



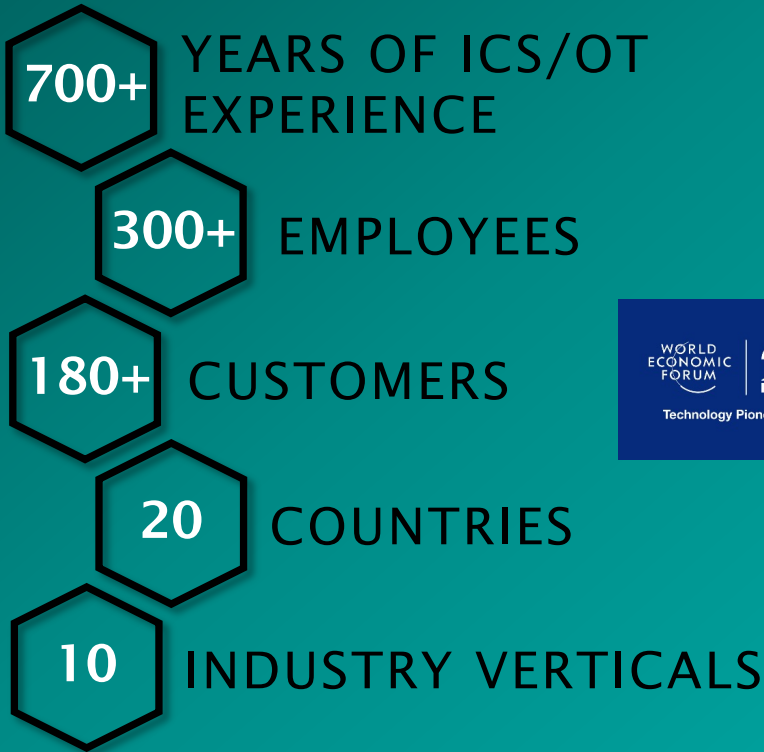
INDUSTRIAL CYBERSECURITY

Safeguarding Civilization

Robert M. Lee
Jon Lavender



BUILT BY PRACTITIONERS FOR PRACTITIONERS



Dragos has the largest team of ICS security specialists in the industry which allows us to make the best technology.

- ELECTRIC
- WATER
- OIL & GAS
- FOOD & BEV
- MANUFACTURING
- MINING
- BLDG AUTO SYS
- TRANSPORTATION
- CHEMICAL
- PHARMACEUTICAL

HQ | Hanover, MD

REGIONAL | Canada, Australia-New Zealand,
GCC, UK/Europe

Including **9** of the **10** largest U.S. electric utilities and **6** of the **10** largest oil and gas companies

DRAGOS IS YOUR ALLY

- ✓ Comprehensive Technology
- ✓ Unique Threat Intelligence
- ✓ Expert-Guided Services



The Dragos Platform

ICS/OT cybersecurity technology for comprehensive asset visibility, vulnerability management, threat detection and response



Worldview Threat Intelligence

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



ICS/OT Security Services

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

White House/DOE ICS Action Plan

- OT/ICS Focus
 - Health and Safety focus (50k+ population centers)
 - Starting with Electric sector; Chem/Water/NG to follow with coordination to industry trades/leaders
- Technology Adoption for Visibility/Detection/Response
 - Historically standards/regulations/frameworks/etc. have been heavily prevention focused
 - Was told ESCC involved in the plan and evaluated multiple vendors for the effort
 - Dragos was informed that were chosen for this effort due to our capabilities and the speed to which utilities could begin the sharing through Neighborhood Keeper
- What's Been Happening?
 - Over 70 utilities are already in Neighborhood Keeper now or are scoping the deployments to join soon with a lot of quickened movement due to the action plan
 - The goal for the industry is to move now, some confusion on that topic, but from our view most are
 - NERC has been very supportive of the community and is issuing a Practice Guide today to help ease the compliance discussions around deploying OT monitoring technologies
 - E-ISAC is undergoing training and investments to leverage Neighborhood Keeper directly to add additional value to participants, expectation is August

COMMUNITY WIDE CHALLENGES

ISSUES BEYOND YOUR OPERATIONS



LIMITED ICS/OT VISIBILITY

Data collection and analysis is often extremely limited and coordination between internal teams is lacking



DEFENDING IN ISOLATION

Lack of coordination and sharing inside organizations and the across community due to information security concerns



INFORMATION LATENCY

The speed at which existing information sharing programs operate denies organizations sufficient time to plan defense or response

security expertise?



“For these reasons and numerous others, the industry has been working to assess adversary capabilities through a keyhole, rather than through a deeper collection and broader field of vision.”



IDAHO NATIONAL LAB
“Neighborhood Keeper
Program Review”

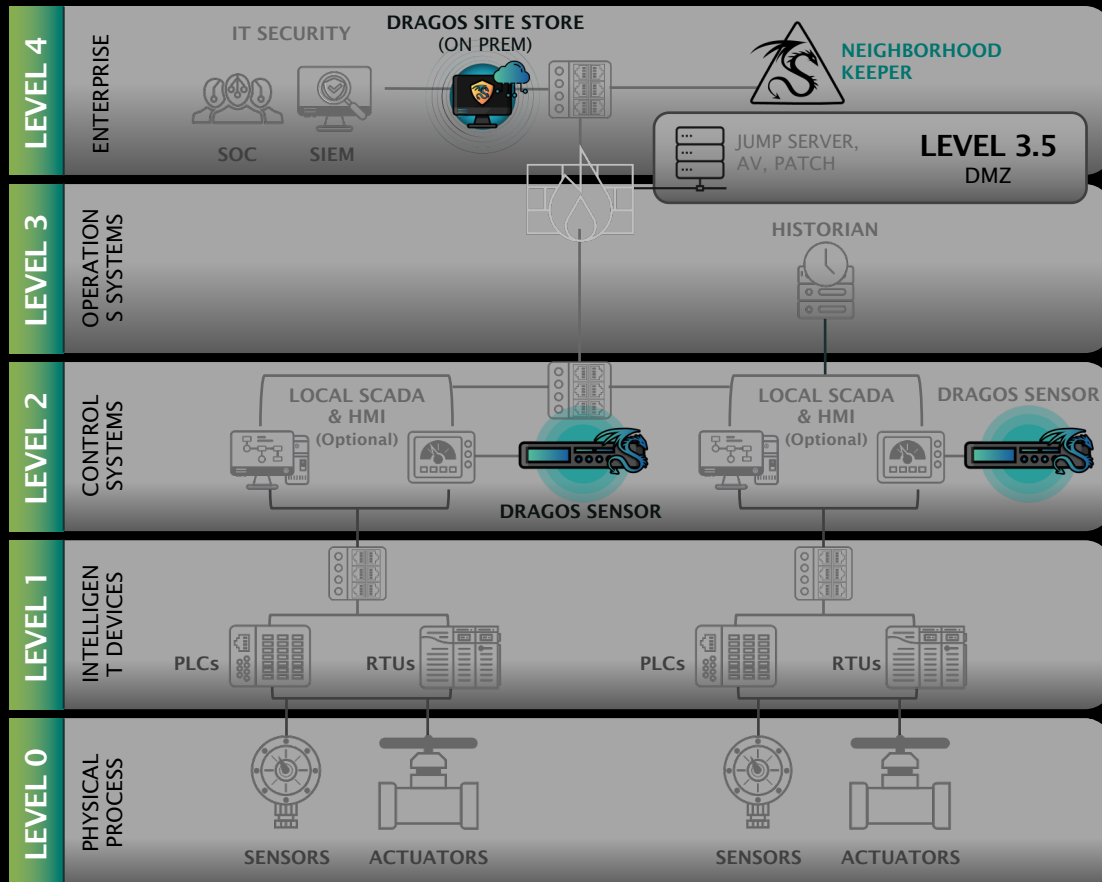
THE DRAGOS PLATFORM

FOR INDUSTRIAL CYBERSECURITY



Neighborhood Keeper Deployment

Purdue Model



The Dragos Platform's sensor is deployed passively in the ICS/OT Networks such as plant or substation networks.

The sensor connects to the Dragos Platform's server in the Enterprise or DMZ network and provides ongoing asset, vulnerability, and threat identification to the user.

The server connects to Neighborhood Keeper (US AWS Cloud hosted) through an encrypted connection.

The novelty is that data is not shared, questions are federated to members

INDUSTRY VALIDATION



Idaho National Laboratory Review

“The program provides the community of cyber operators a supervisory control and data acquisition (SCADA) situational awareness equivalent of detections occurring across participating organizations. This will provide participants with visibility to adversary activities beyond their own organization.”

“Neighborhood Keeper program stakeholders will see great value in this wide area view capability as participants can identify a coordinated activity or a broad campaign targeting multiple critical infrastructure entities”

- Idaho National Laboratory, “Neighborhood Keeper Program Review”



Southern
Company





“Neighborhood Keeper gives us the opportunity to work as a community to engage and respond to these threats.”

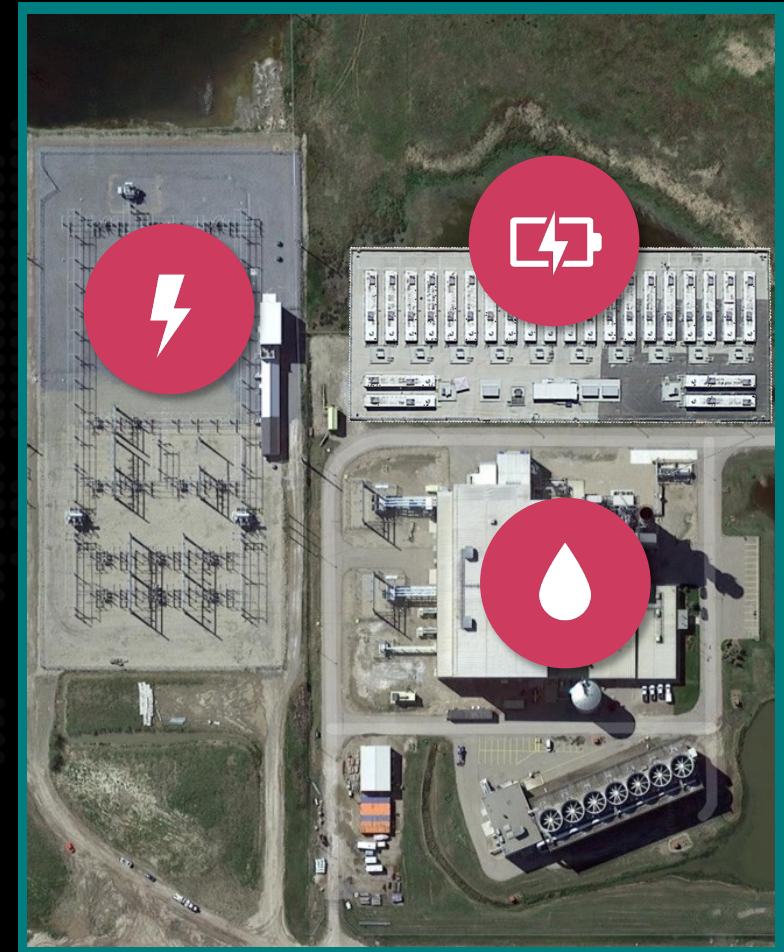
Curley Henry

Executive Director, Cybersecurity
Strategy & Architecture

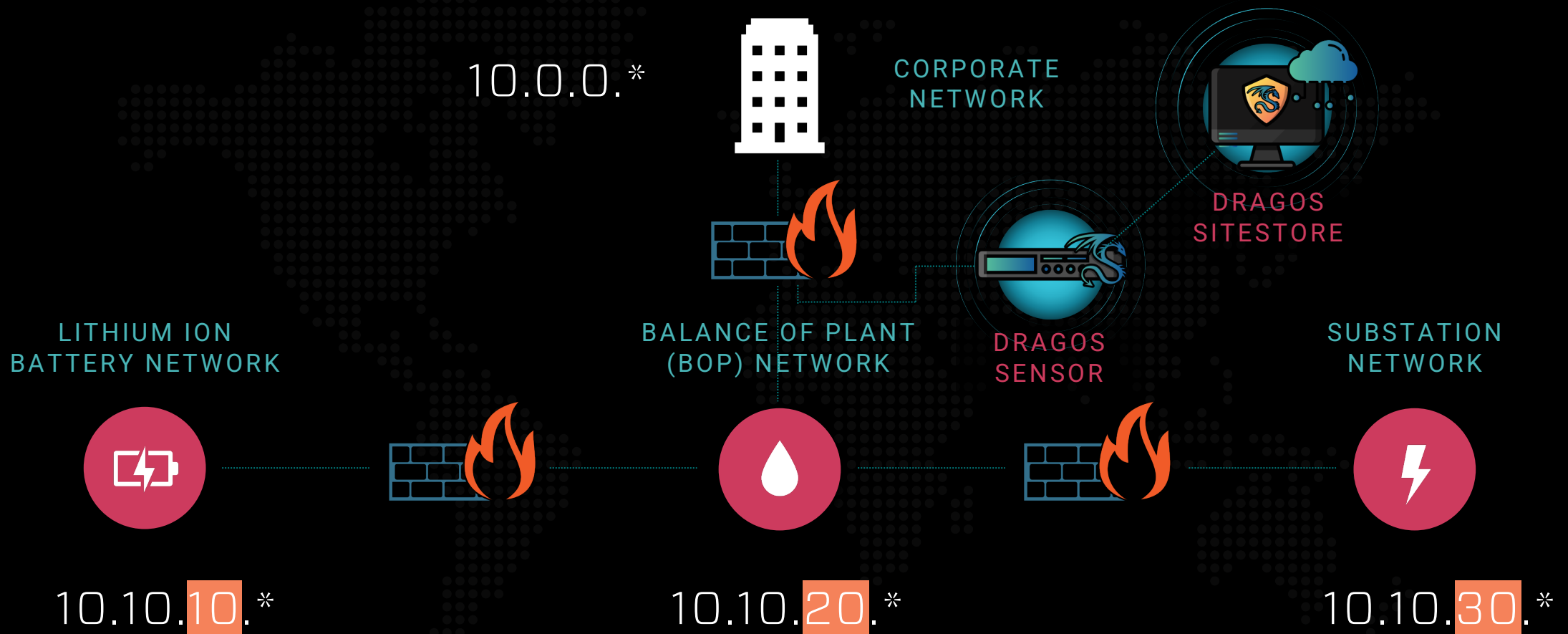
Demo

CYBERVILLE ENERGY CENTER

-  240 kV Transmission Substation
-  10MW, 40MWh Battery Storage System
-  44 MW – Combined Cycle Gas Generation
-  Black Start Facility / Peaker Facility



CYBERVILLE ENERGY CENTER NETWORK OVERVIEW

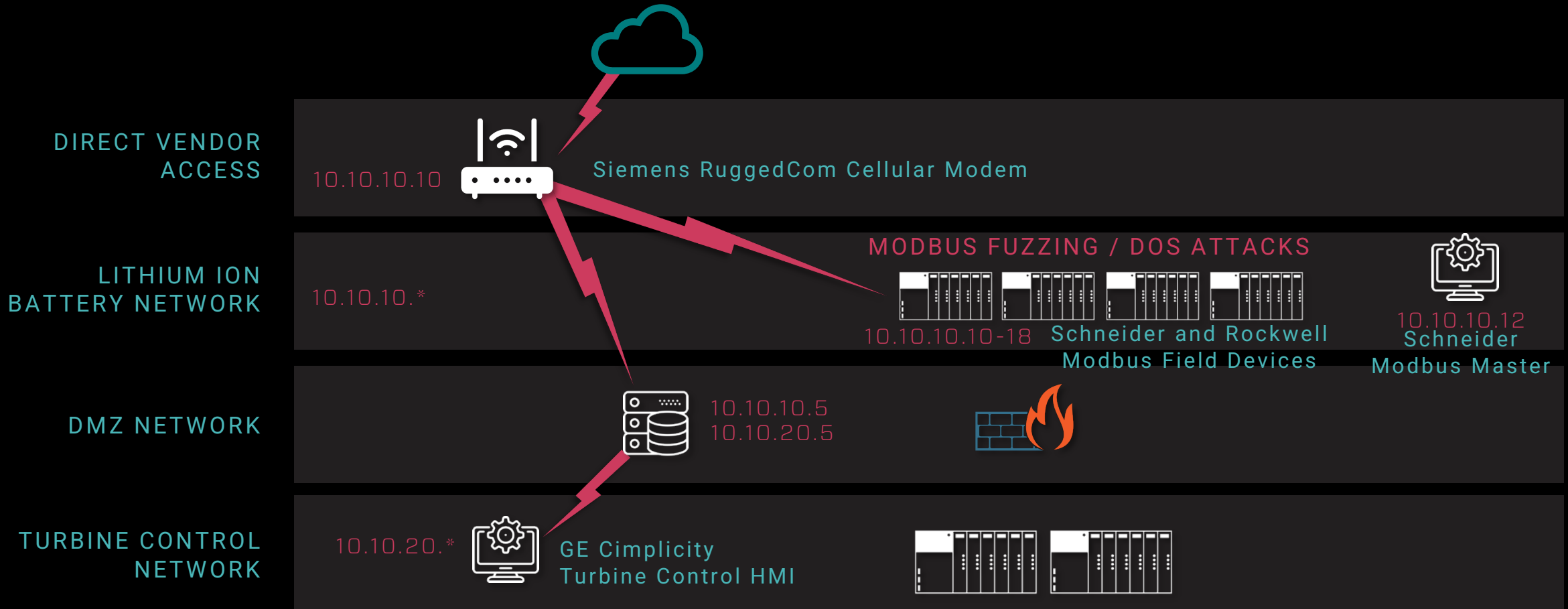


INITIAL ACCESS	EXECUTION	PERSISTENCE	EVASION	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND & CONTROL	INHIBIT RESPONSE FUNCTION	IMPAIR PROCESS CONTROL	IMPACT
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting		Point & Tag Identification	Device Restart/Shutdown		Rogue Master Device		Loss of View		
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings		Manipulation of View
						Screen Capture		Modify Control Logic		
	Program Download		Rootkit							
	System Firmware			Utilize/Change Operating Mode						
	Utilize/Change Operating Mode									

OUR SCENARIO

ATTACK SCENARIO

DISTRIBUTED ENERGY RESOURCES



DRAGOS NEIGHBORHOOD KEEPER

COLLECTIVE DEFENSE AND COMMUNITY-WIDE VISIBILITY



SHARED GLOBAL INSIGHTS

Threats, vulnerabilities, supply chain risks, and insights shared across the participant community at machine-speed



AMPLIFIED ICS RESOURCES

Dragos remotely analyzes output of detections and notifies participants of severe threats, who can optionally request assistance from the community



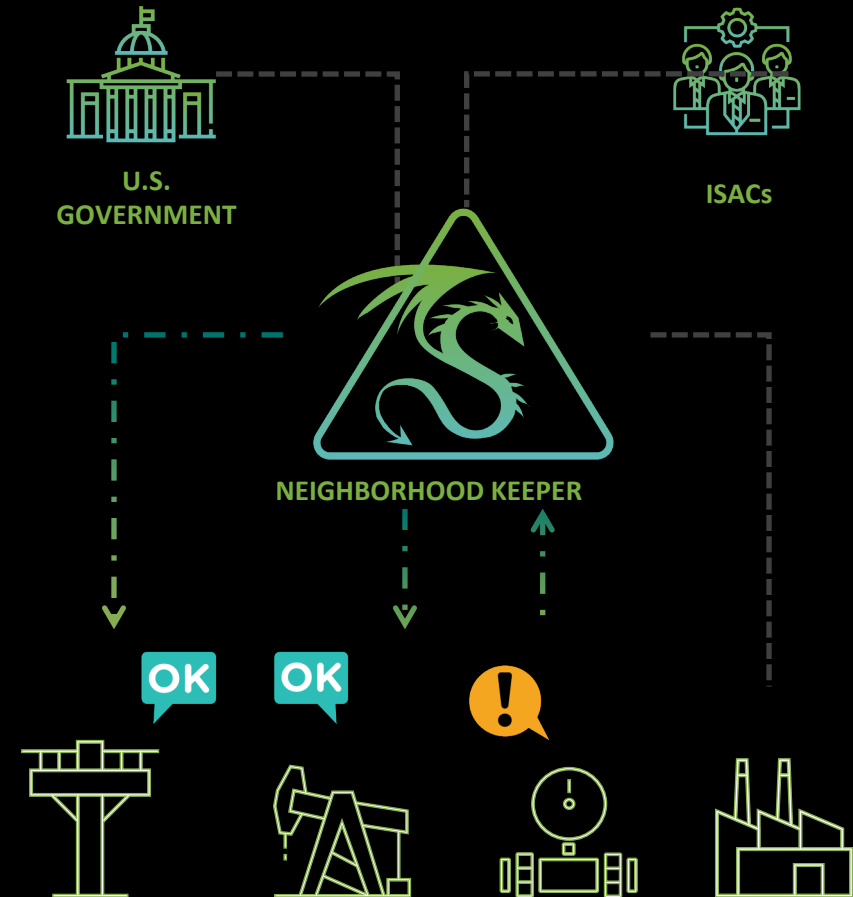
ANONYMIZED

Participant data is technologically irreversible. No sensitive data (e.g., logs, IP addresses) leaves participants' sites



FREE OPT-IN

Dragos Platform customers may choose to opt-in to help our global infrastructure community



Thank You

1 - Neighborhood Keeper was developed in partnership with the Department of Energy.

Acknowledgment: "This material is based upon work supported by the Department of Energy under Award Number(s) DE-OE0000898."

Disclaimer: "This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof."