
DRAGOS
INDUSTRIAL CONTROL SYSTEMS CYBERSECURITY
VISIBILITY. DETECTION. RESPONSE.

DRAGOS
OVERVIEW

Founded in 2016 by former members of the NSA who specialize in **hunting and responding to national threats** to industrial infrastructure and **building the tools** to combat them

$48M Raised
120+ Employees
105+ Customers

HQ: Hanover, Maryland
Regional: Houston, Texas

Robert M. Lee

Founder
Chief Executive Officer

Jon Lavender

Founder
Chief Technology Officer

Justin Cavinee

Founder
Chief Data Scientist

BUILT BY PRACTIONERS FOR PRACTIONERS

Dragos ICS practitioners have been the first responders of the world's most significant industrial cyber attacks

30% More Dedicated ICS Software Engineers Than Competitors

50% Of Dragos Practitioners Focused on R&D for Dragos Platform

200+ Years of ICS Security Experience

THE SOLUTION

Comprehensive **Technology**

Unique **Threat Intelligence**

Expert-Guided **Services**

THE DRAGOS PLATFORM

ICS **monitoring software** for comprehensive **asset identification**, **threat detection** and **response**

DRAGOS WORLDVIEW

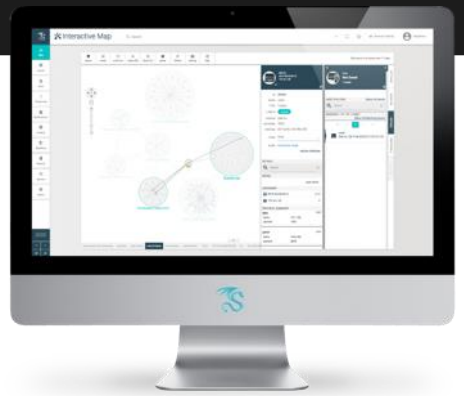
In-depth **situational awareness** of the threat landscape via **actionable** insights and **intelligence reports**

ICS SECURITY SERVICES

Expert **guidance** to combat and respond to adversaries via **incident response**, **proactive services,** and **training**

THE DRAGOS PLATFORM

THE INDUSTRY'S MOST COMPREHENSIVE ICS TECHNOLOGY



ASSET IDENTIFICATION & ANOMALY DETECTION

Quick, agent-less, and fast passive discovery

Context on assets, their behaviors, and anomalies

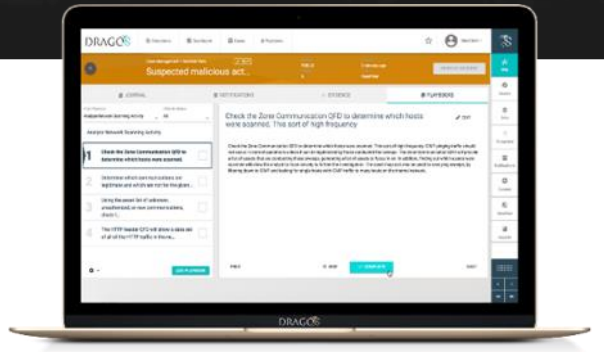
Accurate information to support operations and effective threat detection

THREAT ANALYTICS

Unique ICS threat intelligence on adversary behaviors and their capabilities

More effective detection with fewer false positives via Dragos-authored analytics

Accurate detection to support investigations and incident response



INVESTIGATION PLAYBOOKS

Step-by-step playbooks covering ICS attacks and impacts

Efficient investigations and full analyst workbench for threat remediation

Accurate response to incidents to meet your requirements

THE DRAGOS PLATFORM

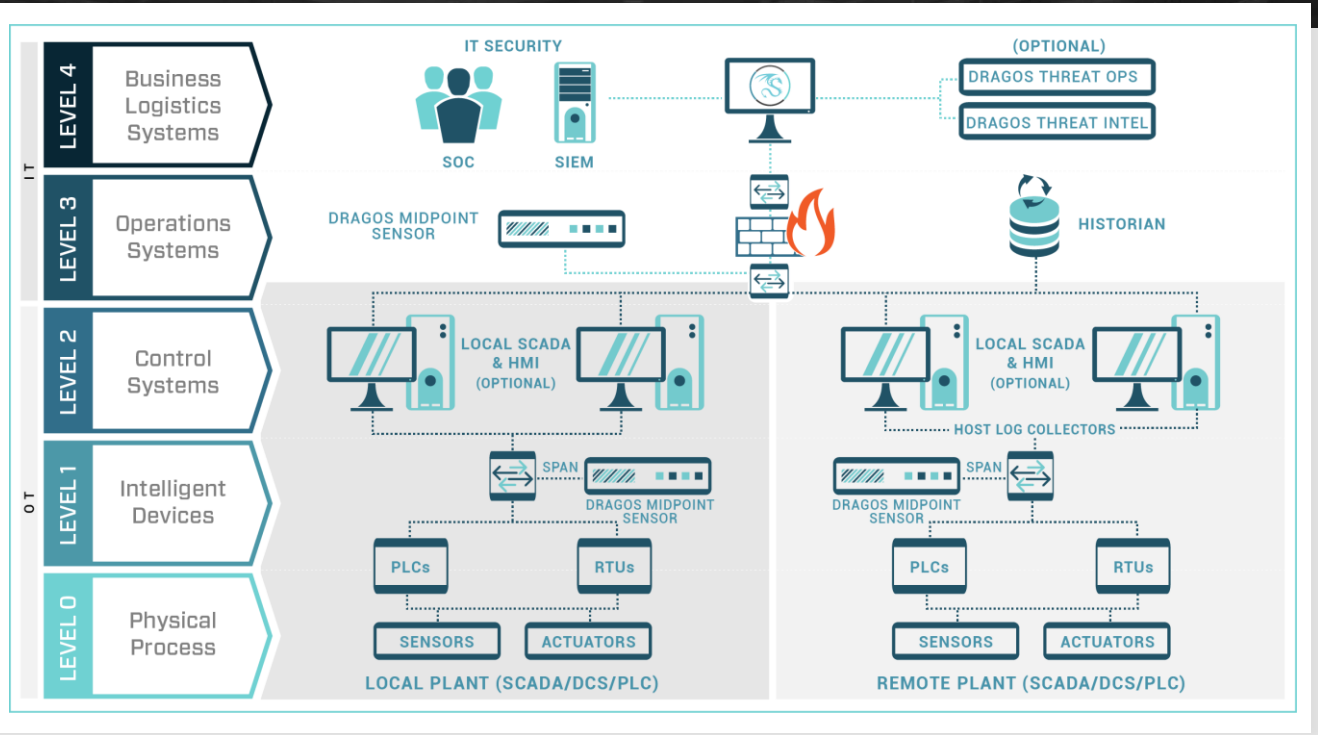
DEPLOYMENT ARCHITECTURE

DRAGOS SITESTORE
Deployable on-premise or in AWS cloud (Managed Hunting option available for cloud)

TRAFFIC COLLECTION
Dragos sensors are primarily deployed via network span or tap

LOGS AND/OR PCAPS
Utilize existing infrastructure, systems, devices, and tools

INTEGRATIONS
Extend visibility and/or enrich data collected




DRAGOS
Neighborhood Keeper
a collaborative threat detection and intelligence program

The Community Challenge

Issues with Efforts Before

Many Community Members Lack Resources

Our smaller infrastructure community members lack resources for budget and personnel to deploy, maintain, and leverage leading technologies on the market.

Information Sharing Struggles in OT/ICS

Many information sharing programs share data or information; they rarely share intelligence. This requires sensitive data to be shared between entities with little curating. Effort is expended on a hope that value will be seen later and indicators do not scale.

Insights into OT/ICS Networks is Limited

Cyber threats target OT/ICS networks yet the collection and analysis from those networks is extremely limited. It definitely does not exist in the smaller infrastructure sites where adversaries can train and prepare undetected.

DRAGOS

Roadmap to Achieve Energy Delivery Systems Cybersecurity Objectives Mapped

Roadmap Item 4.5

(Cyber event detection tools that evolve with the dynamic threat landscape commercially available)

By deploying commercial off the shelf (COTS) industrial specific technology (the Dragos Platform) to the OT network layer of the participants and researching, developing, and deploying industrial specific threat behavior analytics to provide a transposable and scalable form of intelligence-driven threat detection.

Roadmap Item 5.6

(Mature, proactive processes to rapidly share threat, vulnerabilities, and mitigation strategies are implemented throughout the energy sector)

Researching, architecting, and deploying a cloud architecture (analytics framework) that will securely interconnect the OT layer sensors to receive and share, at machine-speed, insights in the form of non-sensitive and non-personal identifiable metadata

Roadmap Item 1.5 and 4.6

(Compelling business case developer for investment in energy delivery systems security)

(Lessons learned from cyber incidents shared and implemented throughout the energy sector)

Research and develop public use-cases and insights from this data to showcase the value of this approach to inform defense and response practices and create a combined threat picture across the energy sector that is freely available to all

DRAGOS

Program Participants and Value

Dragos

The prime on the proposal. The Dragos Platform COTS software will be provided to all participants at no cost. Dragos will perform research and development in three key areas. The first will be stripping the current technology down to a low cost and easier to use form for smaller sites (more focused). Second, the cloud analytics framework will be developed (non-existent today) to centralize and utilize analytical outputs from participants. Third, new threat analytics and playbooks will be researched, developed, deployed, tested, and tuned across the participants to find new threats.

Electricity Information Sharing and Analysis Center (E-ISAC)

Advisory function that will ensure that what is being researched and developed will be useful to the larger electric sector community. Additionally, the focus will be on how to use the analytical outputs to enrich the CRISP dataset. As an example, leveraging when threats in OT occurred to find threats in IT.

Idaho National Laboratory

Advisory function that will ensure that what is being researched and developed will be useful to the Department of Energy and to the view of the national threat landscape. Additionally, they will focus on how to leverage the insights to enrich and enhance CYOTE.

Ameren, First Energy, and Southern Company

Utility participants to deploy the technology and connect to the cloud analytics framework. Detections in their environment, interviews with their personnel, and use-cases jointly produced will ensure the approach is sound and scalable to take to the larger industry especially co-ops and municipalities.

DRAGOS

STEP 01

Low-cost Dragos Platform deployed as a passive appliance in co-ops' and municipalities' OT/ICS environments

DRAGOS

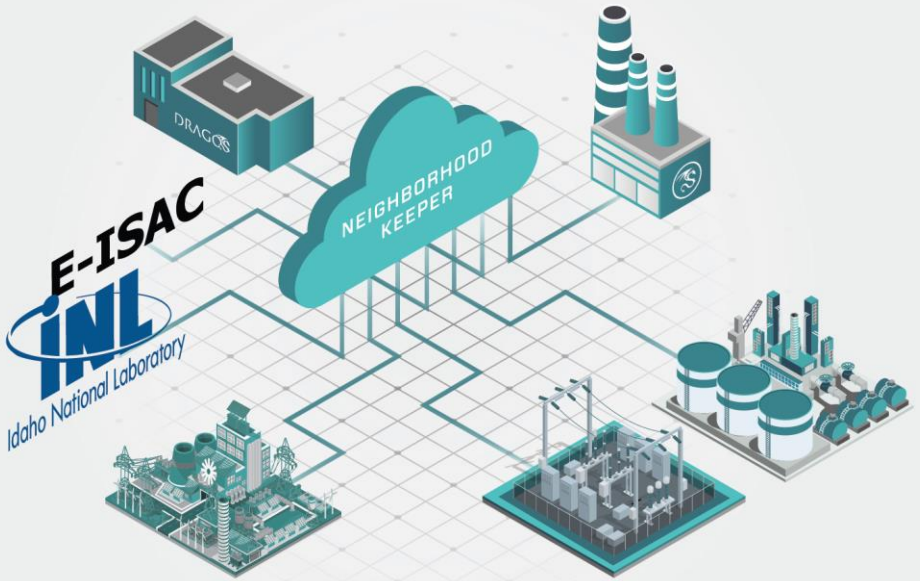
STEP 02

Sites with Dragos Platform deployed connect together. Internal data and sensitive network info are stored on-site and never shared

DRAGOS

STEP 03

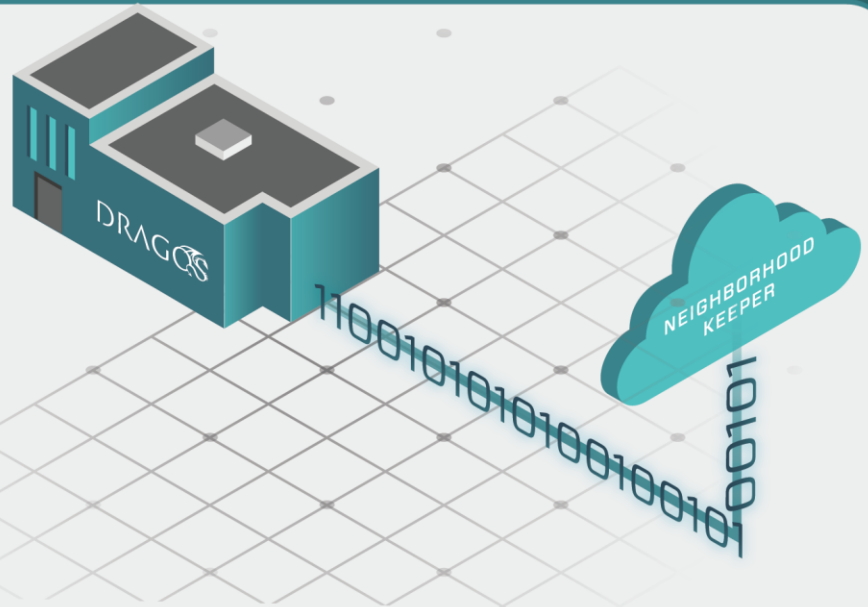
Community partners (E-ISAC, INL, & opt-in Dragos Platform customers) share and receive threat insights



DRAGOS

STEP 04

Dragos' intelligence team creates threat analytics based on behaviors and methods of ICS adversaries



DRAGOS

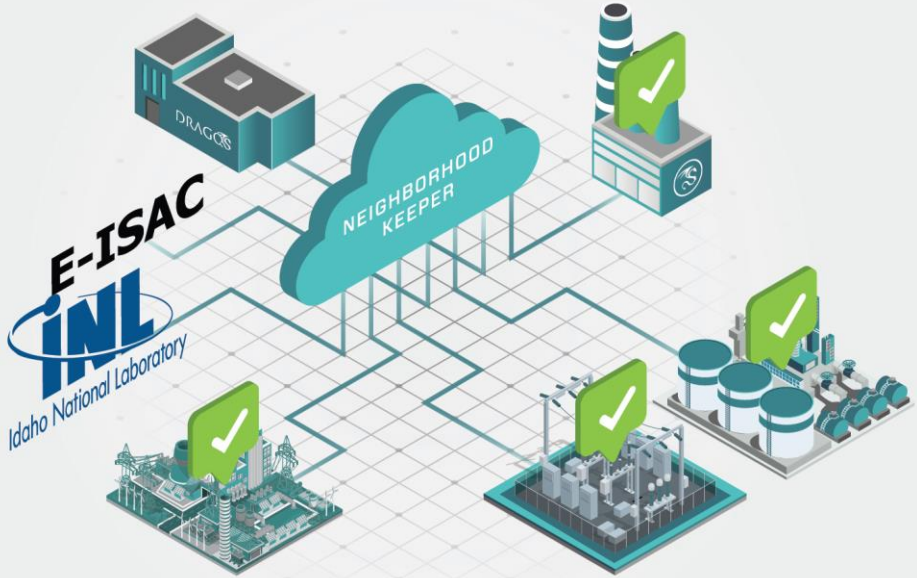
STEP 05

Analytics run at sites; if threats detected, analytic outputs (e.g., metadata: “analytic 3 alerted at 2:30pm”) shared to Neighborhood Keeper

DRAGOS

STEP 06

New threats, trends, and adversary campaigns revealed from analytics help participants gain insights and prioritize defenses



DRAGOS

Expected Outputs From the R&D

A sustainable program to illuminate the industrial threat landscape

Day 1 Value to Participants	The Dragos Platform will immediately provide asset identification and automatic reporting to participants. Threat analytics are also immediately available. Additionally, data is stored onsite and available to any future incident responders
Low Cost	The Dragos Platform will be available to smaller providers at a near-cost pricing
Low Touch Point	Remote analysis of the analytical outputs will be done for the participants and monitoring done for them; if anything is ever particularly bad they'll be notified. No need for additional personnel at participant sites.
No Trust	No sensitive data leaves the participants' sites. It is only analytical outputs no personal identifiable information in the system or available to analysts
Shared Insights	New threat analytics run across the environment will identify threats in OT/ICS networks to share insights of what detections and playbooks (mitigations) work across participants. This will be shared at machine-speed to all participants.
Enrichment	Insights will be leveraged to enrich the national understanding of threats as well as programs such as CRISP and CYTE. Insights can also be used to offer regulation and standards bodies insights into the real risk so the approaches are adapted.

DRAGOS

Program Update

- We have received great interest from Municipalities, Cooperatives, and Investor Owned Utilities who want to participate. We have close to 20 utilities who have expressed interest in being participants and existing public participants:
  - Salt River Project (SRP)
  - Xcel Energy
  - Sacramento Municipal Utility District (SMUD)
  - Ameren
  - FirstEnergy
  - Southern Company
- Currently finishing up our NK deployment with Connexus Energy and 4 other co-ops/munis and look forward to working with them to study the program's impact on their cybersecurity program and report out to the industry

DRAGOS

Program Update

- As the development matures, we are continuing to find ways to keep the program cost low; essentially covering our cloud costs but giving away software at near cost
  - At this point, we are averaging between 25K-40K per year to cover a company
- We have been actively working with the American Public Power Association (APPA), Edison Electric Institute (EEI), Congress, and others who are all working to help find financial support for smaller operators.
- Dragos and EEI have agreed that Cyber Mutual Assistance (CMA) can be leveraged as a vehicle with Neighborhood Keeper for utilities to respond to each other

Upcoming Events

- Association of Large Distribution Cooperatives, Fall IT Workshop – Oct 10-11, 2019
  - With case-study of implementation/successes co-presented with Connexus Energy
- APPA Cybersecurity Summit – Nov 18-20, 2019

DRAGOS

Questions?

keepers@dragos.com

https://www.dragos.com/neighborhood-keeper.html