DRAGOS PLATFORM OVERVIEW

OVERVIEW

The Dragos Platform is an industrial control system (ICS) cybersecurity technology that provides ICS defenders with unprecedented visibility of their assets and communications, knowledge of threats through intelligence-driven analytics, and prescriptive guidance via playbooks to investigate and respond to incidents. The Dragos Platform codifies the expertise of the industry's most trusted ICS cybersecurity team to provide ICS defenders the capabilities needed for scalable, efficient, and effective defenses.

Protection Across the Entire ICS Cybersecurity Framework

The Dragos Platform provides all the necessary capabilities to monitor and defend ICS environments across the entire ICS cybersecurity framework. The modular design allows for staged deployment to address immediate and longer-term needs. It operates as an OT security incident and event management system (SIEM) and can be deployed in a security operations center (SOC) model.

IDENTIFY
Automated asset and communications protocol discovery and enrichment across the network to identify how assets interact

DETECT
Asset and protocol classification with behavioral attributes; set baselines for differential analysis and risk assessment

PROTECT
Extended threat detection includes behavioral analytics and threat hunting guidance through focused queries, reports, and searches

RESPOND
Expert-driven playbooks and case management to facilitate the most effective and efficient incident response and resolution

RECOVER
System learning and feedback to improve response and ongoing monitoring

INDUSTRIAL ASSET ID, THREAT DETECTION, & RESPONSE SOFTWARE BUILT BY ICS CYBERSECURITY EXPERTS

In-depth Situational Awareness via Asset Identification & Visualization

- Deep packet inspection of ICS protocols, network traffic, assets, logs, and historians
- View historical changes to assets across timelines for more accurate baselines
- Unique asset zoning and mapping abilities for efficient environment visibility

Accurate Threat Detection via Threat Analytics

- Analytics derived from adversary tactics, techniques, and procedures
- Reduce false positives and alert fatigue
- In-depth context of threats and how to respond

Rapid Response via Investigation Playbooks

- Step-by-step investigation guidance
- Increase efficiency of response with Dragos best practices
- Lower the barrier of analyst experience to respond to ICS threats

WHY CHOOSE THE DRAGOS PLATFORM?

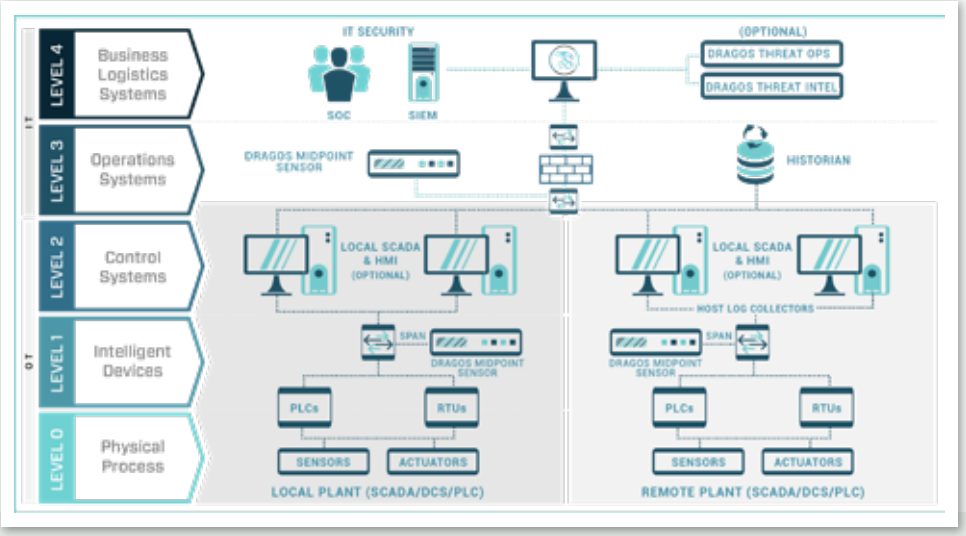
Highly scalable and designed to monitor up to hundreds of thousands of assets across multiple sites at high speeds

Codifies the Dragos team's in-depth knowledge of adversary tradecraft into threat behavior analytics to significantly enhance threat detection

Broad coverage of data sources, a workbench to triage alerts, and investigation playbooks to provide step-by-step guidance and supplement your security team's experience

DPI of ICS protocols, host logs, controller logs, data historian alerts, and more provide the most thorough analysis and understanding possible

PLATFORM DEPLOYMENT AND SYSTEM REQUIREMENTS



DRAGOS SITESTORE

- CPU / 32 GB RAM
- 2 TB SSD Hard Drive
- Deployable on-premise or in cloud (AWS, Azure, Google)

DRAGOS MIDPOINT SENSORS

- Hardware appliance deployed at sites
- Gathers and processes SPAN port traffic from 100Mbps to 1Gbps

SUPPORTED VENDOR PROTOCOL SAMPLES

- Rockwell, Siemens, Schneider, Yokogawa, Honeywell, GE

LICENSING

- Hardware appliance – initial fee
- Annual license fee for software – CAPEX options available
- Support included in license fee

DRAGOS PLATFORM FEATURES AND BENEFITS

FEATURES	BENEFITS
Asset Discovery, Enrichment, Classification, and Exploration	• Significantly reduce time to identify and inventory all assets and traffic on your network • System-generated asset maps and reports provide consistent, time-driven views that are accurate, up-to-date, and thorough • Automatic classification of assets based on behavior • Set one or more baselines and get notifications when specific changes or anomalies occur in the environment over time • Recognize new or rogue assets as they appear; identify assets that have disappeared from the network
Threat Detection and Behavioral Analytics	• Powered by human-based intelligence that identifies adversary tradecraft and campaigns • No bake-in or tuning period required; threat behavior analytics work immediately upon deployment • Detect threats not simply as anomalies to investigate, but with context that guides effective response
Case Management and Workflow	• Notification filtering provides a risk-based approach to management • Playbooks codify incident response and best-practice workflows developed by Dragos experts • Manage incidents and cases from the same console across entire team
Reporting and Dashboards	• Clear Indicator of Compromise (IOC) reports guide attention to vulnerable assets • Easily monitor case, notification, and analyst activity, as well as system-level health and status
Third Party Integrations	• Splunk, QRadar, OSIsoft Pi Historian, LogRythym, Syslog, Windows Host Logs

To learn more about the Dragos Platform, please contact sales@dragos.com or visit dragos.com/platform