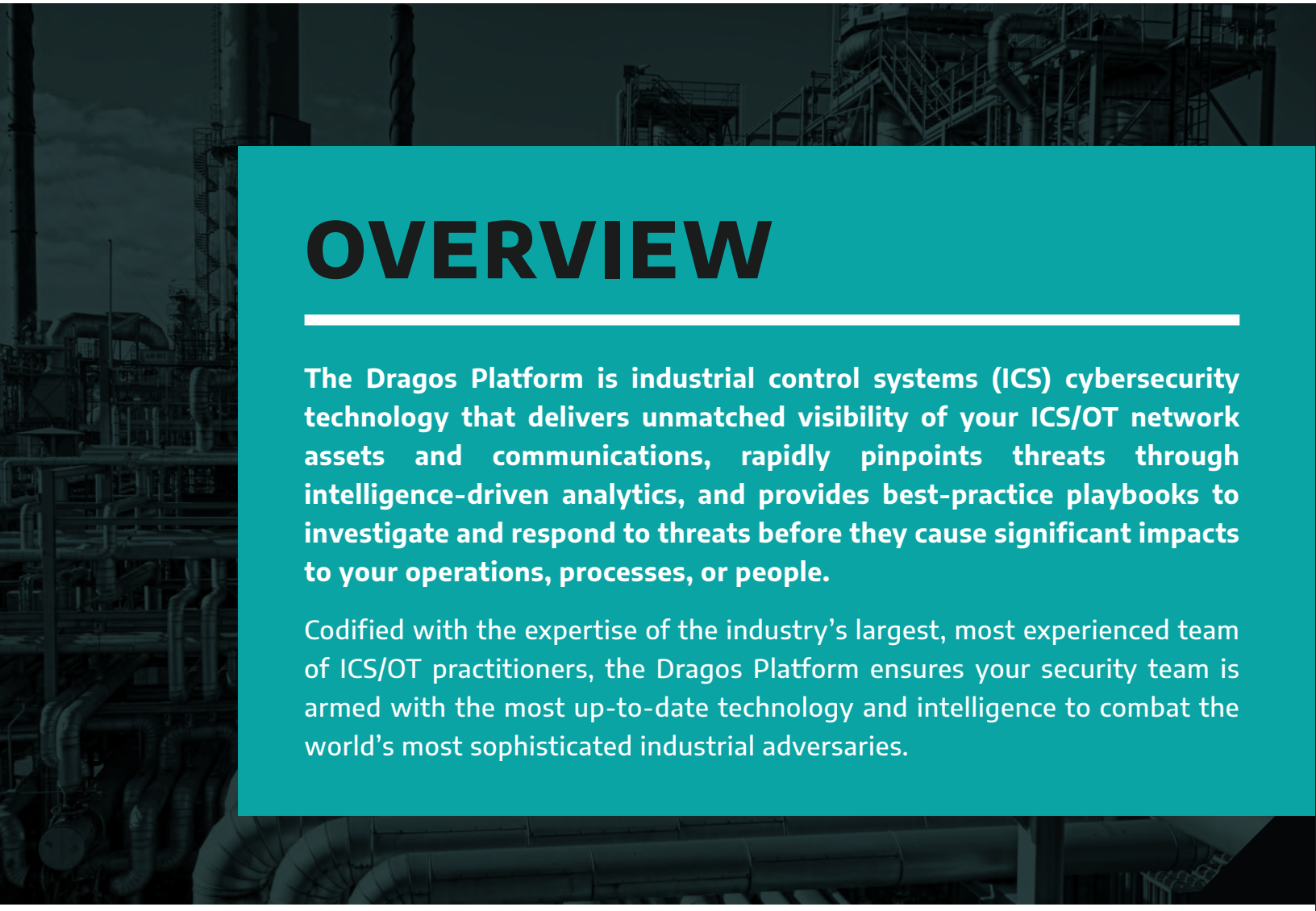
DRAGOS

DRAGOS PLATFORM

ICS/OT CYBERSECURITY TECHNOLOGY TO VISUALIZE YOUR ENVIRONMENT AND DETECT AND RESPOND TO THREATS



OVERVIEW

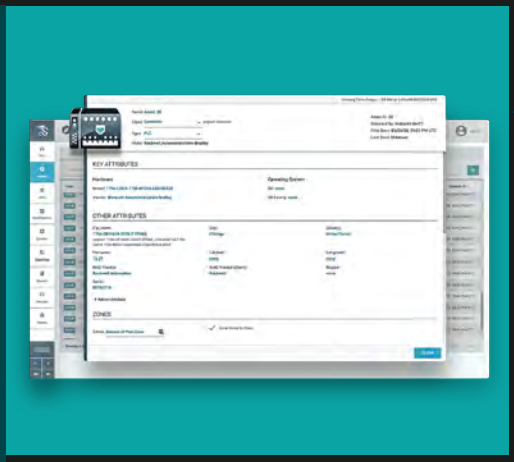
The Dragos Platform is industrial control systems (ICS) cybersecurity technology that delivers unmatched visibility of your ICS/OT network assets and communications, rapidly pinpoints threats through intelligence-driven analytics, and provides best-practice playbooks to investigate and respond to threats before they cause significant impacts 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

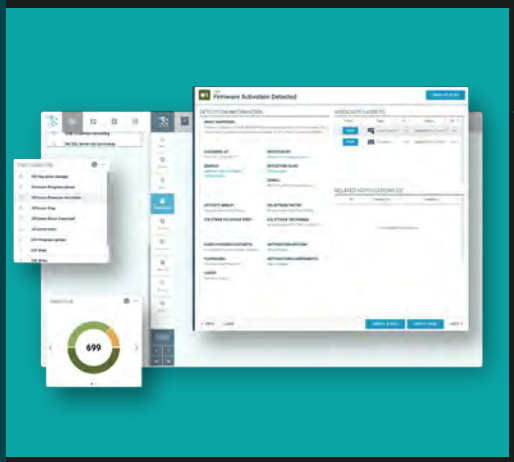
- **REDUCE ICS/OT CYBERSECURITY RISK**
- **PREVENT CATASTROPHIC DOWNTIME**
- **REDUCE THREAT DISCOVERY TIME**
- **DECREASE INCIDENT RESPONSE TIME**
- **AMPLIFY ICS/ OT RESOURCES**
- **IN-DEPTH ICS/ OT ASSET AND DEVICE VISIBILITY**

KEY FEATURES



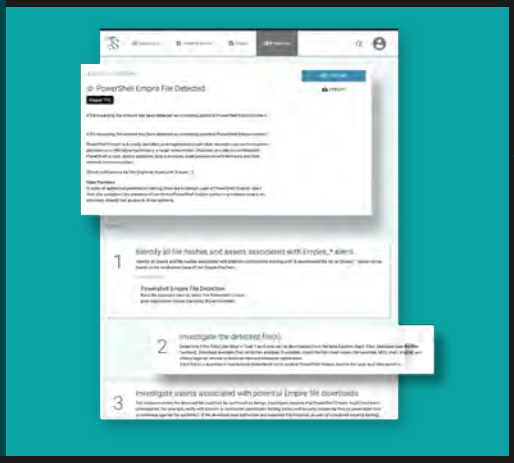
COMPREHENSIVELY VISUALIZE YOUR ICS/OT ASSETS AND ANOMALIES

- ✔ See all ICS/OT network traffic and asset communications
- ✔ Identify normal operations vs. abnormal with timeline and historical views
- ✔ Manage assets with zoning by location, role, type, and subnets
- ✔ Understand in-depth asset details, including vendor, firmware, model, and more



RAPIDLY IDENTIFY AND PINPOINT THREATS

- ✔ Get continuous threat monitoring based on newest behavior-based analytics created by Dragos Threat Intelligence
- ✔ See configuration, modeling, indicator, and threat behavior 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 ICS ATT&CK



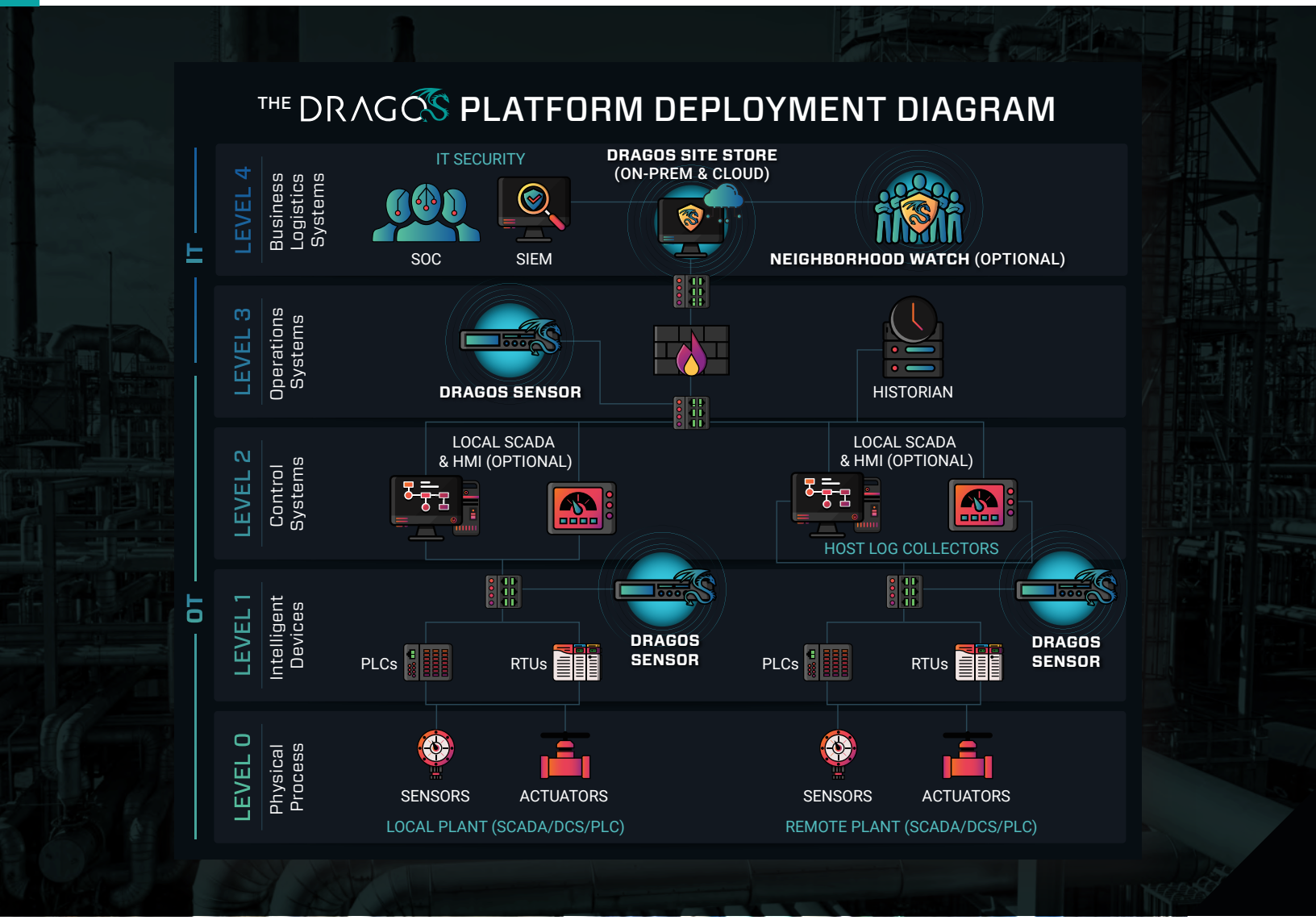
CONFIDENTLY INVESTIGATE AND RESPOND TO THREATS

- ✔ Collaborate seamlessly across teams with a full analyst workbench
- ✔ Use step-by-step investigation playbooks authored by Dragos experts
- ✔ Improve investigation and efficiency with in-depth asset information and custom search information via Dragos Query Focused Datasets

DRAGOS PLATFORM DEPLOYMENT

The Dragos Platform's 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.

PLATFORM DEVELOPMENT AND SYSTEM REQUIREMENTS



FLEXIBLE DEPLOYMENT

The Dragos Platform offers flexible, virtual deployment options, including on-premise and cloud.

DRAGOS SITESTORE

- ✔ Virtually deployable via on premise and cloud

DRAGOS SENSORS

- ✔ Virtually deployable via on premise and cloud
- ✔ Gathers and processes SPAN port traffic from 100Mbps to 1Gbps

EXTENSIVE PROTOCOL & VENDOR SUPPORT

- ✔ Over 130+ ICS and IT protocols supported
- ✔ Vendor support for Rockwell, Siemens, Schneider, Yokogawa, Honeywell, GE, Emerson, SEL, and more

DRAGOS PLATFORM

FEATURES AND BENEFITS

FEATURES	DRAGOS PLATFORM	DRAGOS PLATFORM + NEIGHBORHOOD WATCH (MANAGED SERVICE)
Visualization of ICS/OT asset communications, behaviors, vulnerabilities, and anomalies	✔	✔
Expert-driven ICS/OT environment management and reporting of asset changes	--	✔
Recurring environmental checkups and Dragos Platform tuning	--	✔
Deep Packet Inspection of protocols, host logs, controller logs, data historian, alerts, and more	✔	✔
Threat analytics based off latest attacker TTPs with mapped MITRE ICS ATT&CK detections	✔	✔
Expert-driven alert prioritization and immediate triage support	--	✔
24x7 notification of high-severity alerts with added context and recommendations	--	✔
Full analyst workbench with contextually guided investigation playbooks and Query Focused Datasets	✔	✔
Routine threat hunts based off latest Dragos adversary intelligence	--	✔
Regular reports on threat hunt findings and response recommendations from Dragos Industrial Hunters	--	✔
Regularly delivery of new analytics, Indicators of Compromise, asset and device characterizations, and playbooks via Dragos Knowledge Packs	✔	✔
Ease of deployment with SIEM functionality, plus on-premise and cloud options	✔	✔
Expert-led ICS/OT environment scoping and definition	--	✔
Third party integrations with Splunk, QRadar, OSIsoft Pi Historian, LogRythym, Syslog, Windows Host Logs, and more	✔	✔
Global insights from anonymized customer environment analytics	--	✔

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