

NERC CIP-015: Monitoring Deep Inside Critical Networks to Keep Adversaries Outside

Speakers



Tim Conway
SANS Technical Director of ICS and SCADA programs



Robert M. Lee
Dragos CEO and Founder

Objectives

1 CIP-015-1 INSM Requirements

2 The Importance of Network Security Monitoring

3 Implementation Timeline

4 Building the Foundation for INSM

INSM is Coming! Why?



CIP-005



CIP-007



Guiding Lights

SANS | Research Program

Product Overview

OT Network Visibility and Detective Controls in a NERC CIP World

(Previously published as “Achieving OT Network Visibility and Detective Controls in a NERC CIP World”)

Written by **Tim Conway**
Originally Published June 2021
Updated June 2024

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

This is a Compliance Monitoring and Enforcement Program (CMEP) Practice Guide. It is developed exclusively by the ERO Enterprise under its obligations for independence and objectivity. This CMEP Practice Guide is intended for use by ERO Enterprise Staff to support consistency as they perform CMEP activities. This CMEP Practice Guide is posted publicly solely to provide transparency.

ERO Enterprise CMEP Practice Guide

Network Monitoring Sensors, Centralized Collectors, and Information Sharing

June 4, 2021

Background

To support successful implementation and compliance with the North American Electric Reliability Corporation (NERC) Reliability Standards, the Electric Reliability Organization (ERO) Enterprise¹ adopted the Compliance Guidance Policy.² The Compliance Guidance Policy outlines the purpose, development, use, and maintenance of guidance for implementing Reliability Standards. According to the Compliance Guidance Policy, Compliance Guidance includes two types of guidance – (1) Implementation Guidance and (2) Compliance Monitoring and Enforcement Program (CMEP) Practice Guides.³ This document summarizes some of the requirements in NERC Reliability Standards, but the language of the Reliability Standards is enforceable and supersedes any description in this document.

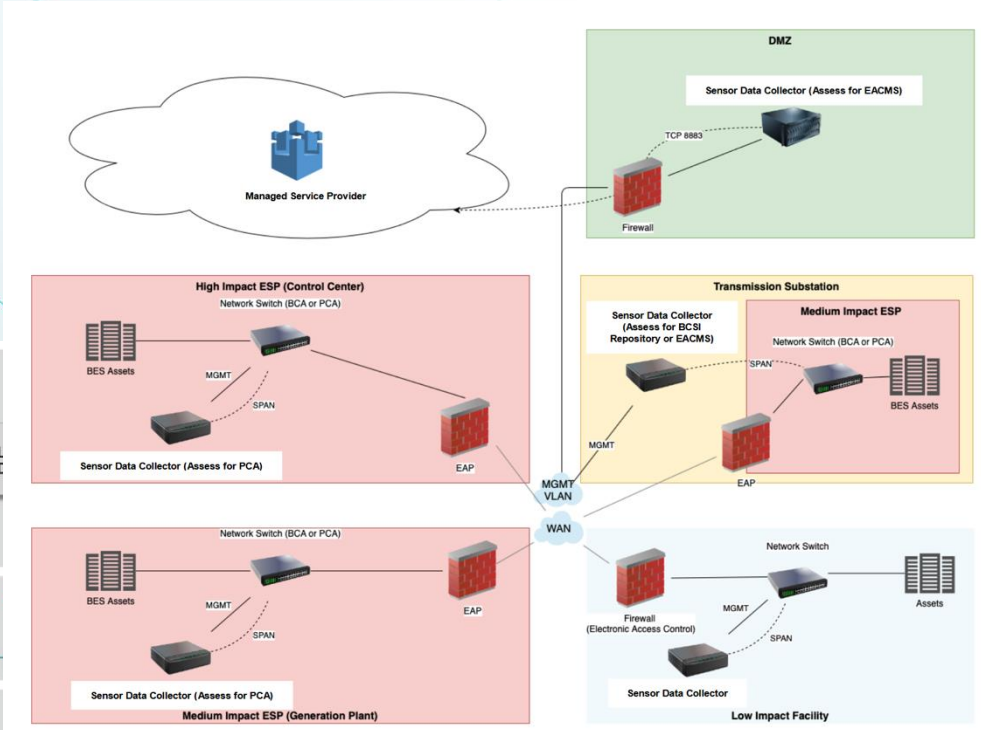
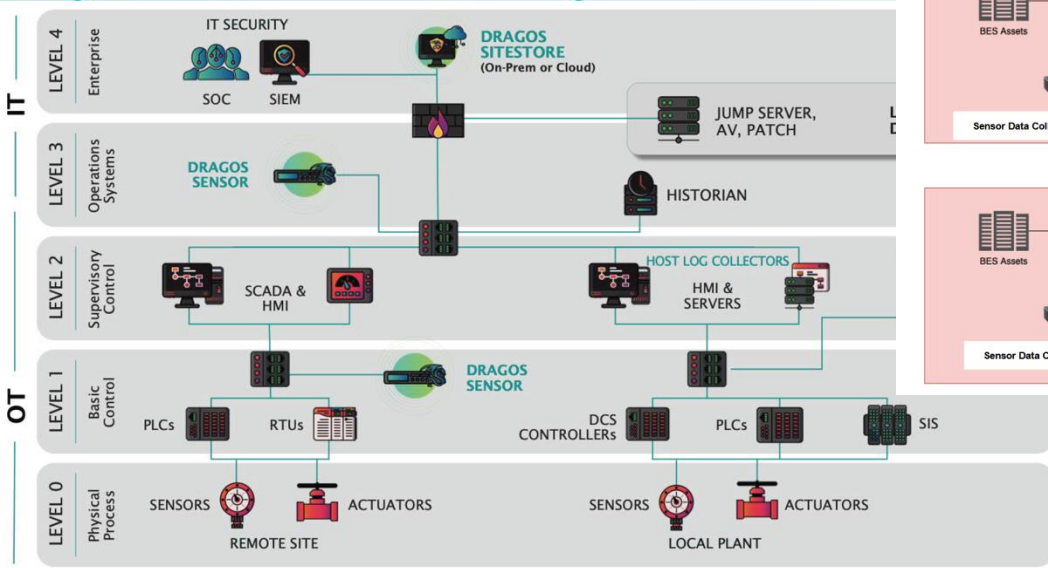
Purpose

On April 20, 2021, the Department of Energy (DOE) launched an initiative, referred to as the 100-day plan, to enhance the cybersecurity of electric utilities' industrial control systems (ICS) and secure the energy sector supply chain. As part of the 100 day plan, DOE is seeking to advance technologies and systems that will provide cyber visibility, detection, and response capabilities for ICS of electric utilities. As stated in DOE's [press release](#), the initiative modernizes cybersecurity defenses and:

- Encourages owners and operators to implement measures or technology that enhance their detection, mitigation, and forensic capabilities;
- Includes concrete milestones over the next 100 days for owners and operators to identify and deploy technologies and systems that enable near real time situational awareness and response capabilities in critical ICS and operational technology (OT) networks;

SANS | Research Program

Guiding Lights



CIP-015 – Internal Network Security Monitoring

CIP-015-1 R1.1

Implement, using a risk-based rationale, network data feed(s) to *monitor* network activity; including connections, devices, and network communications.

CIP-015-1 R1.2

Implement one or more method(s) to *detect* anomalous network activity using the network data feed(s) from Part 1.1.

CIP-015-1 R1.3

Implement one or more method(s) to *evaluate* anomalous network activity detected in Part 1.2 to determine further action(s).

CIP-015-1 R2 and R3

R2 - Retain internal network security monitoring data associated with network activity determined to be anomalous

R3 - Protect data retained to mitigate the risks of unauthorized deletion or modification

CIP-015-1 Internal Network Security Monitoring (INSM) Requirements

Req. 1

Requires Responsible Entities to implement INSM within ESPs for all High and Medium Impact BES Cyber Systems with ERC

Expanded scope expected in version 2, which will include EACMS and PACS outside of the ESP

Collect ... connections, devices, network, communication (R1.1)

Detect anomalous network activity (R1.2)

Evaluate anomalous activity detected to determine action (R1.3)

Technical Rationale

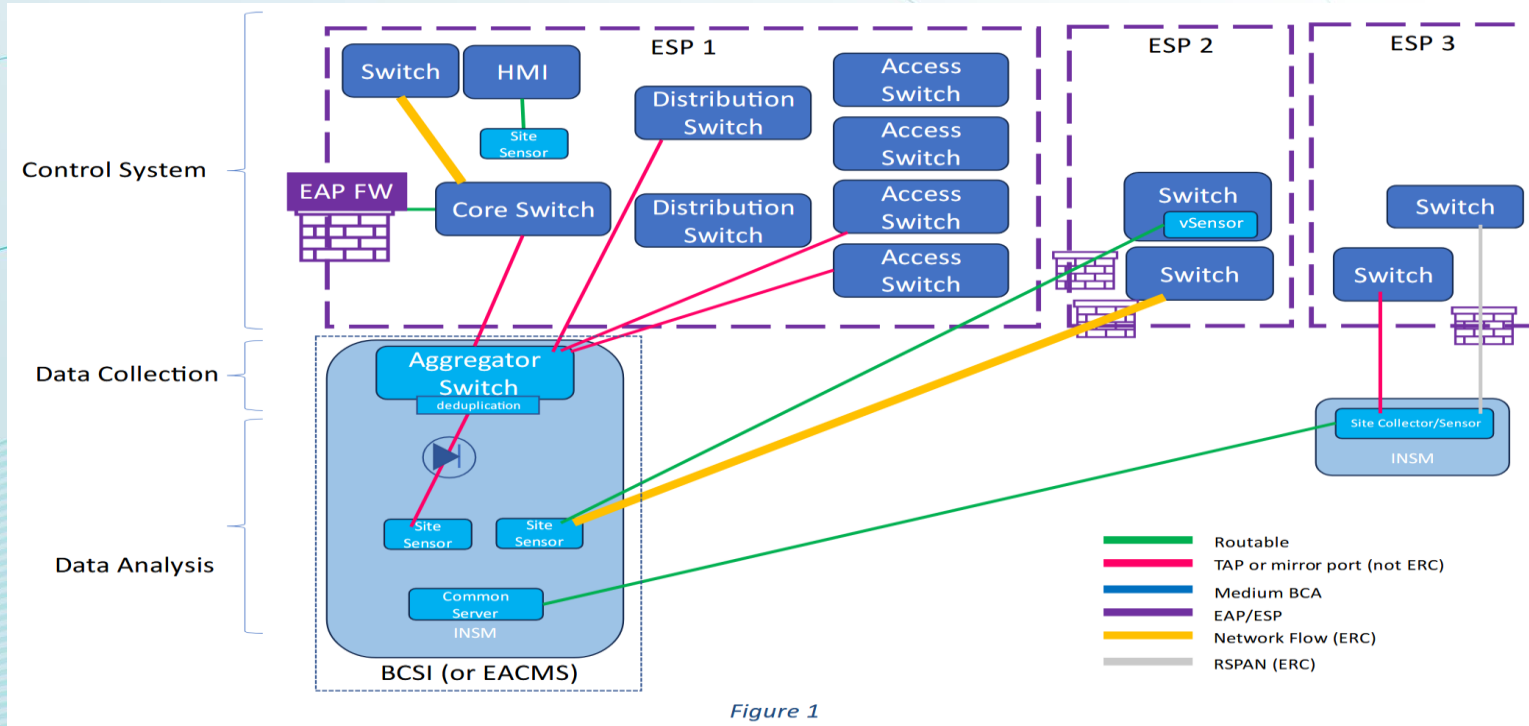


Figure 1

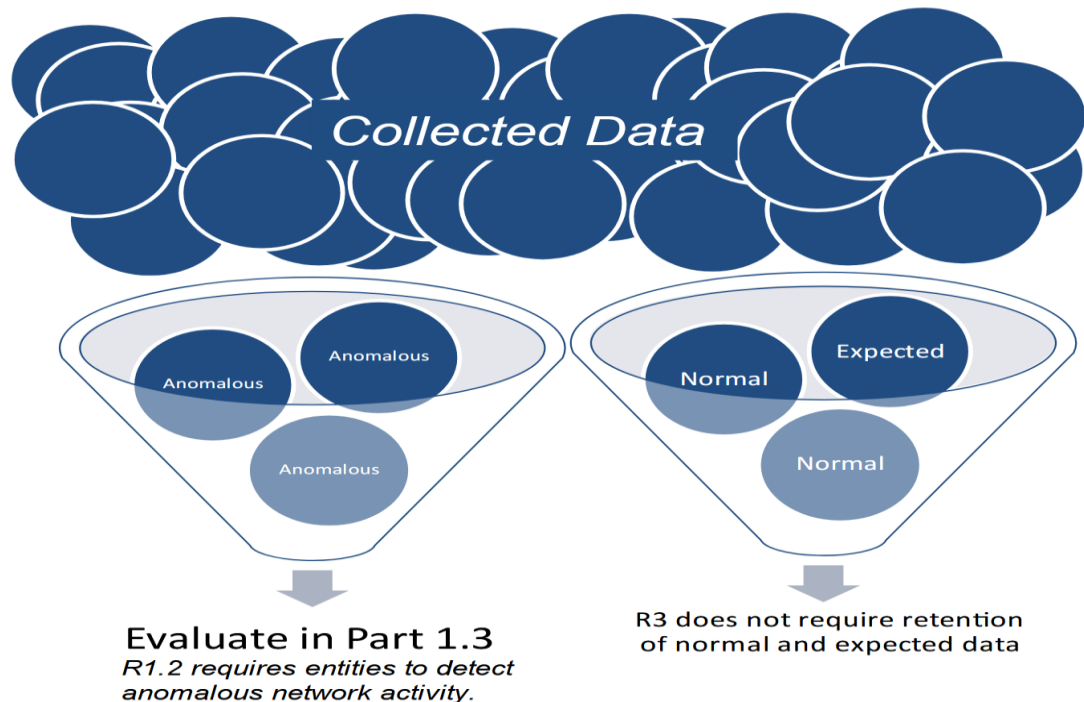
Technical Rationale

R1.1 requires entities to implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications.

R1.2 requires entities to detect anomalous network activity.

R2 requires entities to protect the data collected from unauthorized deletion or modification.

R3 requires entities to retain the data related to anomalous activity for analysis in 1.3 and potentially to meet CIP-008 requirements if the anomalous activity is associated with a cybersecurity incident or attempt to compromise.



CIP-015-1 Internal Network Security Monitoring (INSM) Requirements

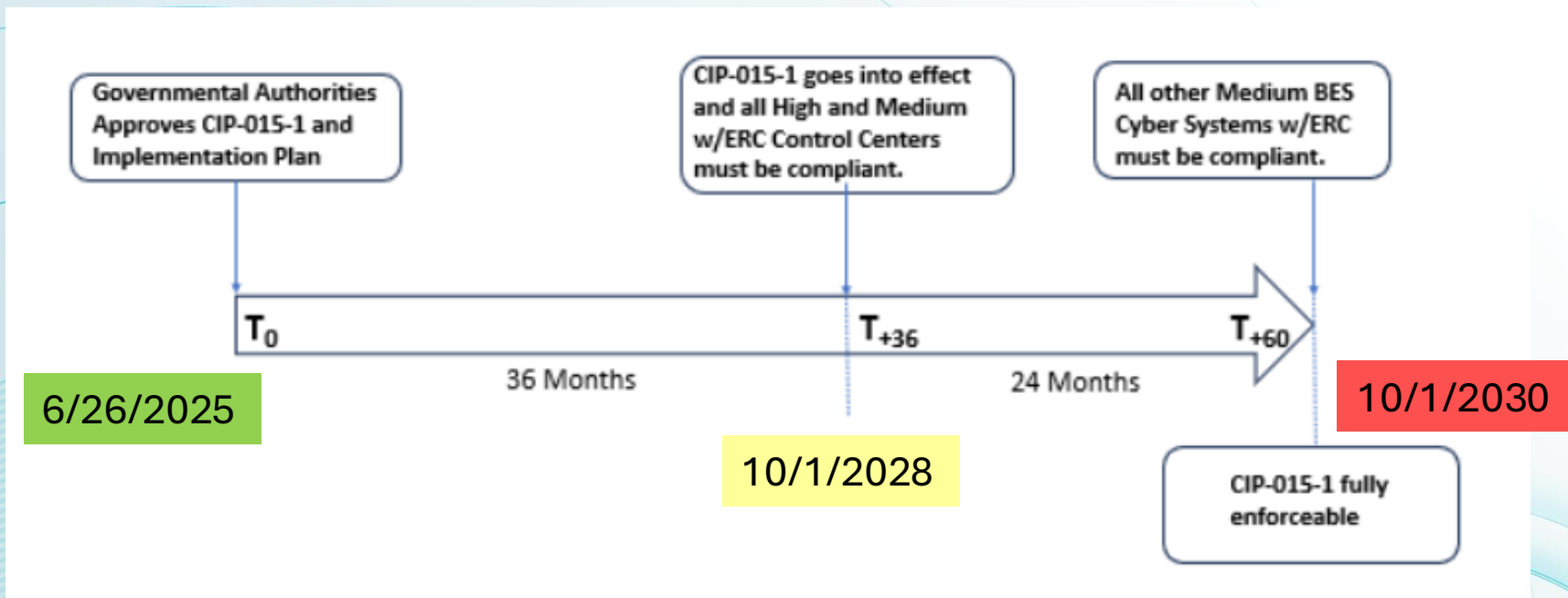
Req. 2

Protect INSM data from unauthorized deletion or modification.

Req. 3

Retain INSM data associated with network activity determined to be anomalous until actions are complete (Requirement R1, Part 1.3).

INSM is Coming..... ?



When Prevention Fails



August
2024



VOLTZITE + Cisco, Fortinet, Ivanti, F5, SonicWall, PaloAlto

Has utilized 0-days used by other PRC adversaries

Quickly integrate and then target devices from released POCs
for remote access assets or other internet-exposed assets

April
2024



BAUXITE + Sophos Firewall (CVE-2022-3236, CVE-2022-1040)

BAUXITE exploited specific Sophos Firewall vulnerabilities to plant the
IOControl backdoor

August
2024



HELLDOWN + Zyxel Firewalls (CVE-2024-42057, CVE-2023-28771)

Unauthenticated command injection allowing remote code execution

Exploited by HELLDOWN targeting manufacturing with leaked Lockbit builder

May
2025



PARASITE + Credential Stuffing + ZKTeco (CVE-2023-38950)

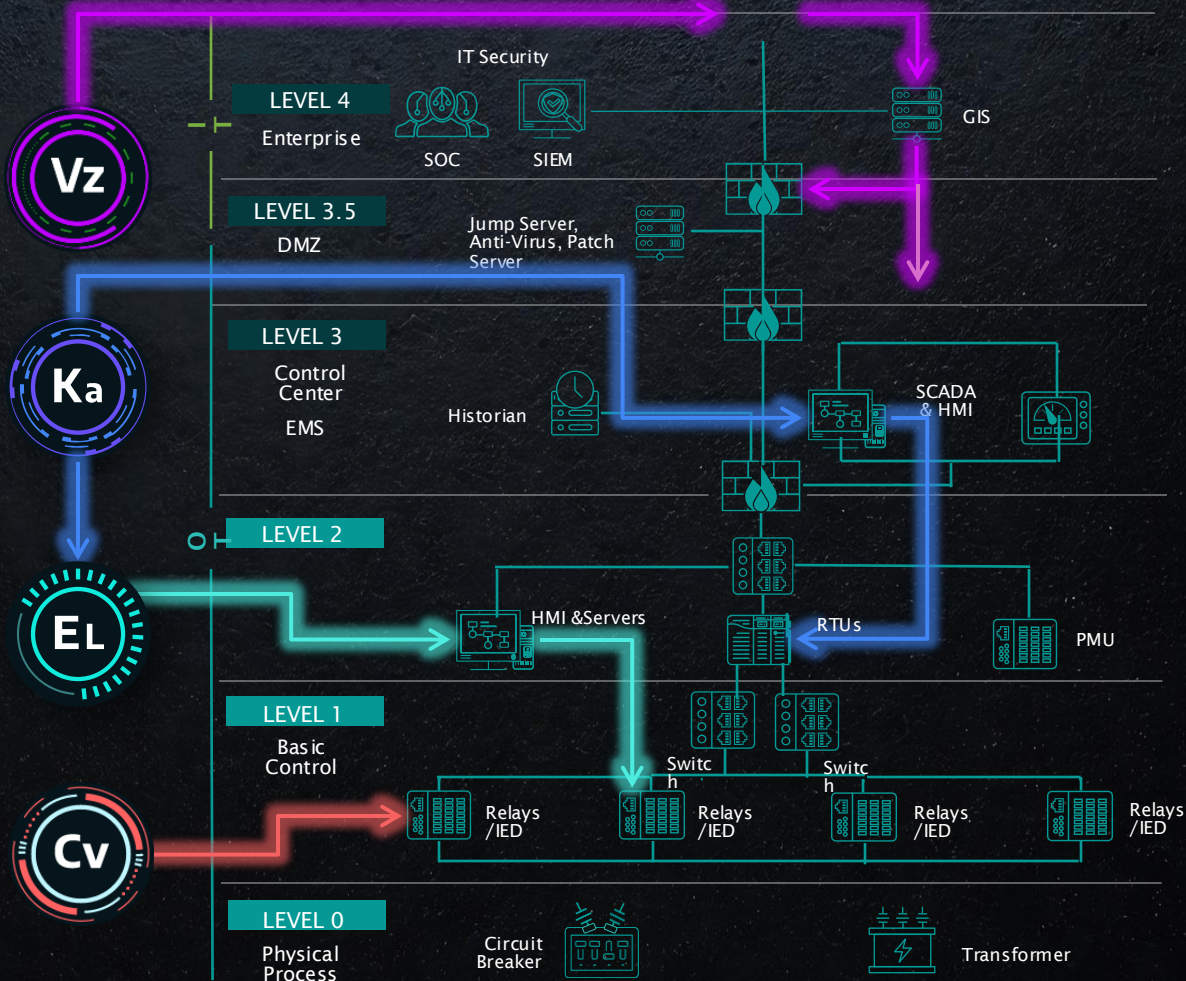
Stolen VPN administrator credentials

Exploited publicly facing ZKTeco BioTime v8.5.5 software

Why INSM is Critical

Threat groups are targeting the **electric sector**.

Utilizing techniques that circumvent traditional network perimeter-based security controls aimed at detecting the initial stages of an attack





Key CIP-015 Dates Coming

2025

June 26, 2025

FERC issued Order No. 907 formally approving NERC CIP-015-1

2026

September 2, 2026

NERC is required to submit modifications to CIP-015-1 to include Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS) outside of the Electronic Security Perimeter (ESP)

2028

October 1, 2028

CIP-015-1 goes into effect for all High Impact and Medium Impact Control Centers and backup Control Centers with External Routable Connectivity (ERC)

2030

October 1, 2030

CIP-015-1 goes into effect for all other Medium BES Cyber Systems with ERC



OT Cybersecurity for Industrial Operations

Technology that understands OT systems & maximizes operations availability. Built for practitioners by the most experienced team of ICS/OT security specialists.

HQ | Hanover, MD, USA

420+ Customers | US & Canada, Australia & NZ, Singapore, Japan, Middle East, & Europe

OT CYBER THREAT INTELLIGENCE

Engage & Educate the Community

Intel team creating reports, answering RFI's, & embedding in orgs with Concierge Analysts

Codify ANALYTICS

OT specific Threat behaviors, IOCs, & vulnerability data



North America's Leading INSM Solution for the Electric Industry

OT CYBER SERVICES

Partner with Customers on Their Journey

TTX's, Architecture Reviews, Compromise Assessments, Pen tests, & OT Incident Response

Codify EXPERTISE

Features, Dashboards, Playbooks built by practitioners for practitioners

INSM with Dragos



R1: Implement processes for INSM of networks protected by the ESP(s) of High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity to provide methods for detecting and evaluating anomalous network activity.

R1.1: Implement, using risk-based rationale, network data feed(s) to monitor activity	<ul style="list-style-type: none">• OT-native passive network monitoring with Dragos Sensors• Edge-compute-enabled east-west monitoring• Single- and multi-sensor threat analytics across trusted zones• Active collection to enrich asset inventory and context
R1.2: Detect anomalous network activity	<p>Intelligence-driven detections with OT context produce high-confidence alerts</p> <ul style="list-style-type: none">• Anomaly-Based Detections<ul style="list-style-type: none">• Modeling Detections• Configuration Detections• Intelligence-Driven Detections<ul style="list-style-type: none">• Threat Behavioral Detections (e.g., TTPs)• Indicators/IoC Detections (IoCs)
R1.3: Evaluate anomalous network activity detected	<ul style="list-style-type: none">• Panel displays four threat detection types for triage• Raw historical evidence supports deep investigation• Query Focused Datasets (QFDs) enable structured, retrospective analysis• Expert-authored playbooks and case management guide consistent evaluation• Integrated ICS/OT threat intelligence adds context and informs escalation

INSM with Dragos



R1: Implement processes for INSM of networks protected by the ESP(s) of High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity to provide methods for detecting and evaluating anomalous network activity.

R2: Retain INSM data associated with anomalous network activity

- Collecting and storing network activity data feeds in support of R1 is a core capability of the Platform
- Indefinite retention for cases opened in the Platform and all associated evidence
- Dataset sizing and associated online/offline storage retention are expandable
- Backup and restore capabilities ensure subjected data is retained, recoverable, and available for audit and investigation

R3: Protect INSM data collected in support of R1 and data retained in support of R2 to mitigate the risks of unauthorized deletion or modification

- System configuration details available including centralized audit logging
- Multi-Factor Authentication (MFA)
- Data retention controls actively enforced, with records verifying last successful backup
- Ability to backup to external locations to ensure redundancy
- Indefinite retention for cases opened in the Platform and all associated evidence

Actions to Consider Now

- ☐ Review current list of High-Impact and Medium-Impact (with ERC) facilities.
- ☐ Identify existing data collection capabilities within ESPs.
- ☐ Consider the feasibility of performing network activity data feed collection from existing network infrastructure.
- ☐ Identify where the analysis task of evaluating detected anomalous activity would be performed.
- ☐ Identify the INSM solutions that best fit in your environment.
- ☐ Prioritize projects across High and Medium-Impact Control centers with ERC.

Actions to Consider Next

- ❑ Develop a workforce plan addressing gaps in job roles and staffing levels. Where appropriate, provide necessary training to develop individuals key to project and program initiatives.
- ❑ Leverage existing test environments to evaluate solutions or tune selected solution detection capabilities.
- ❑ Develop processes supporting CIP-015-1 R 1.1–1.3.
- ❑ Establish playbooks and case management tools in support of R 1.3.
- ❑ Test capabilities by leveraging a CIP-010 active vulnerability assessment in a test environment.
- ❑ Consider projects across other Medium-Impact facilities with ERC.
- ❑ Consider implementation needs for the requirements with expanded applicability to EACMS and PACS.

Actions to Consider if Resources Exist

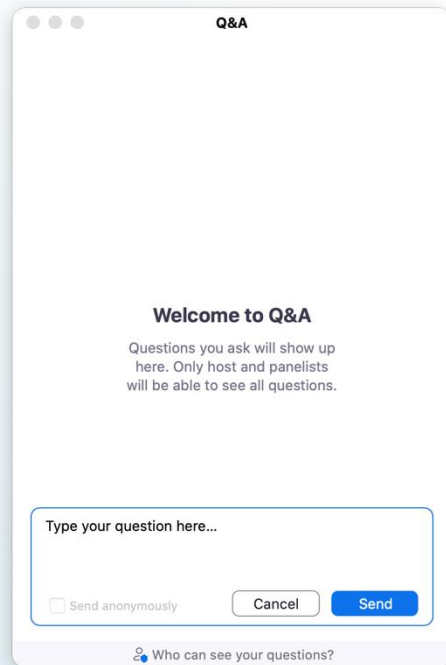
Continuously monitor and contribute:

- ❑ Participate in further industry activity on the directed changes from FERC to CIP-015-1.
- ❑ Review all systems currently identified as EACMS and PACS, and then consider implementation of CIP-015-1 requirements for those CIP-networked environments.
- ❑ Participate in Regional Entity collaboration and outreach efforts focused on CIP-015.
- ❑ If necessary, participate in industry collaboration activity on risk-based data feed selection approaches and consistent treatment of the term “anomalous” across entities.

Q&A

Use **Zoom's** Q&A window to submit questions to our presenters.

Type your question, tell us if it's for a specific presenter, and then click Send.

A screenshot of the Zoom Q&A window. The window has a title bar with three dots and the text "Q&A". The main content area says "Welcome to Q&A" and "Questions you ask will show up here. Only host and panelists will be able to see all questions." Below this is a text input field with the placeholder "Type your question here...". At the bottom left of the input field is a checkbox labeled "Send anonymously". At the bottom right are two buttons: "Cancel" and "Send". At the very bottom of the window is a link that says "Who can see your questions?".

Q&A

Welcome to Q&A

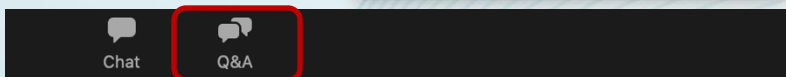
Questions you ask will show up here. Only host and panelists will be able to see all questions.

Type your question here...

☐ Send anonymously

Cancel Send

[Who can see your questions?](#)



Acknowledgments

Thanks to our sponsor:



To our special guest: **Robert M. Lee**

And to our attendees, thank you for joining us today!