□	View	Seve...	ID	Occurred At	Type	Summary	Message	Detected By	Asset IDs	Source Hostname	Dest. Hostname	Source IPv4	Dest. IPv4	Other IPv4	PCAP Statu
□	VIEW	5	321	05/15/24, 10:13 P...	Communicat...	Program Do...	Host 192.16...	CIP Program...	107, 106	remote-module-001	plc-004	192.168.2.254	192.168.1.50	–	–
□	VIEW	4	319	05/15/24, 10:05 P...	Communicat...	Program Upl...	Host 192.16...	CIP Program...	107, 106	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 Stat...	107, 106	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 Stat...	26, 8	–	ews-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 Stat...	26, 8	–	ews-3	192.168.20.30	192.168.11.13	–	–
□	VIEW	3	320	05/15/24, 10:06 P...	Asset	Forced Stop ...	Asset: 22 (1...	CIP Forced S...	107, 106	remote-module-001	plc-004	192.168.2.254	192.168.1.50	–	–
□	VIEW	1	317	05/15/24, 10:05 P...	Communicat...	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, 10:05 P...	Communicat...	NewDestIp ...	Asset:106 se...	New IP Addr...	107, 106	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...	Communicat...	New Comm...	New Comm...	New Comm...	43, 8	server18210.teamvie	ews-3	184.172.60.194	192.168.11.13	–	–
□	VIEW	1	325	05/16/24, 12:13 P...	Communicat...	NewDestIp ...	Asset:8 seen...	New IP Addr...	43, 8	server18210.teamvie	ews-3	184.172.60.194	192.168.11.13	–	–

Showing 1 to 20 of 20 Notifications Rows per page 25 1

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



Contractor Access Outside Main...

Access: PUBLIC
Priority: 4
Created: 05/17/24, 05:13 PM EDT
Author: admin

Journal

Hypothesis:
It looks like a contractor logged in after hours and modified a PLC without authorization.

Justification:
In addition to having a strict change-management process, which has not been initiated for this specific change, it's highl

05/17/24, 05:13 PM EDT - admin created a case

05/17/24, 05:13 PM EDT - admin imported 3 tasks from Playbook: Rockwell PLC Key State Change

05/17/24, 05:13 PM EDT - admin imported 5 tasks from Playbook: New RDP Connection Detected

Authored by
admin
05/17/24, 05:13 PM EDT

Incident response processes have been initiated.

3 320 Forced Stop of PLC over CIP

DETECTION INFORMATION

WHAT HAPPENED:
Asset: 22 (192.168.2.254) issued a forced stop to PLC: 131 (192.168.1.50)

OCCURRED AT: 05/15/24, 10:06 PM EDT
LAST SEEN: 05/15/24, 10:06 PM EDT
COUNT: 1
STATE: UNRESOLVED
DETECTED BY: CIP Forced Stop
SOURCE: 4c82efd6-1492-11ef-8962-ca2683de98f2
DETECTION QUAD: Configuration
ZONES: Pump Vendor Network, Pump system
THREAT GROUP: N/A
ICS CYBER KILLCHAIN STEP: Stage 2 - Deliver
MITRE ATT&CK FOR ICS TACTIC: Execution
MITRE ATT&CK FOR ICS TECHNIQUE: None
QUERY-FOCUSED DATASETS: CIP, CIP Identities, ...
NOTIFICATION RECORD: View in Kibana
PLAYBOOKS: Rockwell PLC Start/Stop/Reset
NOTIFICATION COMPONENTS: View in Kibana
CASES: Contractor Access Outside Maintenance Hours

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.

KNOWLEDGE PACKS

Stay Up to Date with Regular Content Updates

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.**

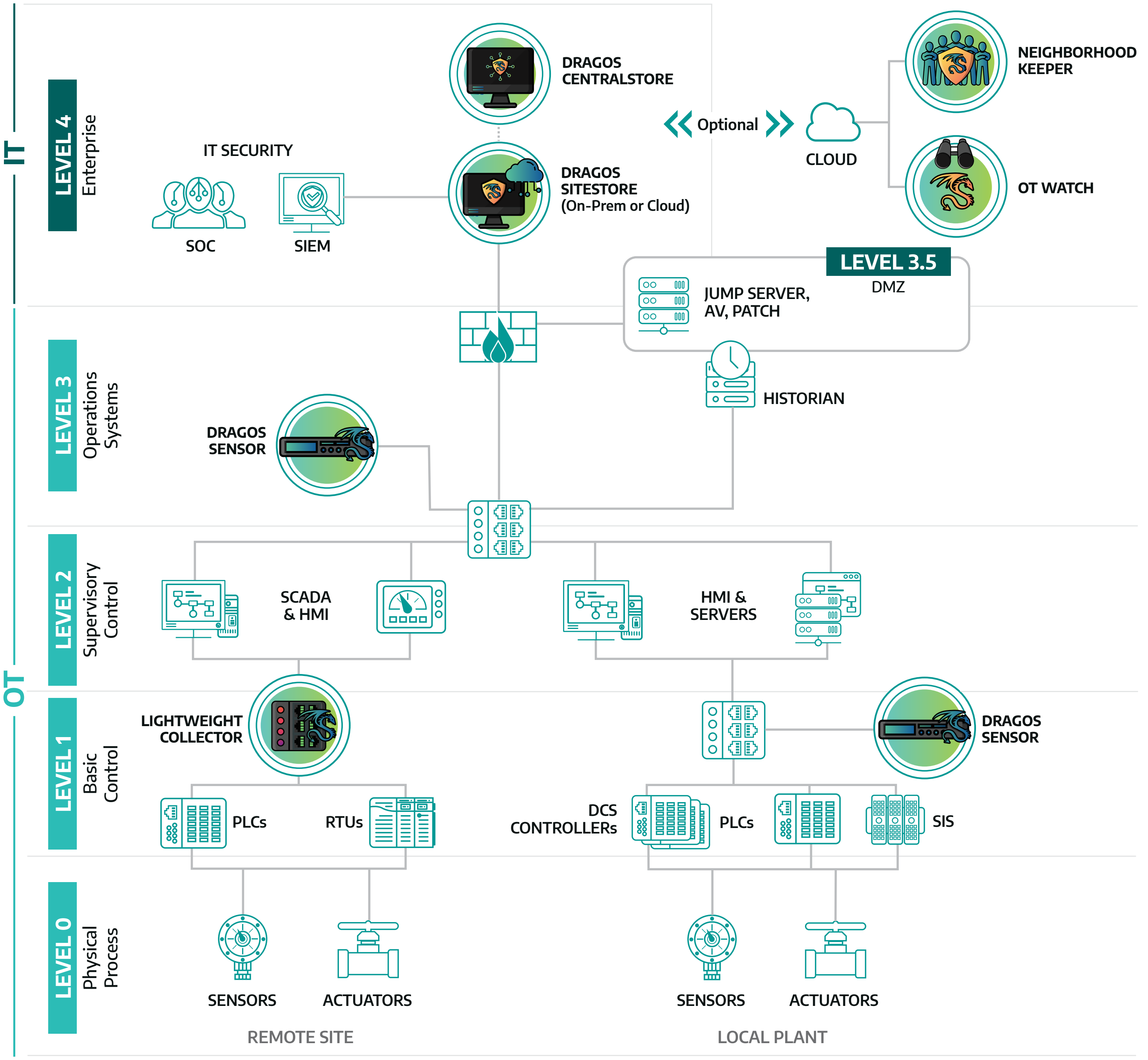
> “With the visibility provided by the Dragos Platform, automated monitoring capabilities alert the security team to potentially malicious behavior between assets and communications, so they can rapidly investigate and respond before attackers can progress.”
>
> — OIL AND GAS CISO —

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 DRAGOS PLATFORM OFFERS FLEXIBLE MONITORING TO ADDRESS CUSTOMER REQUIREMENTS

DRAGOS PLATFORM INPUTS

Sensor and Virtual Appliances:

Dragos Sensors provides comprehensive passive monitoring through both physical sensor appliances and virtual sensors, ensuring extensive coverage, minimal network disruption, and the flexibility of virtual deployment.

Containerized Traffic Forwarding:

Utilize Dragos Lightweight Collector for containerized and edge computing environments to capture east-west traffic locally, then deduplicates, filters, compresses, and forwards network traffic to a Dragos Sensor for dissection.

Data and Project File Import

Enrich the existing asset inventory or generate new assets via data import, project vendor and configuration files, and other third-party sources.

INTEGRATIONS

The Dragos Platform seamlessly integrates with your existing security vendors to provide asset enrichment and enhance overall vulnerability management, threat detection, and response capabilities. Many Dragos customers maximize security by integrating the Platform with leading firewall vendors like Fortinet, Cisco, CheckPoint, and Palo Alto Networks, alongside endpoint solutions from CrowdStrike and CMDB systems like ServiceNow.

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.

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

Threat-Hunting-as-a-Service provides advanced industrial threat hunting for Dragos Platform customers delivered by industry leading ICS security practitioners. OT Watch is the only OT threat hunting service in the market.

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.

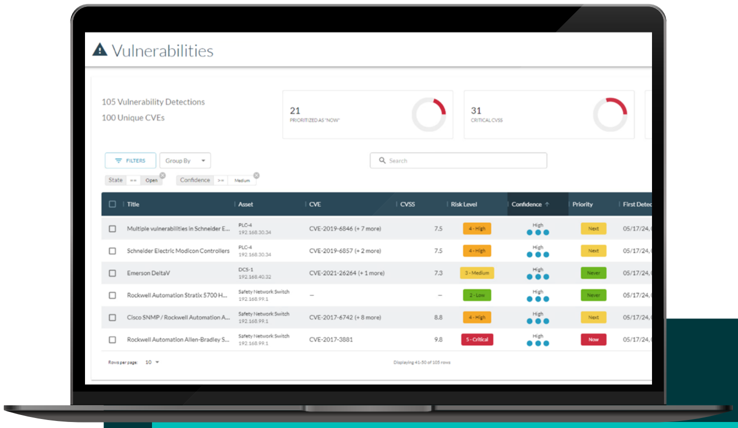
Integrating with Security Operations

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:
https://www.dragos.com/partners/



Vulnerabilities

105 Vulnerability Detections
100 Unique CVEs

21
PRIORITIZED AS "NOW"

31
CRITICAL CVSS

☐	Title	Asset	CVE	CVSS	Risk Level	Confidence	Priority	First Detec
☐	Multiple vulnerabilities in Schneider E...	PLC-4 192.168.30.34	CVE-2019-6846 (+ 7 more)	7.5	4 - High	High ●●●	Next	05/17/24,
☐	Schneider Electric Modicon Controllers	PLC-4 192.168.30.34	CVE-2019-6857 (+ 2 more)	7.5	4 - High	High ●●●	Next	05/17/24,
☐	Emerson DeltaV	DCS-1 192.168.40.32	CVE-2021-26264 (+ 1 more)	7.3	3 - Medium	High ●●●	Never	05/17/24,
☐	Rockwell Automation Stratix 5700 H...	Safety Network Switch 192.168.99.1	–	–	2 - Low	High ●●●	Never	05/17/24,
☐	Cisco SNMP / Rockwell Automation A...	Safety Network Switch 192.168.99.1	CVE-2017-6742 (+ 8 more)	8.8	4 - High	High ●●●	Next	05/17/24,
☐	Rockwell Automation Allen-Bradley S...	Safety Network Switch 192.168.99.1	CVE-2017-3881	9.8	5 - Critical	High ●●●	Now	05/17/24,

Rows per page: 10

Displaying 41-50 of 105 rows

SEE THE POWER OF THE DRAGOS ECOSYSTEM

Get a Demo

DRAGOS
SAFEGUARDING CIVILIZATION

COMMUNITY DEFENSE

DRAGOS PLATFORM

OT THREAT INTELLIGENCE

OT EXPERT SERVICES

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

𝕏 @DragosInc in @Dragos, Inc.