Neighborhood Keeper

Introduction

DRAGOS
NEIGHBORHOOD KEEPER
E-ISAC
INL
Idaho National Laboratory

Matt Bodman
Director of Special Programs

DRAGOS

Who are we?

We enhance ICS defenders’ efficiency and effectiveness via:

- Dragos platform,
- Dragos WorldView intelligence reports, and
- the Dragos Threat Operations Center.

The Dragos platform delivers codified industrial cybersecurity expertise that enables security teams to detect and respond faster to industrial cybersecurity threats, reducing dwell time and down time.

The Community Challenge

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.

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

What is Neighborhood Keeper?

Low-cost, collaborative threat detection and intelligence sharing program formed with industry leaders that makes ICS threat analytics and non-sensitive data accessible to participants

Companies of any size can participate and share non-sensitive data (non-NERC CIP) securely and anonymously across the Neighborhood Keeper community to create ICS-specific insights

Improved visibility of the ICS landscape to create collective threat awareness and enable Cyber Mutual Assistance for all participants

Partnership with Ameren, First Energy, and Southern Company, E-ISAC and Idaho National Labs to conduct R&D, develop use cases, and leverage CRISP and CYOTE data for enrichment

DRAGOS

Other Program Participants and Value

Electricity Information Sharing and Analysis Center (E-ISAC)

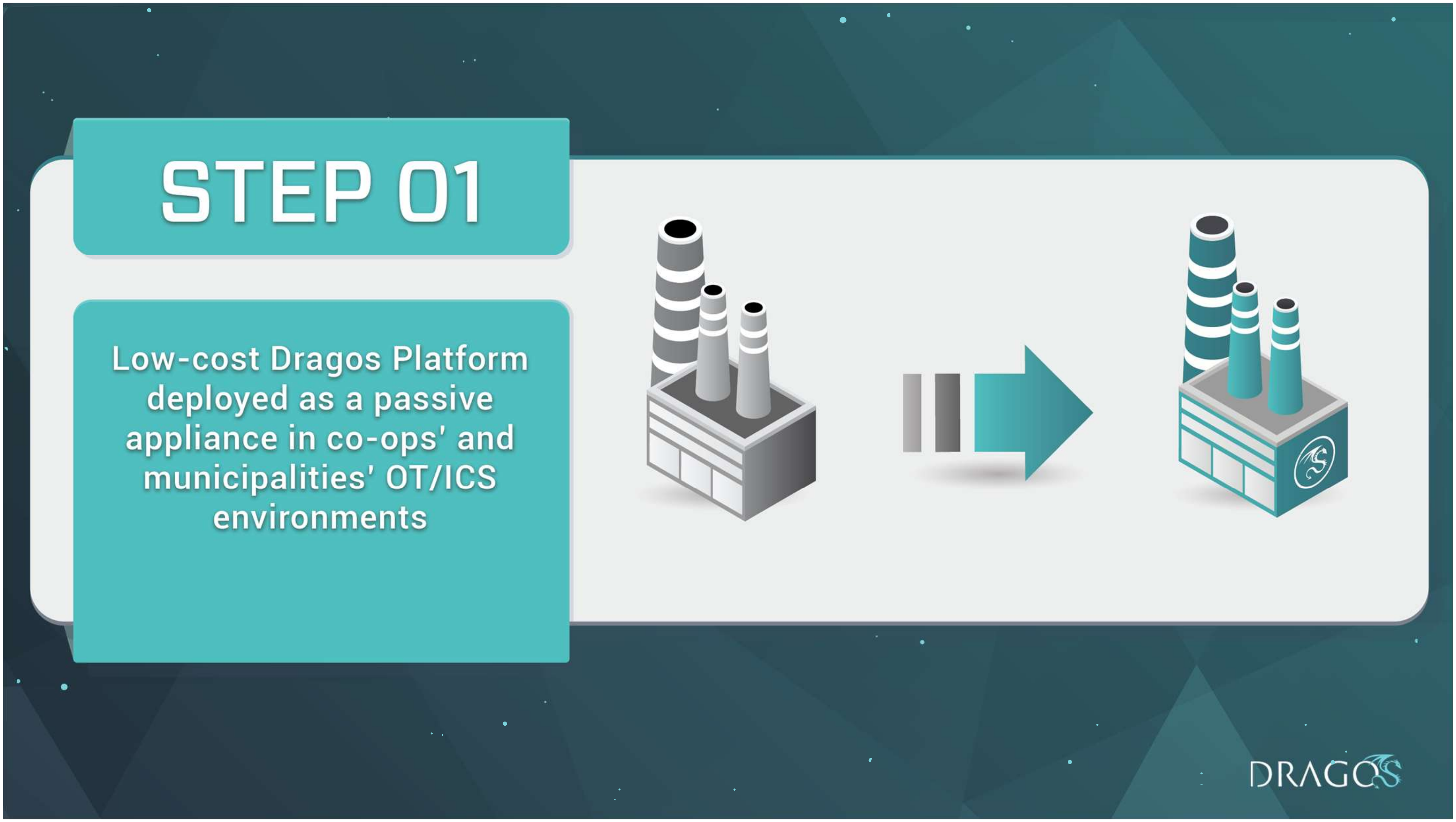
Advisory function that will ensure that what is being researched and developed will be useful to the larger electric sector community. Additionally, the focus will be on how to use the analytical outputs to enrich the CRISP dataset. As an example, leveraging when threats in OT occurred to find threats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



STEP 01

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

STEP 02

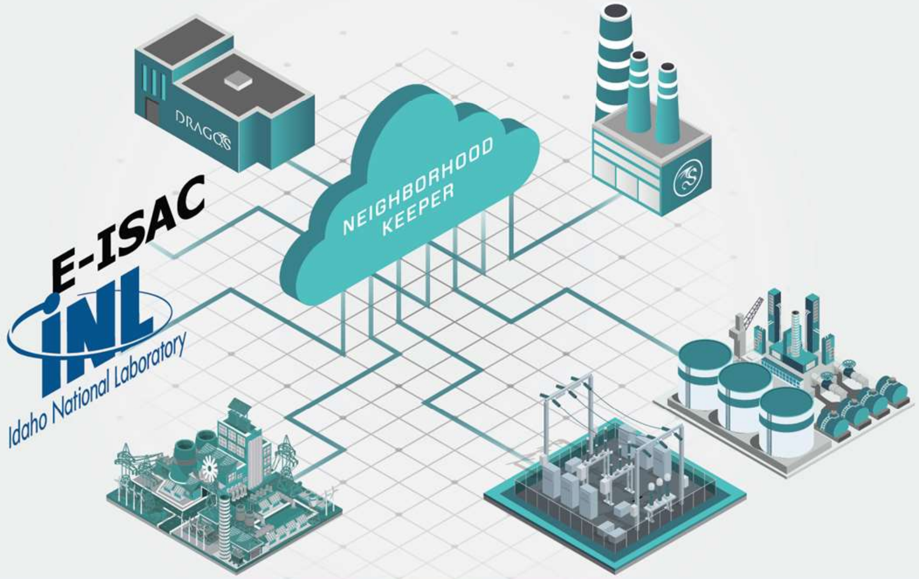
Sites with Dragos Platform deployed connect together. Internal data and sensitive network info are stored on-site and never shared

DRAGOS
NEIGHBORHOOD KEEPER

DRAGOS

STEP 03

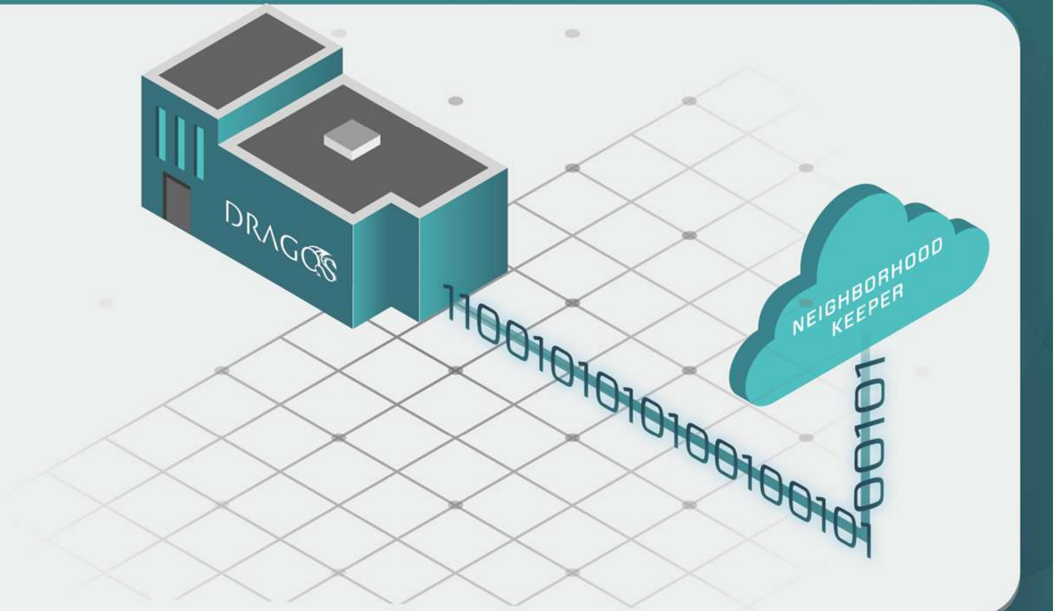
Community partners (E-ISAC, INL, & opt-in Dragos Platform customers) share and receive threat insights



DRAGOS

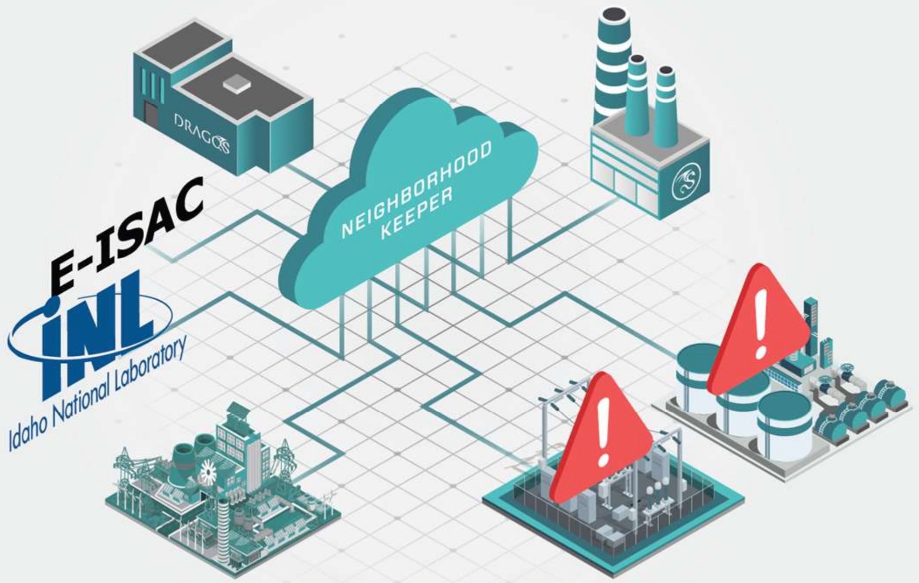
STEP 04

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



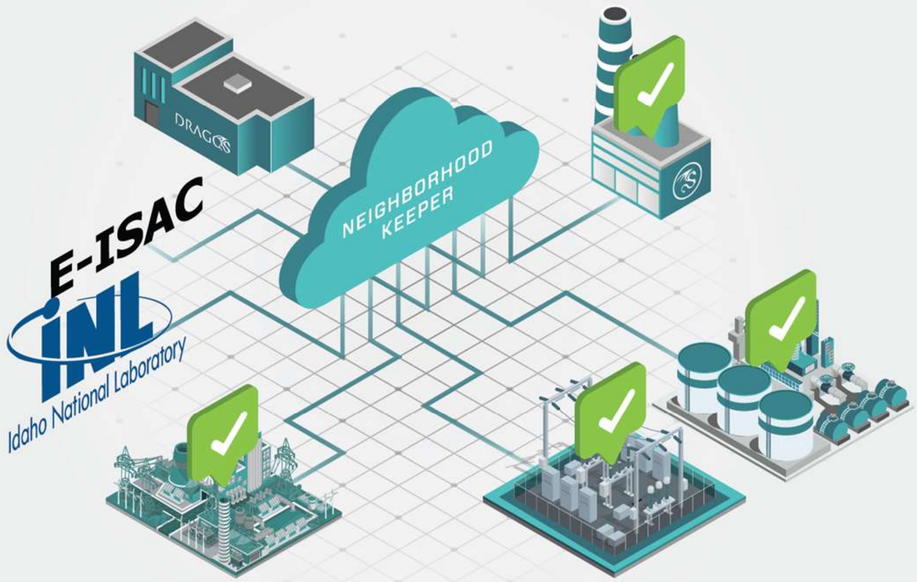
STEP 05

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



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 modified Dragos Platform will be available at an estimated $5-10k a year per network appliance price point for ~15k-45k per year per co-op/municipality.
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.

Expected Outputs From the R&D

A sustainable program to illuminate the industrial threat landscape

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 CYOTE. Insights can also be used to offer regulation and standards bodies insights into the real risk so the approaches are adapted.

Questions?

KEEPERS@DRAGOS.COM

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