Dragos™ **Platform**

DRAGOS

The industrial control system cybersecurity monitoring platform built for ICS defenders by ICS practitioners and cybersecurity experts

Dragos Platform Overview

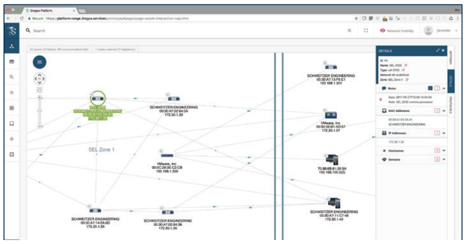
The Dragos Platform is a modular Industrial Control System (ICS) cybersecurity solution that provides ICS defenders with unprecedented knowledge and understanding of their assets and activity, the threats and adversaries they face, and the knowledge and tools to respond. **The Dragos Platform codifies the skills and knowledge of the industry's most trusted ICS practitioners and cybersecurity experts, providing all of the capabilities ICS defenders need to enable a more scalable, efficient, and effective defense.**

Protection Across the Entire ICS Cybersecurity Framework

The Dragos Platform contains all the necessary capabilities to monitor and defend ICS environments across the entire ICS cybersecurity framework. It is modularly designed so that it can be deployed in whole or in parts 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.

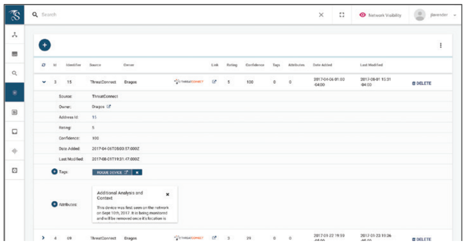
- **Identify:** automated asset and communications protocol discovery and enrichment across the network to identify how assets interact
- **Detect:** asset and protocol classification with behavioral attributes; set multiple baselines for differential analysis and risk assessment
- **Protect:** extended 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

Asset Discovery



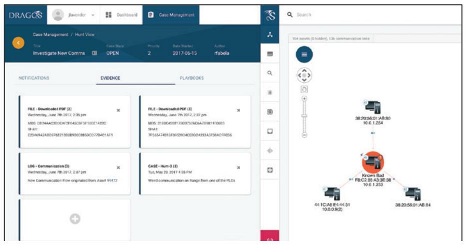
- Passively identify all assets and communications on the network
- Visualize and map network security zones and identify attack paths
- Set one or more network baselines against which to monitor changes

Threat Detection



- Deploy and manage behavioral analytics developed by the Dragos Intelligence team
- Indictor of Compromise and Query-Focused Datasets provide starting points for threat hunting
- Identification, prioritization and filtering of notifications enables rapid response

Case Management and Workflow



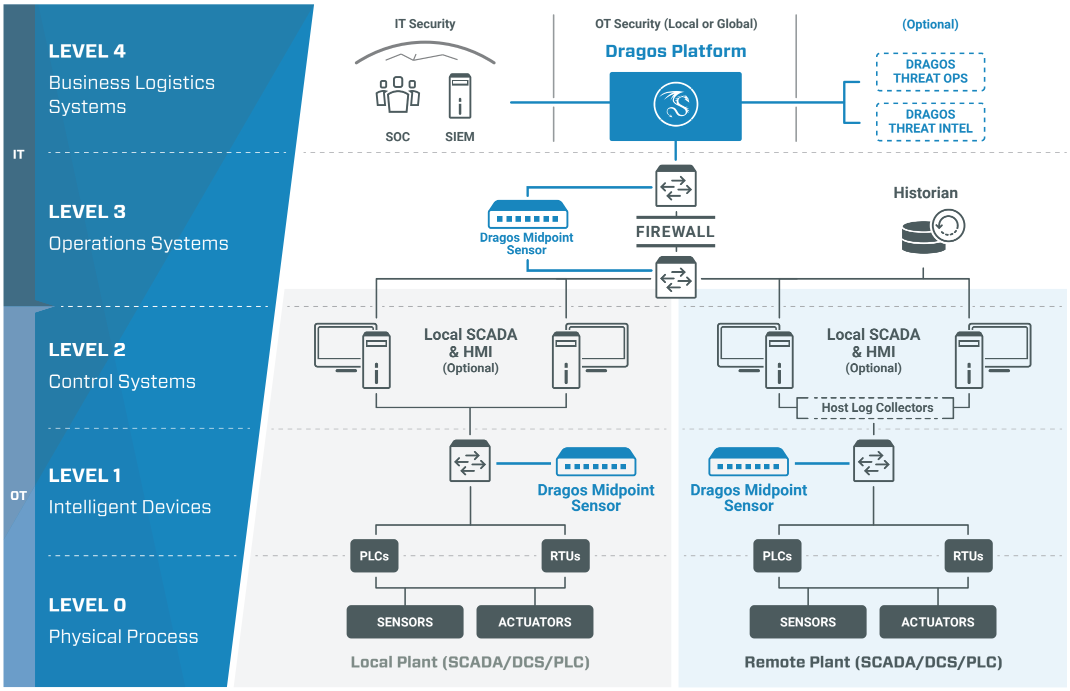
- Use case management tools to manage incident response case notes, forensics and collaboration
- Playbooks from Dragos experts drive standardized, best practice response
- Automation and orchestration between different security tools reduces workload
- Reporting and Dashboards monitor analyst and system activity

Why choose the Dragos Platform?

- The Platform is highly scalable and designed to monitor up to hundreds of thousands of assets across multiple sites at high speeds
- The Platform codifies Dragos' human analysts' deep knowledge of adversary tradecraft into behavioral analytics that significantly enhance threat detection. There is nothing artificial about our intelligence.
- The Platform goes beyond deep packet inspection on ICS protocols, incorporating host logs, controller logs, data historian alerts and more, to provide the most thorough analysis and accurate understanding possible.
- The Platform's threat alerts are contextually enhanced through behavioral analytics, enabling faster, more informed incident investigation and response aided by Dragos tools and best practice recommendations.

Dragos™ **Platform**

Platform Development and System Requirements



Dragos Sitestore

- 4 CPU / 32 GB RAM
- 2 TB SSD Hard Drive
- VMWare ESX Host and can be deployed to a virtual environment
- Deployable on-premise or in cloud (AWS, Azure, Google)

Dragos Midpoint Sensors

- Hardware-deployed appliance in Small, Medium or Large
- Handles up to 1GB data rates

Sample of Supported Protocols

ModbusTCP, Ethernet/IP, Profinet, OPC, IEC 61850, IEC 104

Licensing

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

Feature	Benefits
Asset Discovery, Enrichment, Classification and Exploration	■ Significantly reduce the amount of time necessary to identify and inventory all assets and traffic on your network ■ System-generated asset maps and reports enable you to have a consistent, time-driven view that is accurate, up-to-date, and thorough ■ Enrich Asset information to tailor behavioral analytics and improve security profile ■ Automatic classification of assets based on behavior ■ Set one or more baselines, notify 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; behavioral analytics work immediately upon deployment ■ Detect threats not simply as anomalies, 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 security operations 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 Assets that are vulnerable ■ Easily monitor case, notification, and analyst activity, as well as system-level health and status
Third Party Integrations	■ Firewalls, Alarm Servers, Data Historians, Existing Asset Trackers, Log Storage, and open APIs to extend

Contact Information

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