WATERFALL®
Stronger Than Firewalls

DRAGOS

Achieving Manageable Zero Trust for OT Networks

VISIBILITY | UNDERSTANDING | PROTECTION | MONITORING

February 2021

Today's Agenda

- OT visibility – identifying what is on your operational network.
- Understanding your most critical zones.
- Zero Trust for OT networks.
- Segmentation of critical zones and monitoring for a complete OT security solution.
- The joint solution and tools to make it all achievable and manageable.

OT NETWORK SECURITY CHALLENGES

- IT/OT Convergence
- OT Threat Landscape Growing
- Lack of OT Visibility
- Lack of Accurate Asset Inventory and Network Map
- Cyber and Operational Vulnerabilities
- Monitoring required to track changes, errors, intrusions and attacks ongoing.
- Flat, unsegmented networks proving to be more vulnerable, segmentation recommended.
- Adding segmentation can represent a high impact of change via traditional approaches.
- Managing sub-parameters or segmented networks is an ongoing management challenge.

THE JOINT SOLUTION

DRAGOS

- A passive solution to produce an accurate asset inventory and network map.
- Providing full OT visibility – devices, locations, interactions and interdepdencies.
- Critical assets and processes now mapped and understood in single pane of glass.
- Your OT Zero Trust areas are identified and understood.

WATERFALL
Stronger Than Firewalls

- Hardware enforced unidirectional solution, physically securing segmentation.
- Reduce critical areas from your attack surface – micro-segmentation or broader segmentation.
- Waterfall supports segmentation in the most secure and maintenance free manor.
- Solution has least impact of change and complexity in enabling segmentation.
- Enforces Zero Trust

DRAGOS

- Dragos solution's monitoring, detection and full capability continues seamlessly from enclave and network wide.

WATERFALL
Stronger Than Firewalls

- Other data required from segmented area can be provided in real time..

COMMON CUSTOMER CHALLENGES

ASSET VISIBILITY

WHAT WE HEAR:

- I need to know what’s on my network?
- Do I have misconfigurations and security gaps?
- Are there rogue devices?
- When did changes take place?
- What is happening inside the control protocols?

HOW THE DRAGOS PLATFORM HELPS:

- Network visibility and asset identification
- Deep packet inspection covering a variety of protocols and vendors (e.g., EthernetIP/CIP, DNP3, ModbusTCP, BACNet, Honeywell, Emerson, Rockwell, GE, SEL, etc.)
- Timeline analysis

ASSET VISIBILITY

Image provided by Dragos, Inc.

DRAGOS

WATERFALL® Stronger Than Firewalls

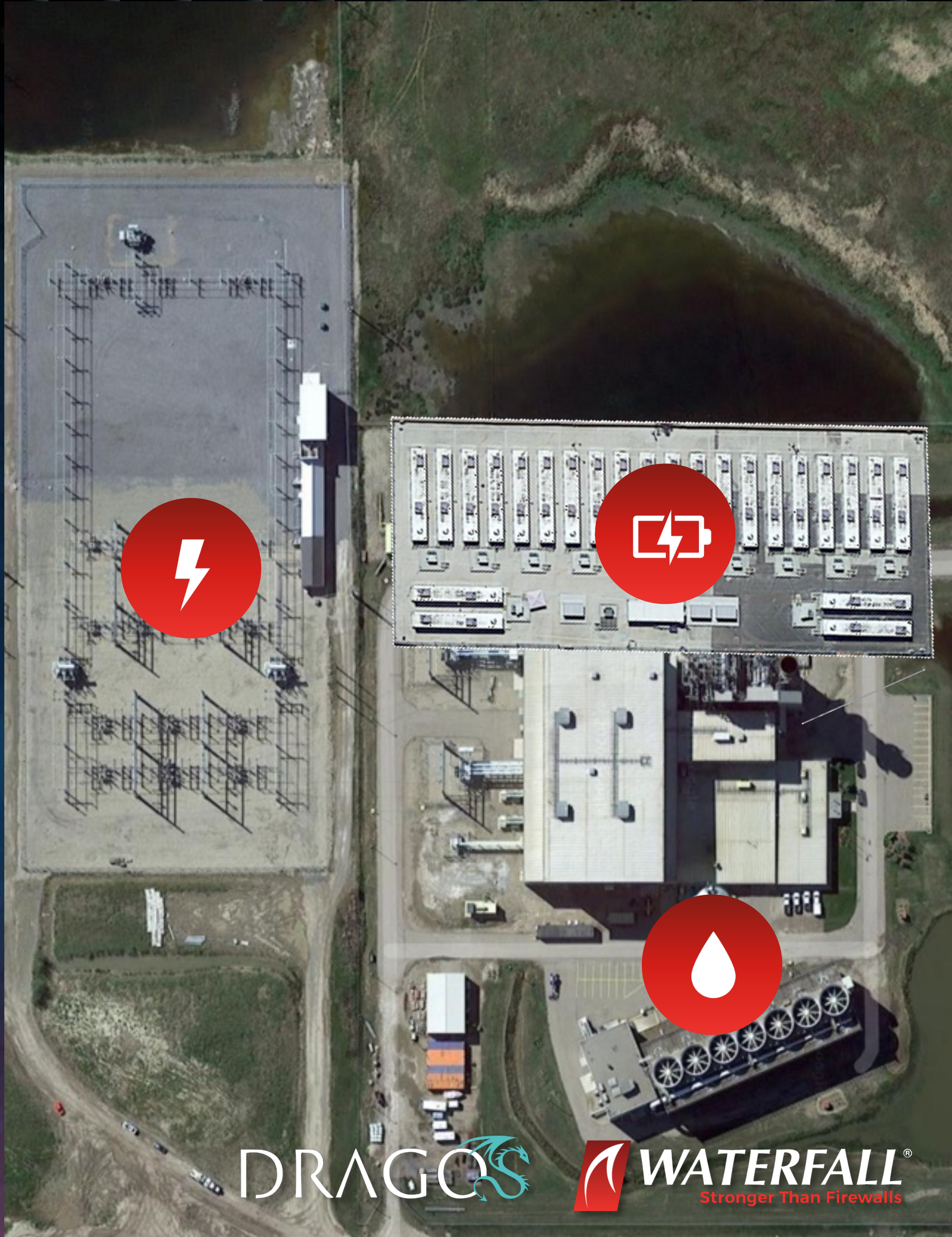
DEMO SCENARIO:

VISIBILITY AND ASSET IDENTIFICATION

A JOURNEY TO CYBERVILLE

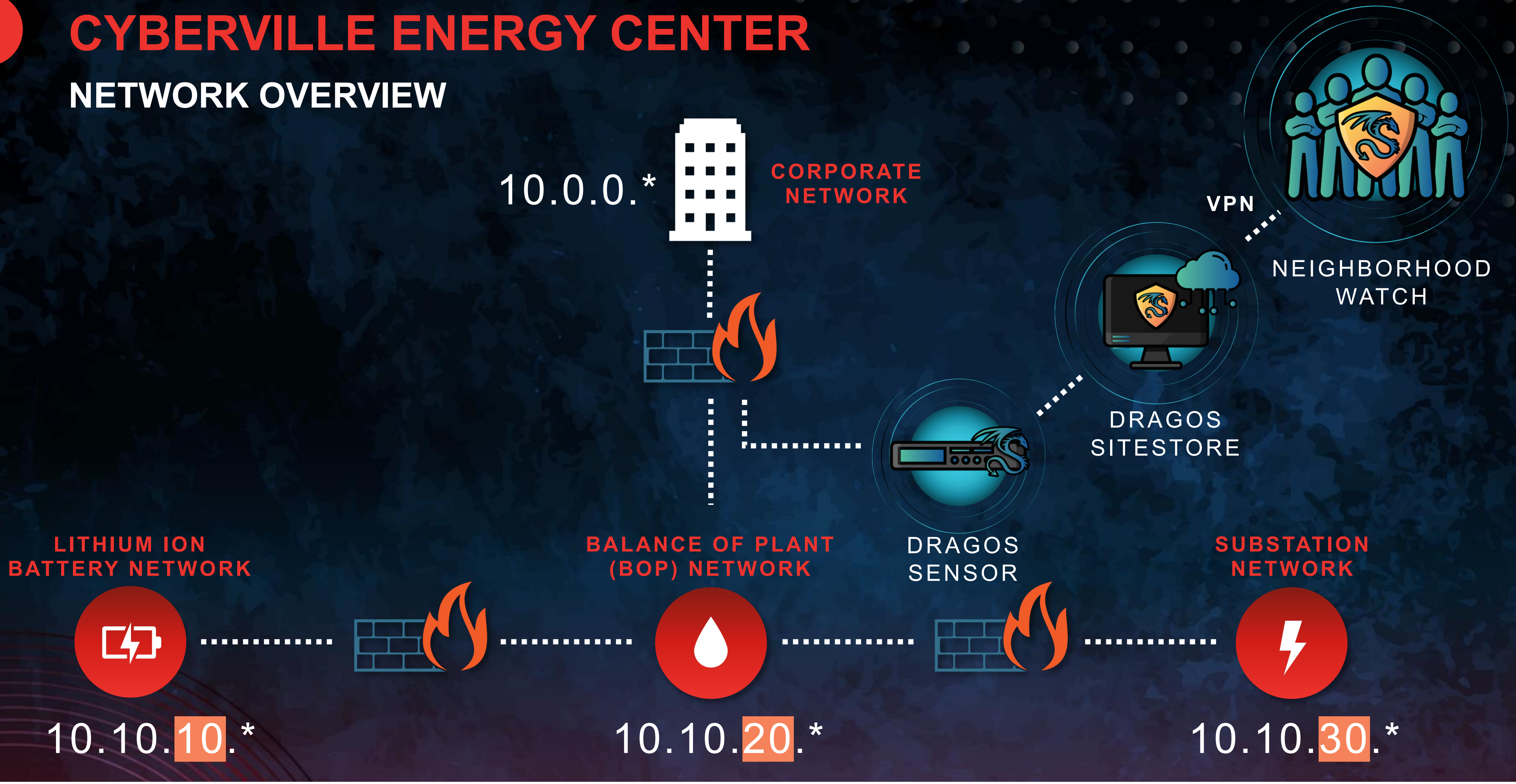
CYBERVILLE ENERGY CENTER

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

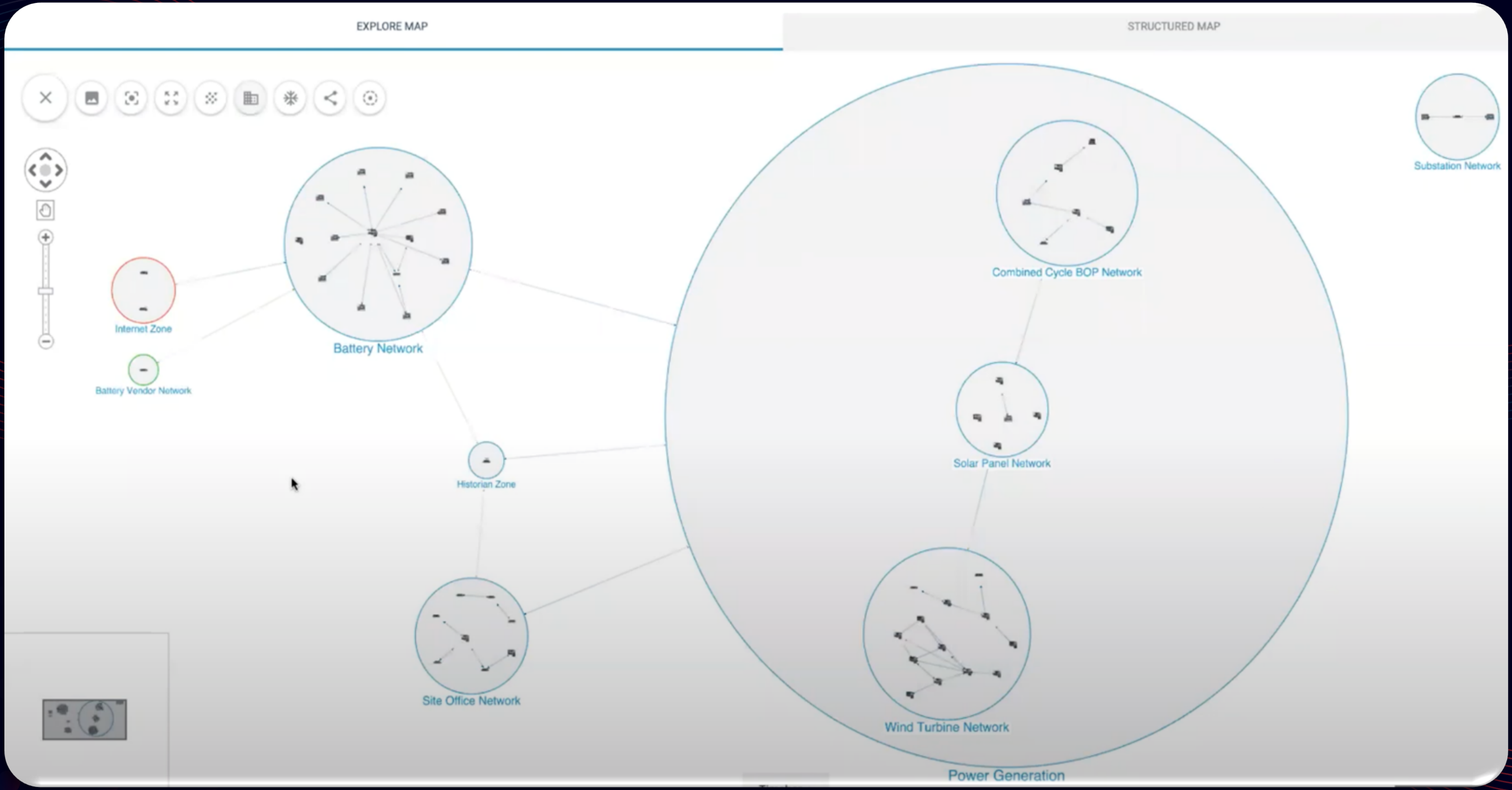


CYBERVILLE ENERGY CENTER

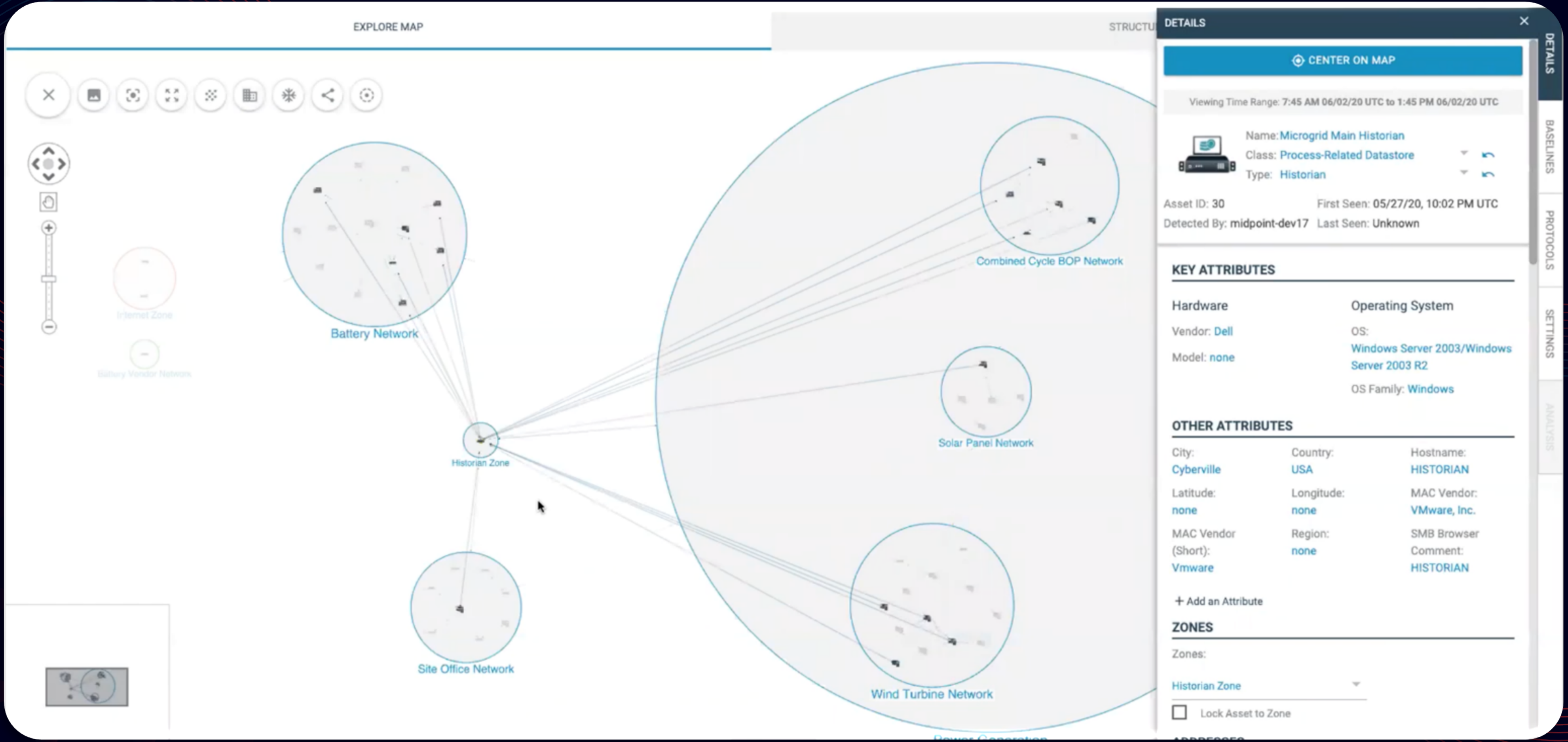
NETWORK OVERVIEW



DRAGOS PLATFORM FOR ICS/OT VISIBILITY



DRAGOS PLATFORM FOR ICS/OT VISIBILITY



DETAILS

Viewing Time Range: 7:45 AM 06/02/20 UTC to 1:45 PM 06/02/20 UTC

Name: Microgrid Main Historian
Class: Process-Related Datastore
Type: Historian

Asset ID: 30
First Seen: 05/27/20, 10:02 PM UTC
Detected By: midpoint-dev17
Last Seen: Unknown

KEY ATTRIBUTES

Hardware
Vendor: Dell
Model: none

Operating System
OS: Windows Server 2003/Windows Server 2003 R2
OS Family: Windows

OTHER ATTRIBUTES

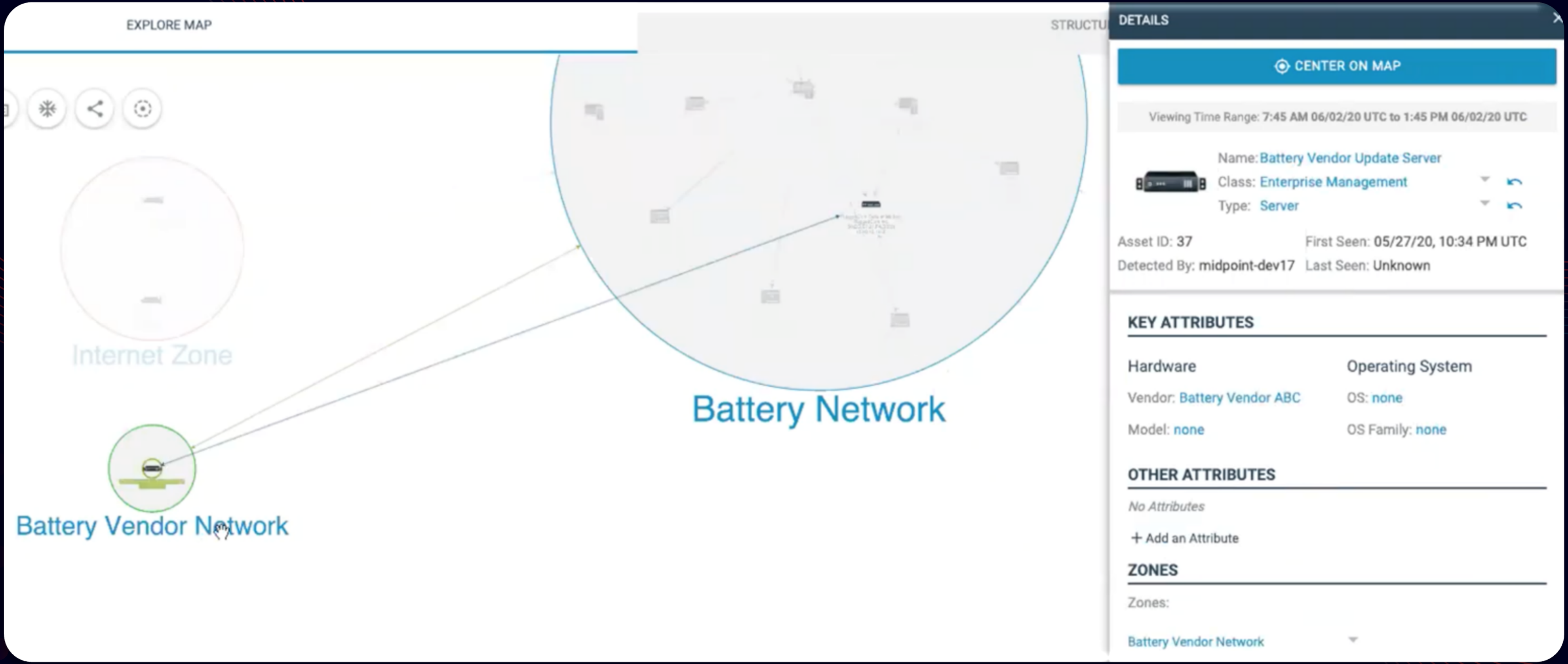
City: Cyberville
Country: USA
Hostname: HISTORIAN
Latitude: none
Longitude: none
MAC Vendor: VMware, Inc.
MAC Vendor (Short): Vmware
Region: none
SMB Browser Comment: HISTORIAN

ZONES

Zones: Historian Zone

□ Lock Asset to Zone

DRAGOS PLATFORM FOR ICS/OT VISIBILITY



Viewing Time Range: 7:45 AM 06/02/20 UTC to 1:45 PM 06/02/20 UTC

Name: Battery Vendor Update Server
Class: Enterprise Management
Type: Server

Asset ID: 37 First Seen: 05/27/20, 10:34 PM UTC
Detected By: midpoint-dev17 Last Seen: Unknown

KEY ATTRIBUTES

Hardware	Operating System
Vendor: Battery Vendor ABC	OS: none
Model: none	OS Family: none

OTHER ATTRIBUTES

No Attributes

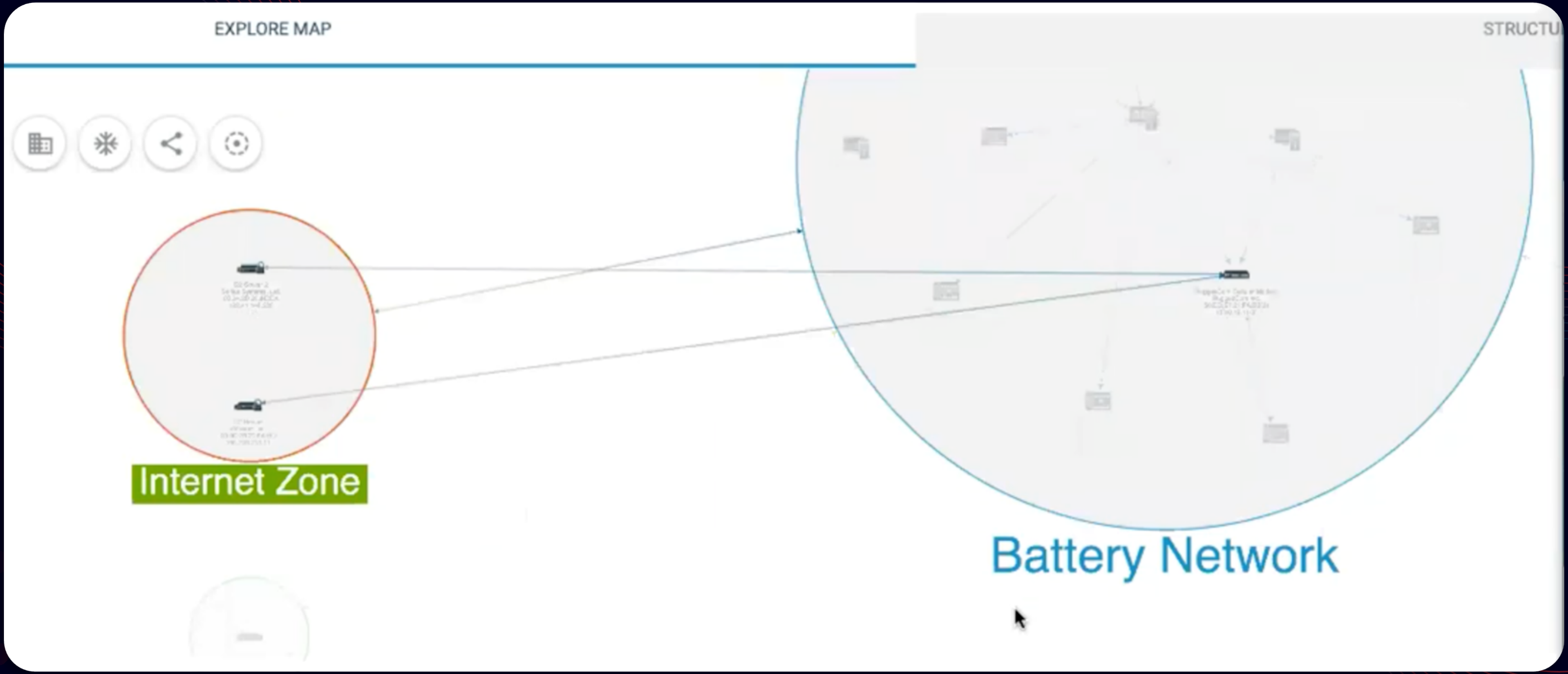
+ Add an Attribute

ZONES

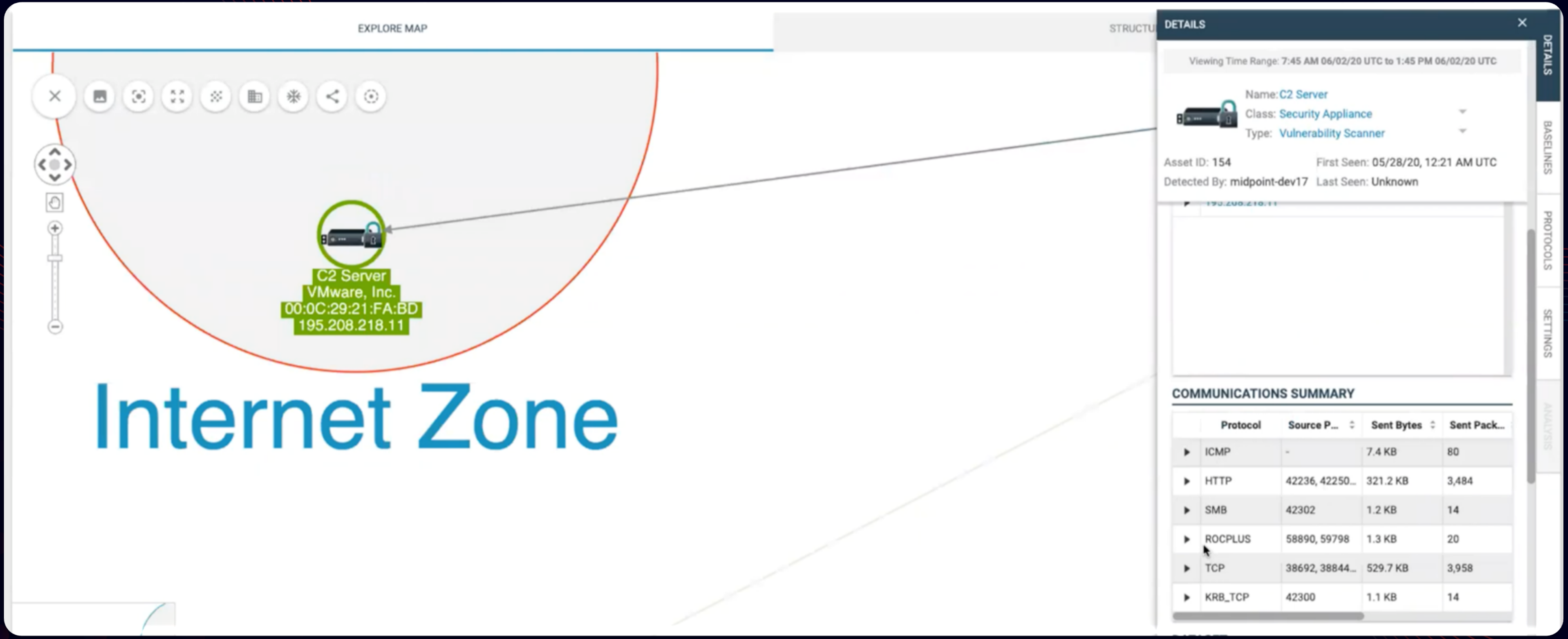
Zones:

Battery Vendor Network

DRAGOS PLATFORM FOR ICS/OT VISIBILITY



DRAGOS PLATFORM FOR ICS/OT VISIBILITY



DETAILS

Viewing Time Range: 7:45 AM 06/02/20 UTC to 1:45 PM 06/02/20 UTC

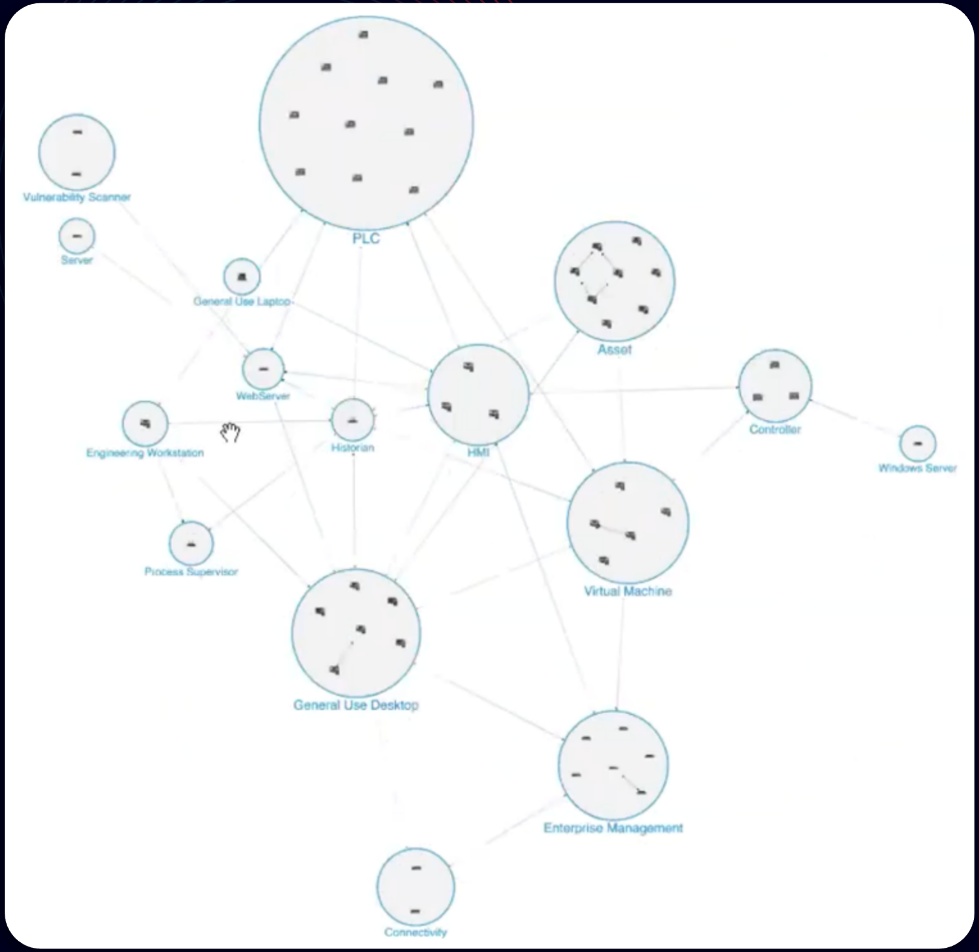
Name: C2 Server
Class: Security Appliance
Type: Vulnerability Scanner

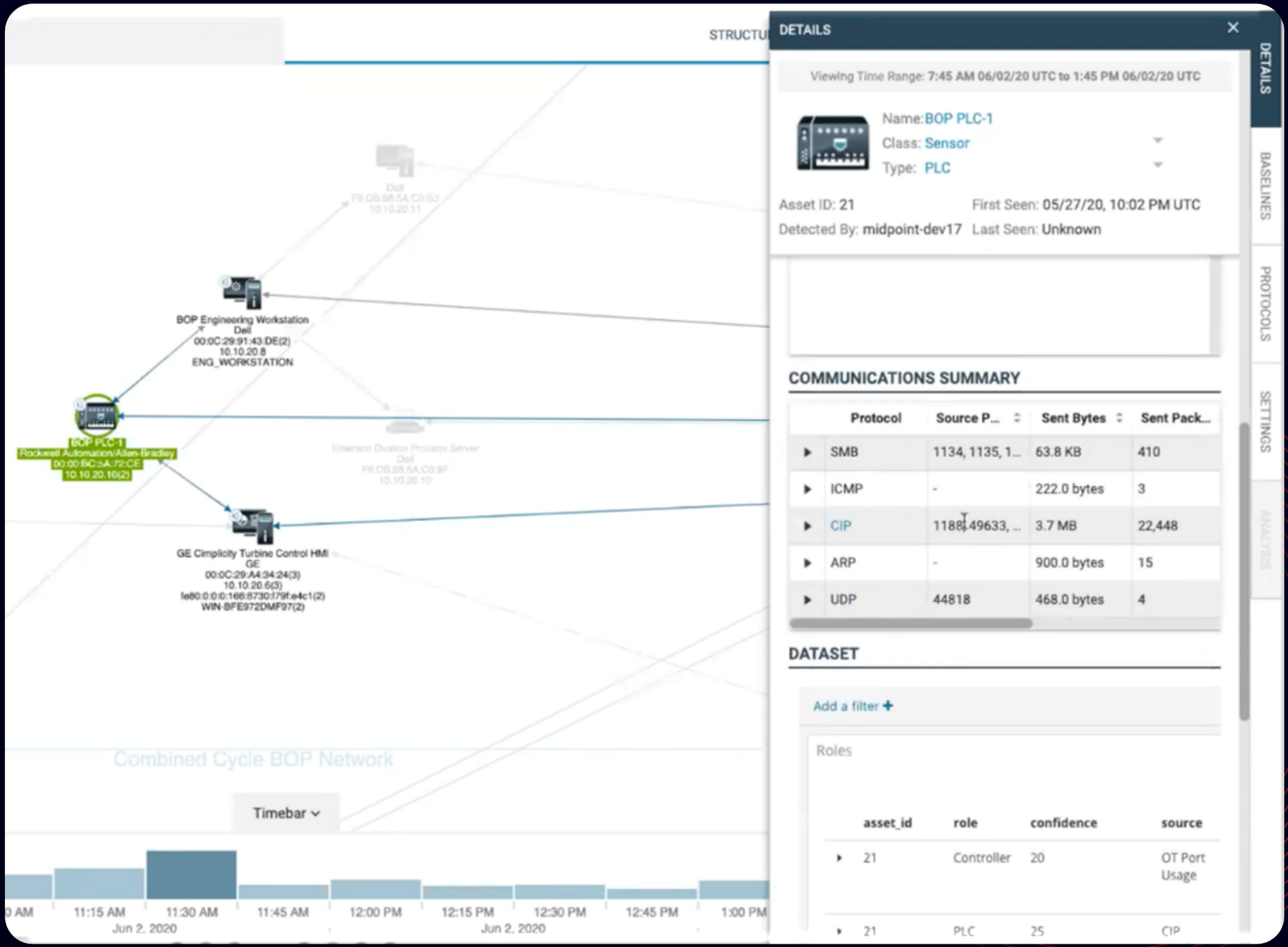
Asset ID: 154
First Seen: 05/28/20, 12:21 AM UTC
Detected By: midpoint-dev17
Last Seen: Unknown

COMMUNICATIONS SUMMARY

	Protocol	Source P...	Sent Bytes	Sent Pack...
▶	ICMP	-	7.4 KB	80
▶	HTTP	42236, 42250...	321.2 KB	3,484
▶	SMB	42302	1.2 KB	14
▶	ROCPLUS	58890, 59798	1.3 KB	20
▶	TCP	38692, 38844...	529.7 KB	3,958
▶	KRB_TCP	42300	1.1 KB	14

DRAGOS PLATFORM FOR ICS/OT VISIBILITY





DETAILS

Viewing Time Range: 7:45 AM 06/02/20 UTC to 1:45 PM 06/02/20 UTC

Name: BOP PLC-1
Class: Sensor
Type: PLC

Asset ID: 21
First Seen: 05/27/20, 10:02 PM UTC
Detected By: midpoint-dev17
Last Seen: Unknown

COMMUNICATIONS SUMMARY

	Protocol	Source P...	Sent Bytes	Sent Pack...
▶	SMB	1134, 1135, 1...	63.8 KB	410
▶	ICMP	-	222.0 bytes	3
▶	CIP	1188, 49633, ...	3.7 MB	22,448
▶	ARP	-	900.0 bytes	15
▶	UDP	44818	468.0 bytes	4

DATASET

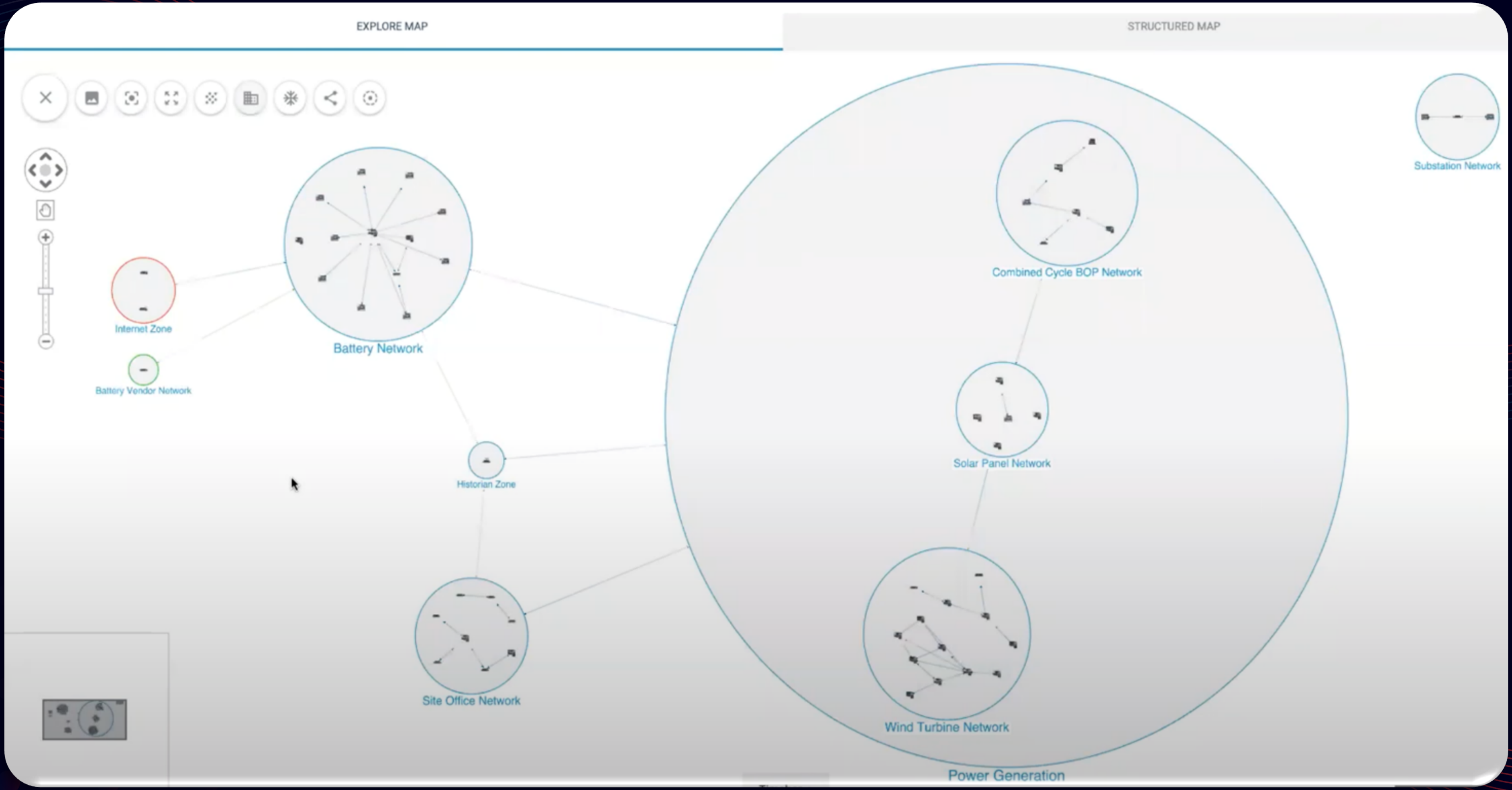
Add a filter +

Roles

	asset_id	role	confidence	source
▸	21	Controller	20	OT Port Usage
▸	21	PLC	25	CIP

DRAGOS WATERFALL® Stronger Than Firewalls

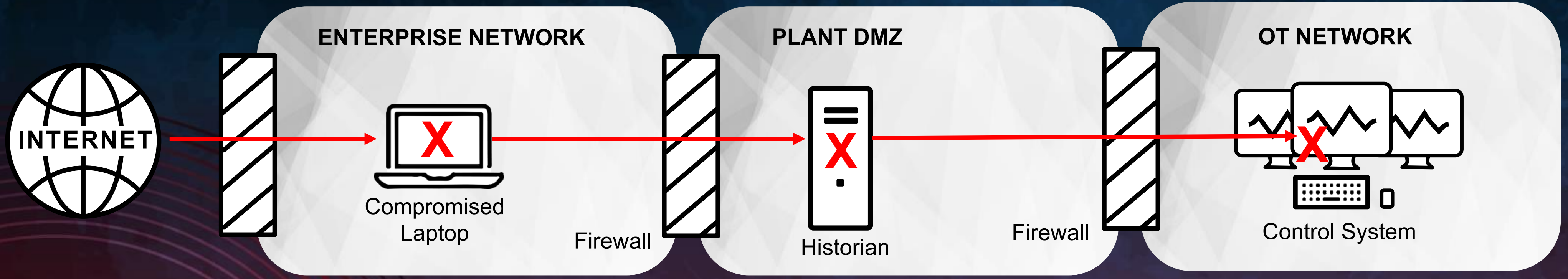
DRAGOS PLATFORM FOR ICS/OT VISIBILITY



Source Dragos, Inc.

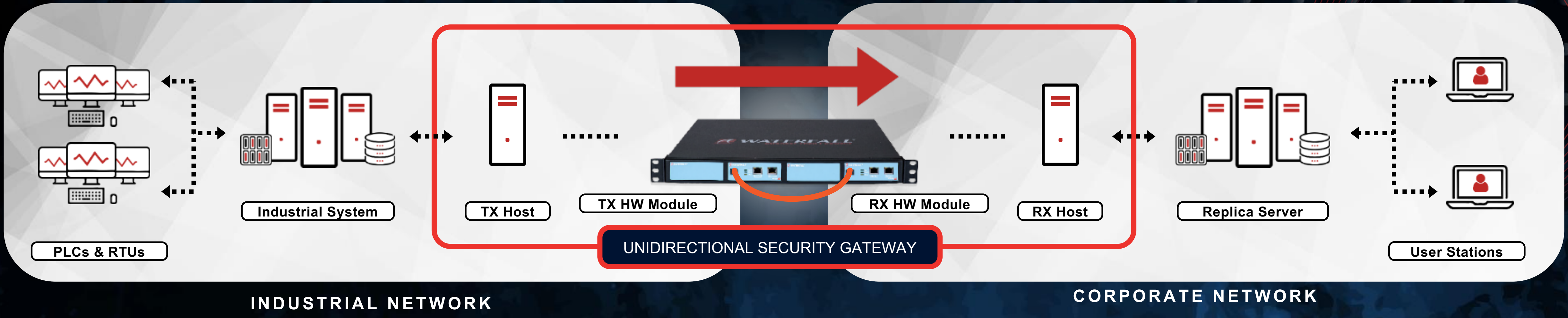
MODERN ATTACK PATTERN

- Modern attacks routinely pivot: stealing passwords, hashes, Kerberos tickets or other credentials
- Each compromised machine is operated remotely by the attacker, gathering information and credentials for next step
- Ultimate target is the control system – for sabotage, to plant ransomware, to steal secrets, or other consequences



DRAGOS WATERFALL® Stronger Than Firewalls

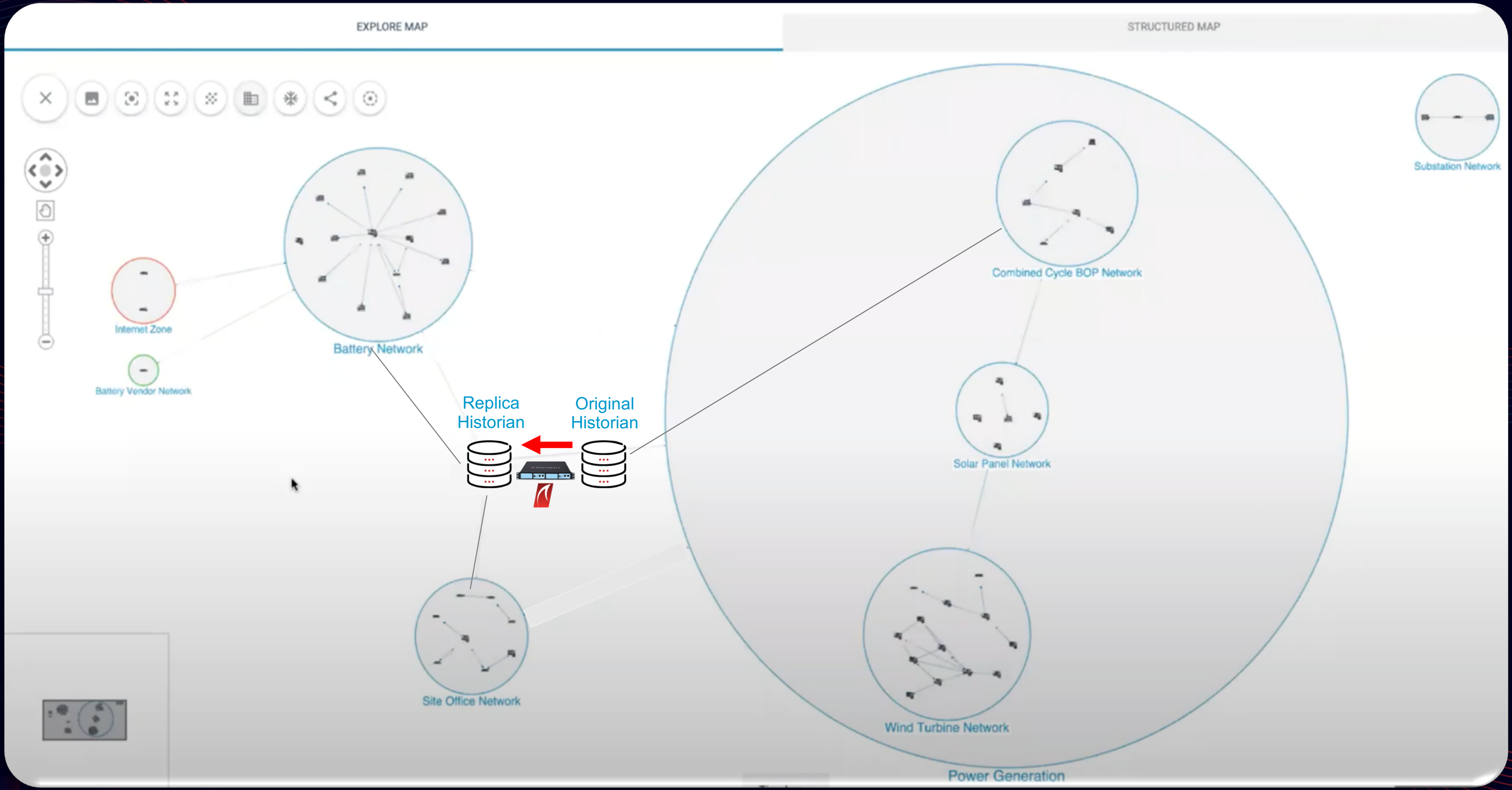
UNIDIRECTIONAL SECURITY GATEWAY



Hardware enforced security, providing a low maintenance, low impact and more secure means of segmentation than firewalls.

- Hardware sends information in only one direction, while software replicates servers & emulates devices/protocols
- Typically deployed from high secure to lower secure areas within OT networks, or directly from OT to IT networks
- Works with firewalls to provide a deeper protective layer for the most critical & zero trust OT areas
- No attack, no matter how sophisticated, can propagate back to the protected network through the gateway hardware
- Enforces Zero Trust through stand alone design

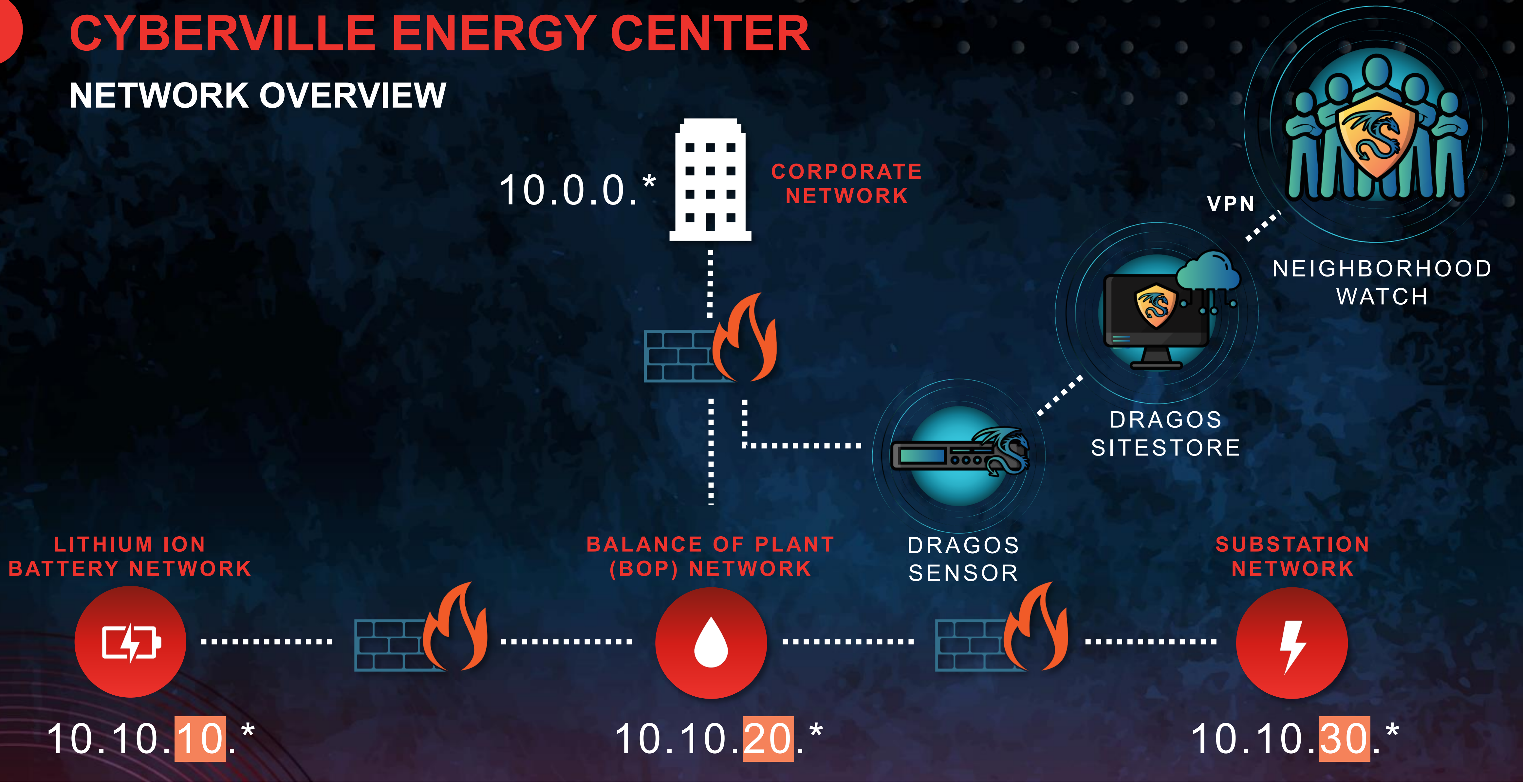
DRAGOS PLATFORM FOR ICS/OT VISIBILITY



Source Dragos, Inc.

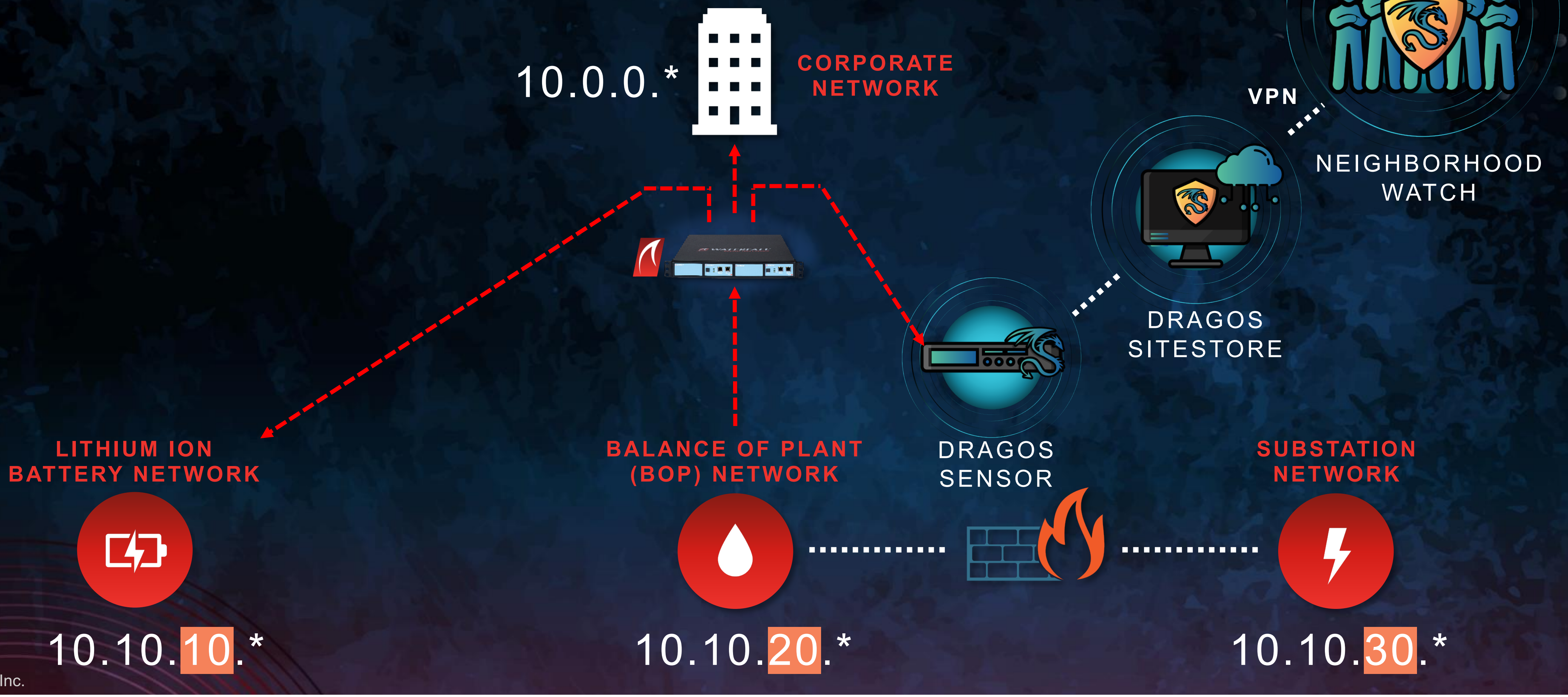
CYBERVILLE ENERGY CENTER

NETWORK OVERVIEW



CYBERVILLE ENERGY CENTER

NETWORK OVERVIEW



10.0.0.*

CORPORATE NETWORK

VPN

NEIGHBORHOOD WATCH

DRAGOS SITESTORE

DRAGOS SENSOR

LITHIUM ION BATTERY NETWORK

BALANCE OF PLANT (BOP) NETWORK

SUBSTATION NETWORK

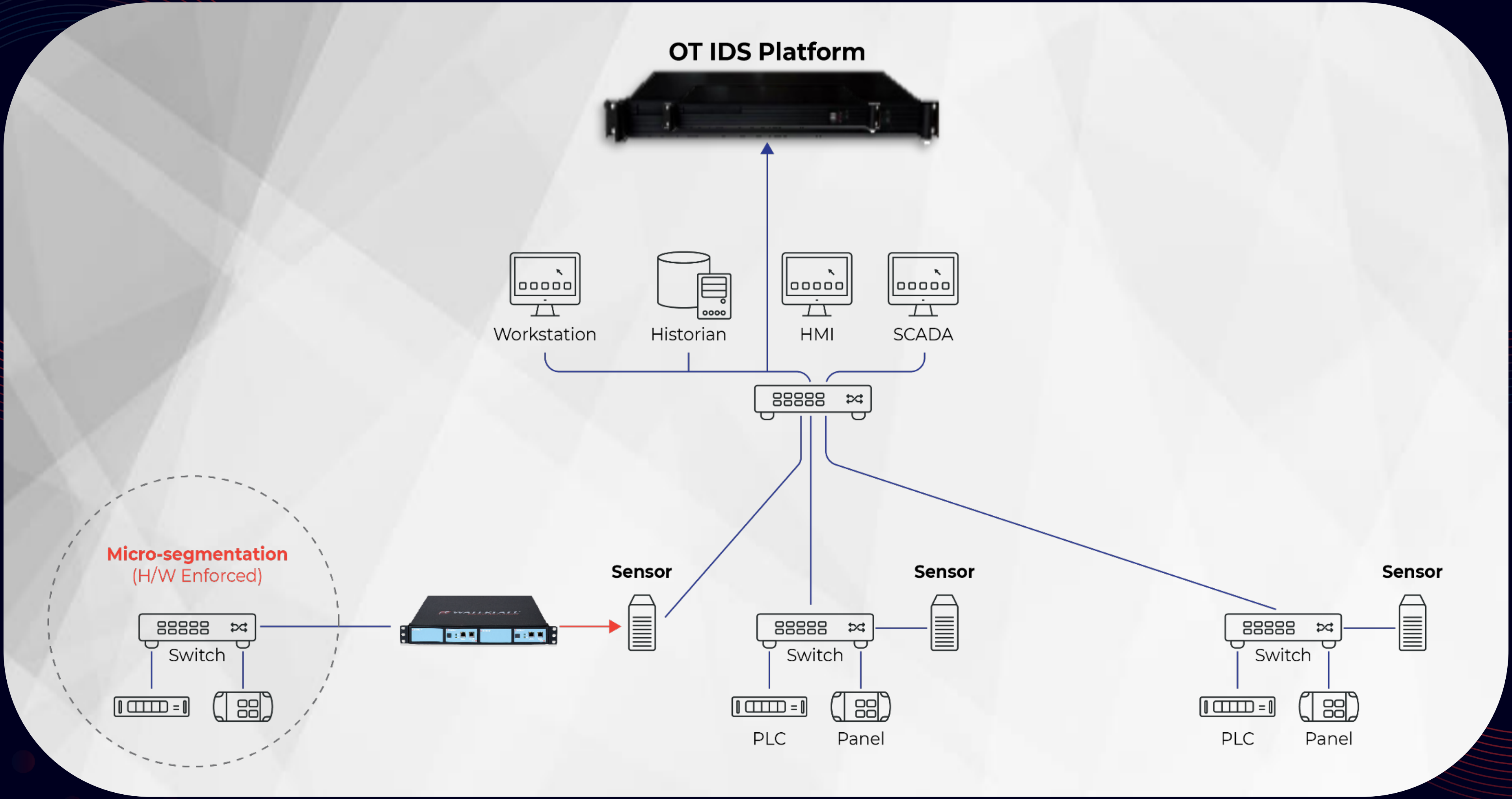
10.10.10.*

10.10.20.*

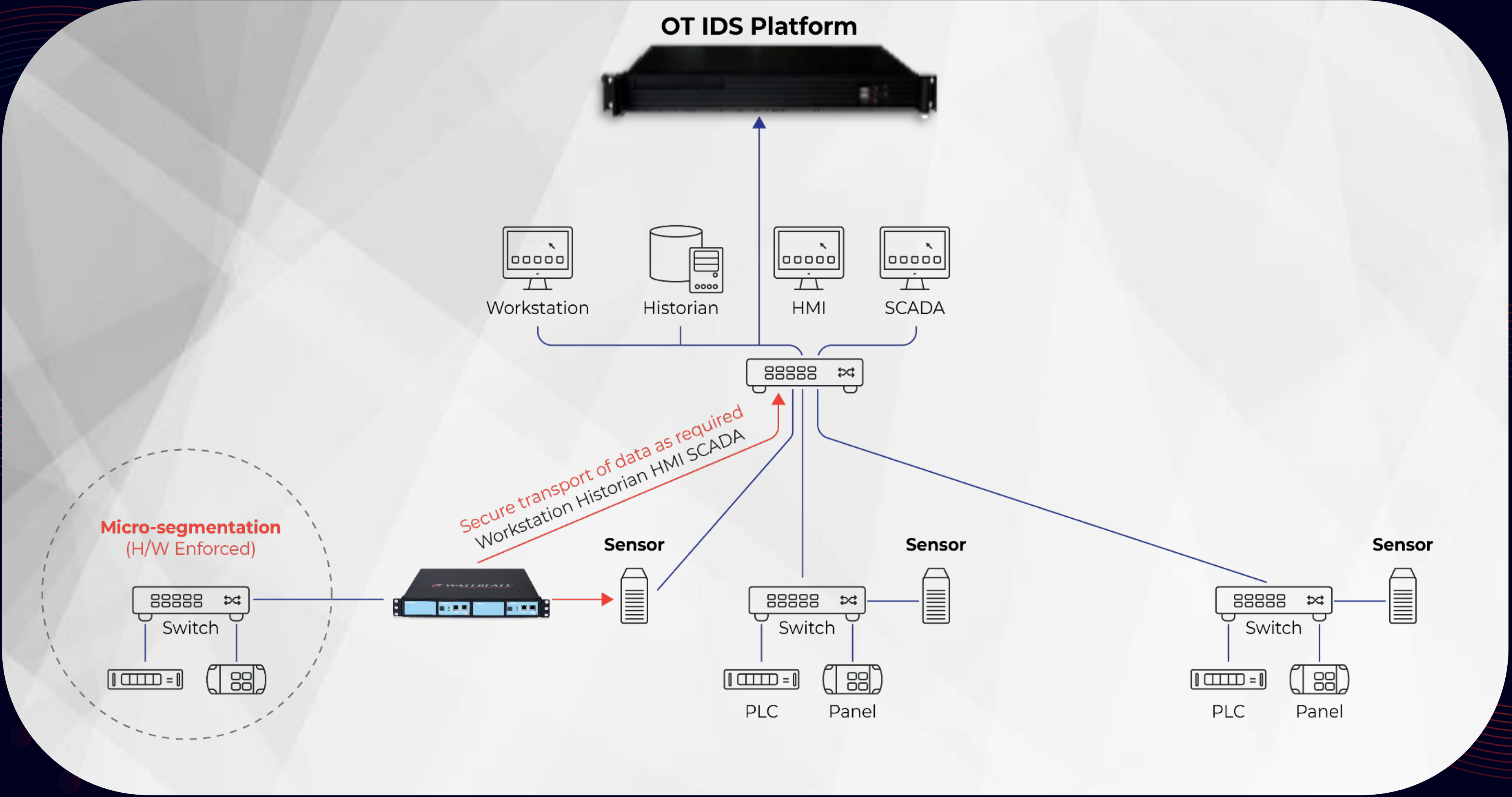
10.10.30.*

Source Dragos, Inc.

WATERFALL FOR IDS



WATERFALL FOR IDS AND WORKSTATION HISTORIAN, HMI & SCADA



WATERFALL INDUSTRIAL SOFTWARE SUPPORT

HISTORIANS & DATABASES

- OSIsoft: PI System, PI Asset Framework, PI Backfill
- GE: iHistorian, iHistorian Backfill, OSM, Bently-Nevada System1,
- Schneider-Electric: Wonderware eDNA, Wonderware Historian, Wonderware Historian Backfill, SCADA Expert ClearSCADA
- AspenTech IP.21, Rockwell FactoryTalk Historian, Honeywell Alarm Manager, Scientech R*Time,
- Microsoft SQL Server, Oracle MySQL, PostgreSQL

FILE TRANSFER

- Folder mirroring, Local Folders
- FTP/S, SFTP, TFTP, SMB, CIFS, NFS, HTTPFS
- Log Mirroring

INDUSTRIAL APPLICATIOINS AND PROTOCOLS

- Siemens S7 & PCS7 Historian
- OPC DA, A&E, HDA, HDA Backfill and OPC UA
- Emerson: EDS,
- Yokogawa OPC, GE iFix
- Modbus, DNP3, ICCP, IEC 60870-5-104, Omni Flow

OTHER CONNECTORS

- TimeSync, Netflow
- Video & audio streaming
- Kaspersky, Norton, FortiGate, Check Point, McAfee and OPSWAT Anti-virus updaters
- OPSWAT Metasploit
- WSUS and Linux Repository updaters
- Tenable Nessus Network Monitor, Nessus Security Center Updates
- Remote printing

ENTERPRISE MONITORING

- FireEye: Helix & Managed Defense
- Email/SMTP, SNMP, Syslog
- HP ArcSight, Splunk, Splunk Universal Forwarder, IBM QRadar, McAfee ESM, CyberX, Radiflow iSID, ForeScout Silent Defence, Dragos, Indegy,
- MSMQ, IBM MQ, Active Message Queue, AMQP, TIBCO,
- SolarWinds Orion, Thales Aramis, IOSight, Panorama

REMOTE ACCESS

- Remote Screen View
- Secure Bypass

DRAGOS WATERFALL® Stronger Than Firewalls

CERTIFICATIONS & ASSESSMENTS

- US DHS SCADA Security Test Bed
- Certified Common Criteria EAL4+ High Attack Potential
- Certified ANSSI CSPN – Security Certification First Level
- Japanese CSSC Test Bed
- Digital Bond Labs
- South Korea KC Certification
- Israel Testing Laboratories Certification
- National IT Evaluation Scheme (NITES) Singapore Govt

GLOBAL STANDARDS

- NERC NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
- ISA
- enisa THE EU CYBER SECURITY AGENCY
- NIST National Institute of Standards and Technology
- Department for Transport
- ICS-CERT INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
- ANSSI
- IEC INTERNATIONAL ELECTROTECHNICAL COMMISSION
- industrial internet CONSORTIUM

MANUFACTURING THREAT PERSPECTIVE

- 66 percent of attacks directly accessing the ICS network from the internet
- 100 percent of organizations had routable network connections into their operational environments
- New vulnerabilities F5, Palo Alto Networks, Citrix, and Juniper network devices been exploited by attackers

Source Dragos, Inc.

DRAGOS

Cyber Threat Perspective

MANUFACTURING SECTOR

NOVEMBER 2020

DRAGOS, INC.
Intel@Dragos.com
@DragosInc

Source Dragos, Inc.

SUMMARY

- Operational control workflows and key interdependencies are clarified
- Critical assets and operations are better identified and understood
- Critical areas have hardware-enforced segmentation and are protected to a zero trust level from cyber attack as well as operational errors
- Entire OT network, including segmented areas, are continuously monitored for operational malfunction and cyber intrusions
- Joint solution is passive, non-disruptive and low maintenance with little impact on overall operations.

Validation of Joint Deployment

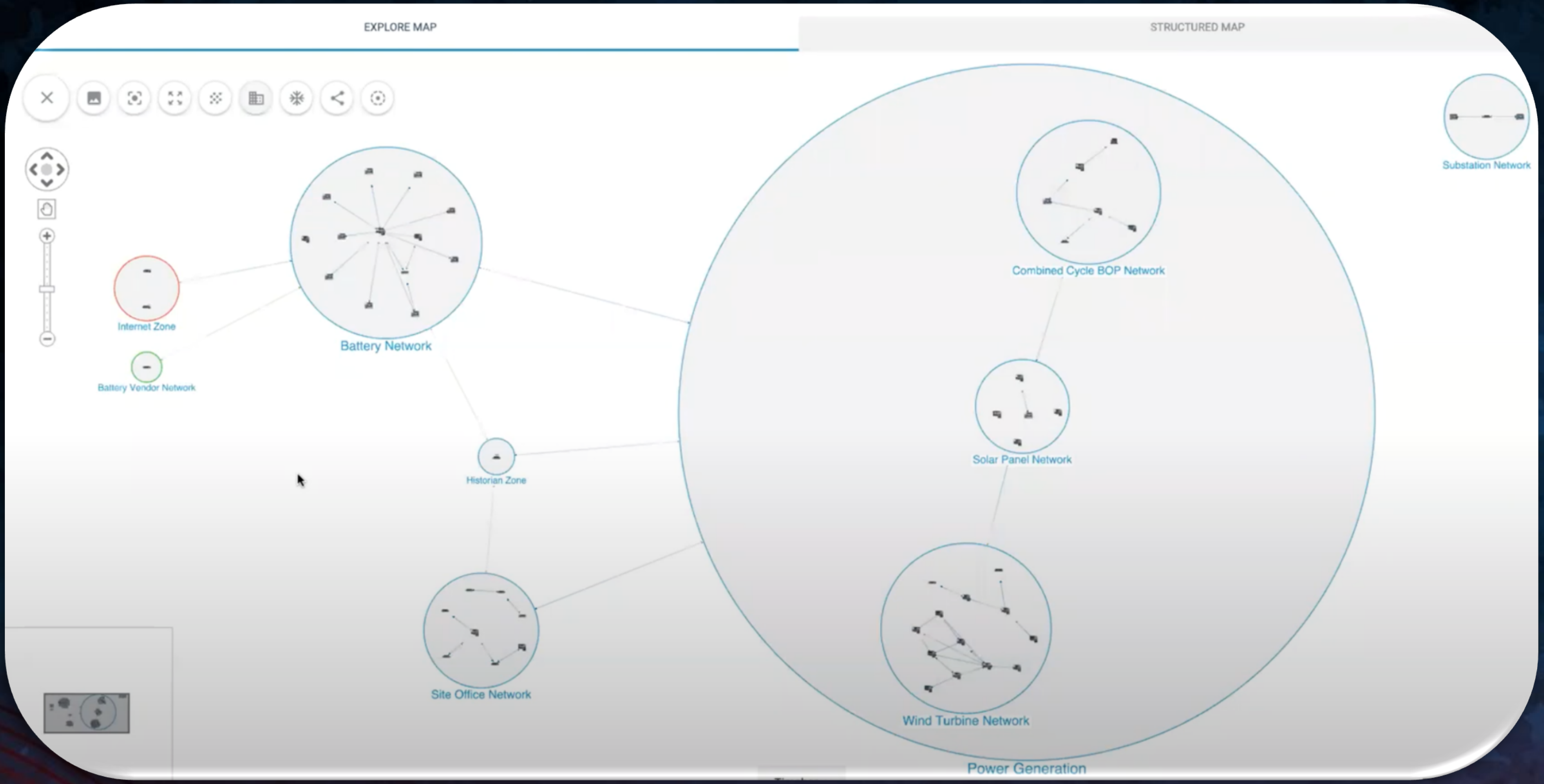


Image provided by Dragos, Inc.

Q & A