INDUSTRIAL CYBERSECURITY PLATFORM

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

DRAGOS PLATFORM 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.

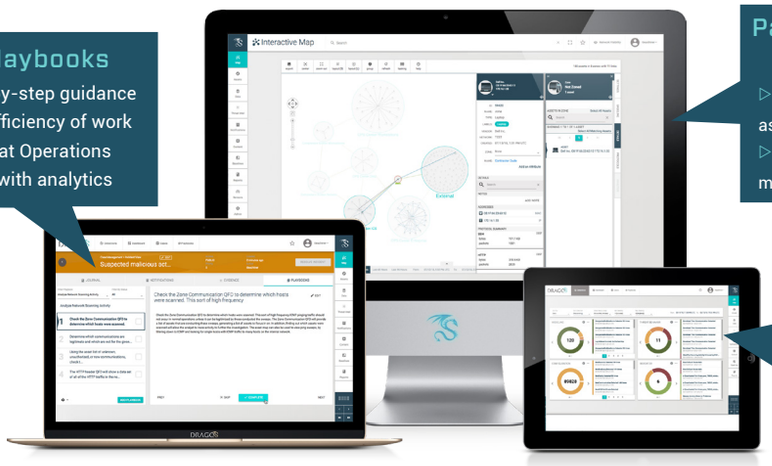
IDENTIFY ASSETS | Deep packet inspection (DPI) of ICS protocols, traffic, and asset characterizations, ability to consume host logs and controller events, and integrations with ICS assets such as data historians provide a complete view of ICS environments

DETECT THREATS | Complex characterizations of adversary tactics, techniques, and procedures through threat behavior analytics pinpoint malicious activity on ICS networks and provide in-depth context to alerts

RESPOND | Expert-authored investigation playbooks and case management guide defenders step-by-step through the investigation process to enable independence and transfer knowledge from our team to ICS defenders

Investigation Playbooks

- Provide defenders step-by-step guidance
- Increase effectiveness/efficiency of work
- Authored by Dragos Threat Operations Center & uniquely paired with analytics



Passive Asset Identification & Visualization

- DPI analyzes ICS protocols, network traffic, assets, logs, & historians
- View changes to assets across timelines for more accurate baselines

Threat Behavior Analytics

- Pinpoint malicious behavior
- ICS adversary behaviors tracked by the Dragos Intel Team and characterized into analytics
- Reduce false positives in comparison to anomaly detection

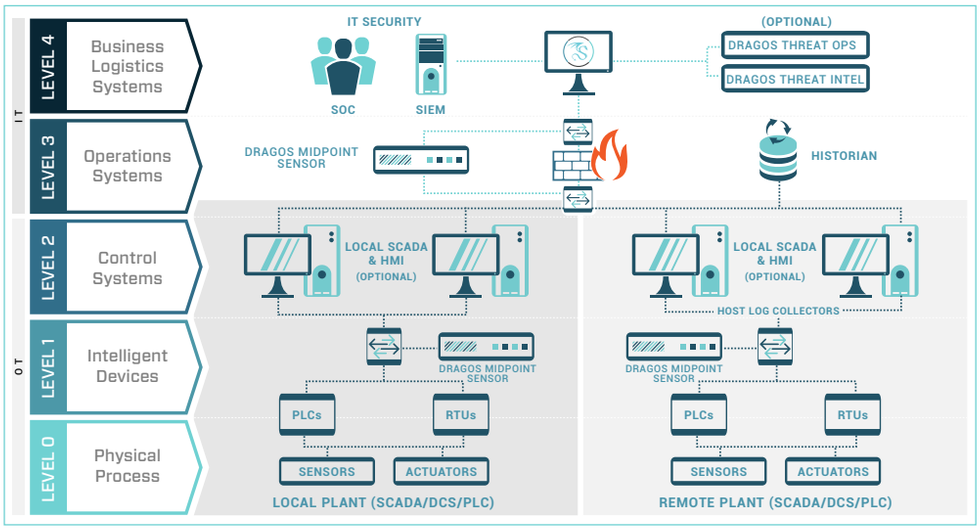
WHY CHOOSE THE DRAGOS PLATFORM?

- 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 that significantly enhance threat detection
- Broad coverage of data sources, a workbench to investigate alerts, and investigation playbooks to guide analysts step-by-step and supplement security teams' experience
- Deep packet inspection of ICS protocols, host logs, controller logs, data historian alerts, and more provide the most thorough analysis and understanding possible

INDUSTRIAL CYBERSECURITY PLATFORM

The Dragos Platform contains all the necessary capabilities to monitor and defend ICS environments. It combines the functionality of an OT security incident and event management system (SIEM), network detection and anomaly system, and incident response platform with the experience and intelligence of the Dragos team.

PLATFORM DEPLOYMENT ARCHITECTURE



DRAGOS SITESTORE

- 2x 12c CPU
- 128GB Memory
- 6x 6TB Hard Drives
- Deployable on-premise or in AWS cloud

DRAGOS MIDPOINT SENSOR

- Hardware appliance deployed at small or medium 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

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 Behavior 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 cross-team
Reporting and Dashboards	▷ Clear Indicator of Compromise 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, Pi Historian, LogRythym, Syslog, Windows Host Logs

1745 Dorsey Road
Hanover, MD 21076 USA
dragos.com | info@dragos.com