DRAGOS®
PLATFORM

OT CYBERSECURITY TECHNOLOGY THAT BRINGS VISIBILITY, DETECTION, AND RESPONSE TO YOUR INDUSTRIAL OPERATIONS

OVERVIEW

The Dragos Platform is operational technology (OT) cybersecurity technology that delivers unmatched visibility of your industrial control system (ICS) assets and communications. It rapidly pinpoints threats through intelligence-driven analytics, identifies and prioritizes vulnerabilities, and provides best-practice playbooks to guide teams as they investigate and respond to threats before they cause significant impact to your operations, processes, or people.

Codified with the expertise of the industry's largest, most experienced team of ICS/OT practitioners, the Dragos Platform ensures your security team is armed with the most up-to-date technology and intelligence to combat the world's most sophisticated industrial adversaries.

KEY BENEFITS

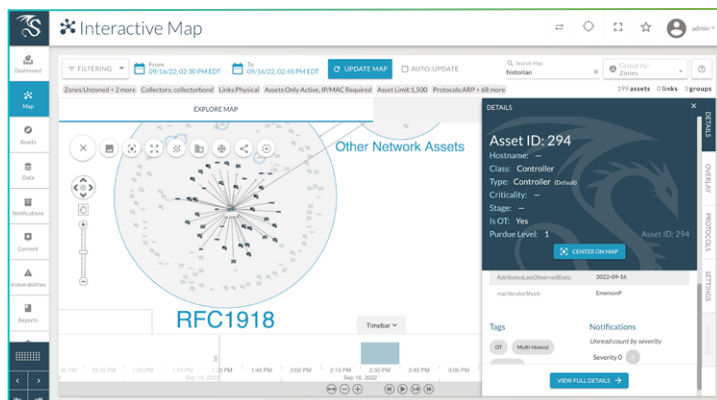**SECURELY ACCELERATE** DIGITAL TRANSFORMATION

MANAGE RISK TO PROTECT CORE BUSINESS

**EMPOWER** AUDIT AND COMPLIANCE PROGRAM ADHERENCE

KEY FEATURES

ASSET VISIBILITY & NETWORK MONITORING

Deep Contextual Insight for Industrial Cybersecurity Teams

- ☑ See ICS/OT network traffic and asset communication in depth

- ☑ Identify normal vs. abnormal operations with timeline views and baseline deviations

- ☑ Asset lifecycle management with zoning by location, role, type, or subnets

- ☑ Discover rich device details, including vendor, firmware, model, and more
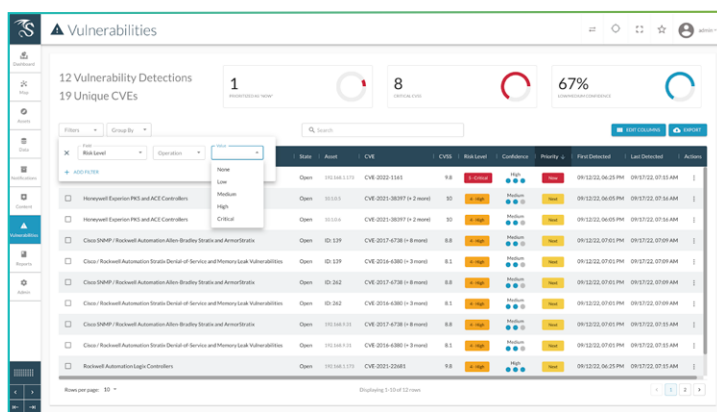
FULL CYCLE VULNERABILITY MANAGEMENT

Purpose Built for ICS/OT

- ☑ Risk levels that the Dragos Threat Intelligence team validates, enriches, and updates with real-world context, independent of CVSS scores

- ☑ Clear guidance on where to start with simple "Now, Next, Never" ratings

- ☑ Choose whether to accept, mitigate, or remediate vulnerability risk - individually or in bulk, for life-cycle disposition

- ☑ Built-in confidence ratings for each

KEY FEATURES
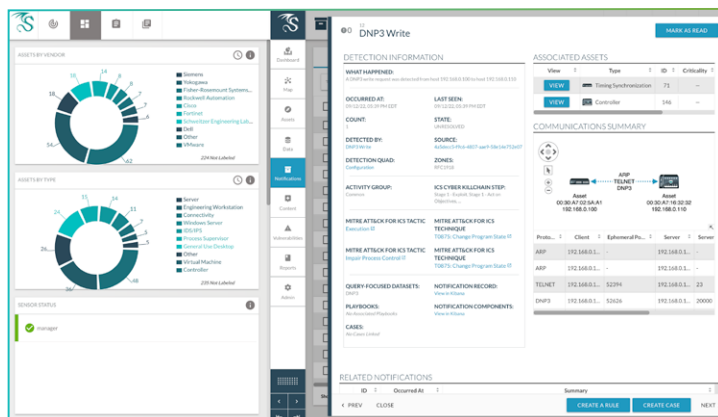
INDUSTRY LEADING THREAT ANALYTICS

Mapped to MITRE ATT&CK for ICS

- ☑ Gain continuous threat monitoring using latest behavior-based analytics created by Dragos Threat Intelligence

- ☑ See configuration, modeling, indicator, and threat detections from a single dashboard

- ☑ View threat levels and prioritize by severity

- ☑ Receive in-depth alerts with context of adversary tactics, techniques, and procedures (TTPs) mapped to MITRE ATT&CK for ICS
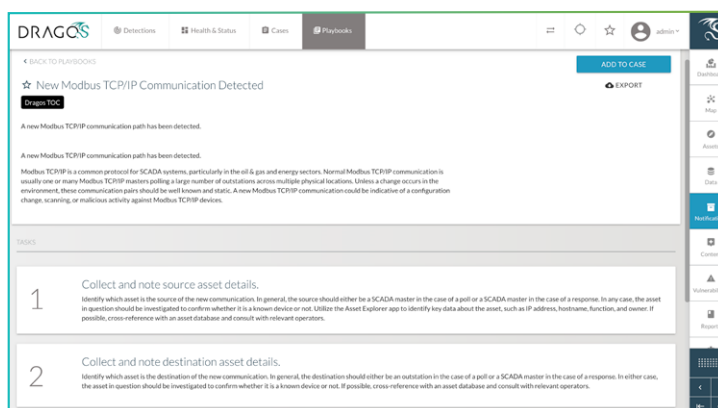
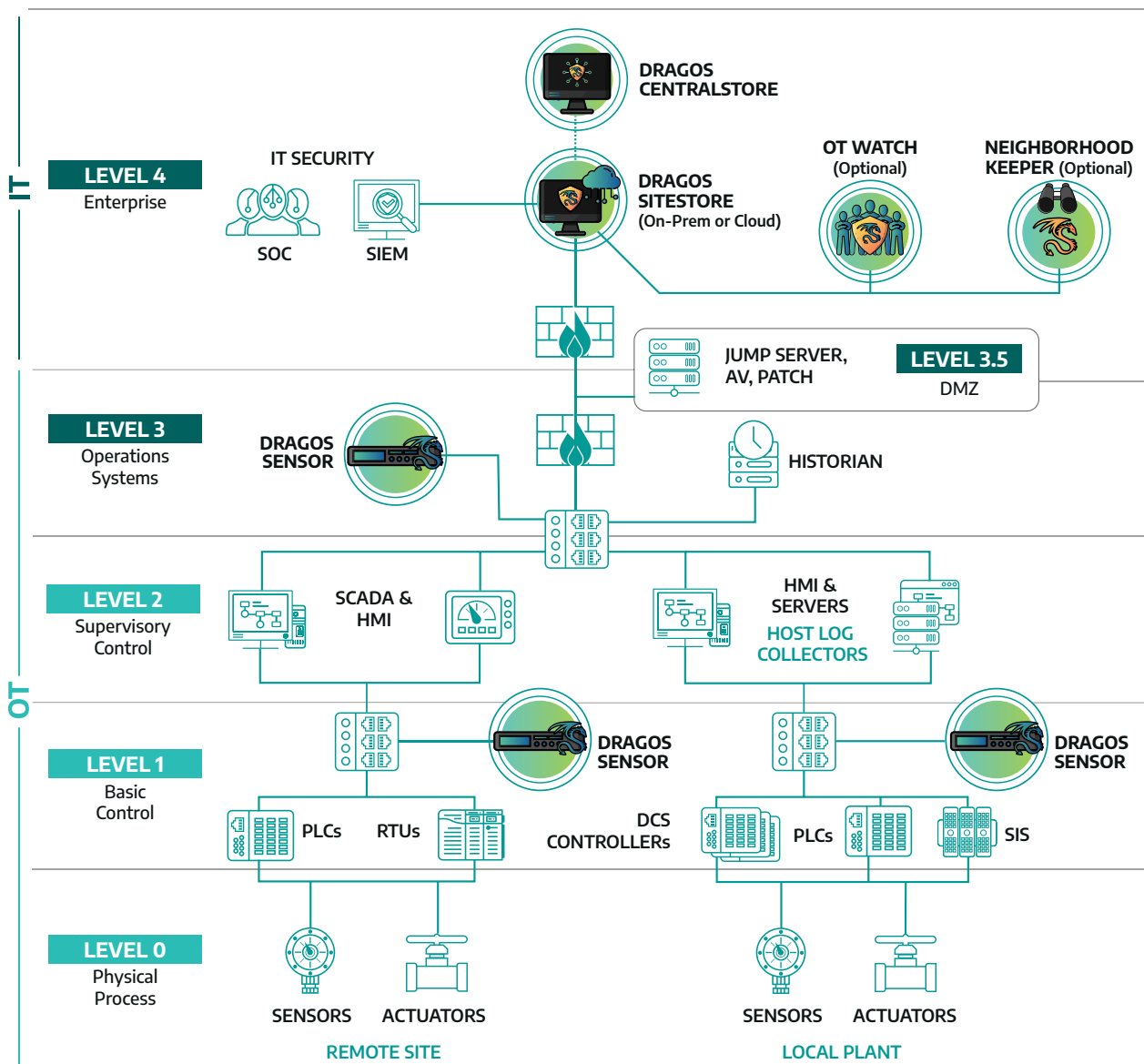## CYBER ANALYST-FOCUSED WORKBENCH

With Easy to Follow Investigation Playbooks

- ☑ Support incident response through cross-team collaboration and case management

- ☑ Use step-by-step investigation playbooks authored by Dragos experts

- ☑ Improve investigation efficiency with in-depth asset information and custom search information via Dragos Query-Focused Datasets

DRAGOS PLATFORM DEPLOYMENT

The Dragos Platform is continually updated with the latest threat intelligence based on Dragos front-line experience to keep your team one step ahead of adversaries. It's the most effective and the most efficient platform available today for industrial cybersecurity.

THE DRAGOS
PLATFORM DEPLOYMENT DIAGRAM

DRAGOS CENTRALSTORE

LEVEL 4
Enterprise

IT SECURITY

SOC   SIEM

DRAGOS SITESTORE (On-Prem or Cloud)

OT WATCH (Optional)

NEIGHBORHOOD KEEPER (Optional)

IT

JUMP SERVER, AV, PATCH

LEVEL 3.5
DMZ

LEVEL 3
Operations Systems

DRAGOS SENSOR

HISTORIAN

LEVEL 2
Supervisory Control

SCADA & HMI

HMI & SERVERS

HOST LOG COLLECTORS

OT

LEVEL 1
Basic Control

DRAGOS SENSOR

DRAGOS SENSOR

PLCs   RTUs

DCS CONTROLLERs

PLCs   SIS

LEVEL 0
Physical Process

SENSORS   ACTUATORS

SENSORS   ACTUATORS

REMOTE SITE

LOCAL PLANT

FLEXIBLE DEPLOYMENT

The Dragos Platform offers flexible deployment options for both physical and virtualized environments, whether on-premises and cloud-based.

DRAGOS CENTRALSTORE

- ☑ Enterprise-scale OT visibility, detection, and response.
- ☑ Multi-site, multi-organization Dragos Platform architecture.
- ☑ Consistent, centralized risk management and reporting.

DRAGOS SITESTORE

- ☑ Available in both hardware appliance or virtualized versions.
- ☑ Central management and reporting console for distributed Dragos sensors.

DRAGOS SENSORS

- ☑ Available as hardware appliance with ruggedized options or virtualized.
- ☑ Gathers and processes SPAN port traffic from 25Mbps to 1Gbps.

EXTENSIVE PROTOCOL & VENDOR SUPPORT

- ☑ Extensive list of OT/IT protocols continuously updated based on customer requirements. For current list, click here.
- ☑ Vendor support for Rockwell, Siemens, Schneider, Yokogawa, Honeywell, GE, Emerson, SEL, ABB, and more.

DRAGOS PLATFORM FEATURES & BENEFITS

FEATURES	Dragos Platform	Dragos Platform + Neighborhood Keeper	Dragos Platform + OT Watch (Managed Service)
Visualization of ICS/OT asset communications, threats, vulnerabilities, and anomalies	✓	✓	✓
Visualization of ICS/OT assets, network communications, vulnerabilities, and threats	✓	✓	✓
Threat analytics based on attacker TTPs mapped against MITRE ATT&CK for ICS detections	✓	✓	✓
Full analyst workbench with guided investigation playbooks and Query-Focused Datasets	✓	✓	✓
Regular delivery of new analytics, Indicators of Compromise, asset and device characterizations, and playbooks via Dragos Knowledge Packs	✓	✓	✓
Flexible deployment options including hardware appliances or virtualized, on premises or cloud-based	✓	✓	✓
Integrations with Crowdstrike, Splunk, QRadar, Fortinet, ServiceNow, OSIsoft Pi Historian, LogRythym, Syslog, and more	✓	✓	✓
Vulnerability management designed for OT with CVSS enrichment, risk level corrections, and clear guidance on "Now, Next, Never" prioritization	✓	✓	✓
Collective-defense capability to allow the sharing of insights and detections with other trusted participants while protecting their identity	✓	✓	✓
Enable direct communication to participants from trusted industry partners such as Information Sharing and Analysis Centers (ISACs)	—	✓	—
Receive curated intelligence from Trusted Advisers such as ISACs	—	✓	—
Recurring environmental checkups and Dragos Platform tuning	—	—	✓
Expert-driven alert prioritization and triage support	—	—	✓
Automated weekly reports summarizing threat hunting activities, outcomes from notification triage, and recommendations to protect and harden your environment	—	—	✓
Routine threat hunts based off latest Dragos adversary intelligence	—	—	✓
Proactive threat hunts based on Dragos intelligence, emerging threats and industry security events	—	—	✓

To learn more about the Dragos Platform or to request a demo, contact sales@dragos.com.

WWW.DRAGOS.COM/PLATFORM

TO LEARN MORE ABOUT DRAGOS AND OUR TECHNOLOGY, SERVICES, AND THREAT INTELLIGENCE, PLEASE VISIT WWW.DRAGOS.COM.

sales@dragos.com

@DragosInc

DRAGOS®

Dragos Global Headquarters
1745 Dorsey Road | Suite R
Hanover, MD 21076
855.372.4670