DRAGOS®

NERC CIP-015

Internal Network Security Monitoring

Phil Tonkin
Shelby Brooks

Objectives

1. NERC CIP-015 INSM Requirements
2. Threat Groups are Targeting Electric
3. How Dragos Platform Enables INSM Requirements
4. The Importance of Threat Intelligence
5. Time is Now: Understanding Incentives
6. Implementation Timeline
7. Why Dragos for INSM?

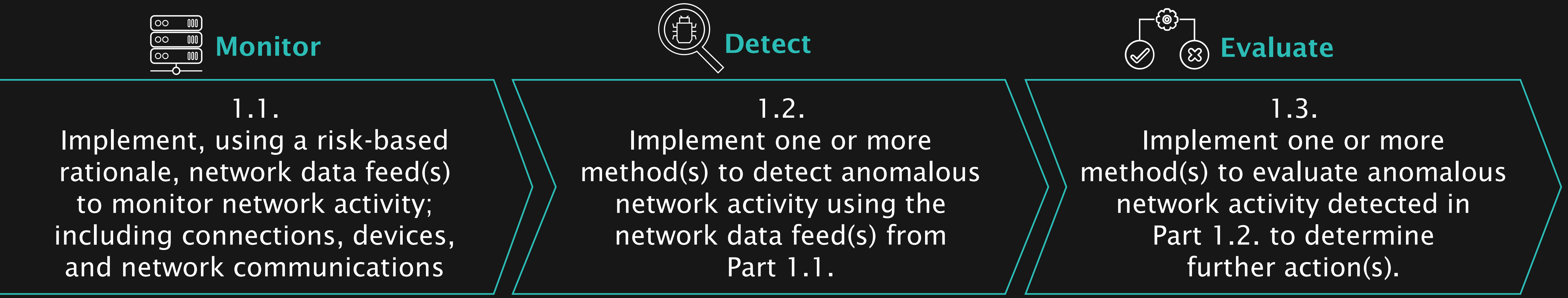
CIP-015 Internal Network Security Monitoring (INSM)

Objective: Monitor internal network traffic—specifically, East-West (lateral) movements within a trusted zone—to better detect adversaries who have circumvented traditional perimeter defenses to detect and respond faster.

INSM Requirements Summary

1st Requirement

Each Responsible Entity shall implement one or more documented process(es) for internal network security monitoring of networks protected by the Responsible Entity’s ESPs 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.



Monitor

1.1.
Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications

Detect

1.2.
Implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1.

Evaluate

1.3.
Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s).

INSM Requirements Summary

2nd Requirement

Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to **retain internal network security monitoring data** associated with network activity determined to be anomalous by the Responsible Entity at a minimum until the action is complete in support of Requirement R1, Part 1.3.

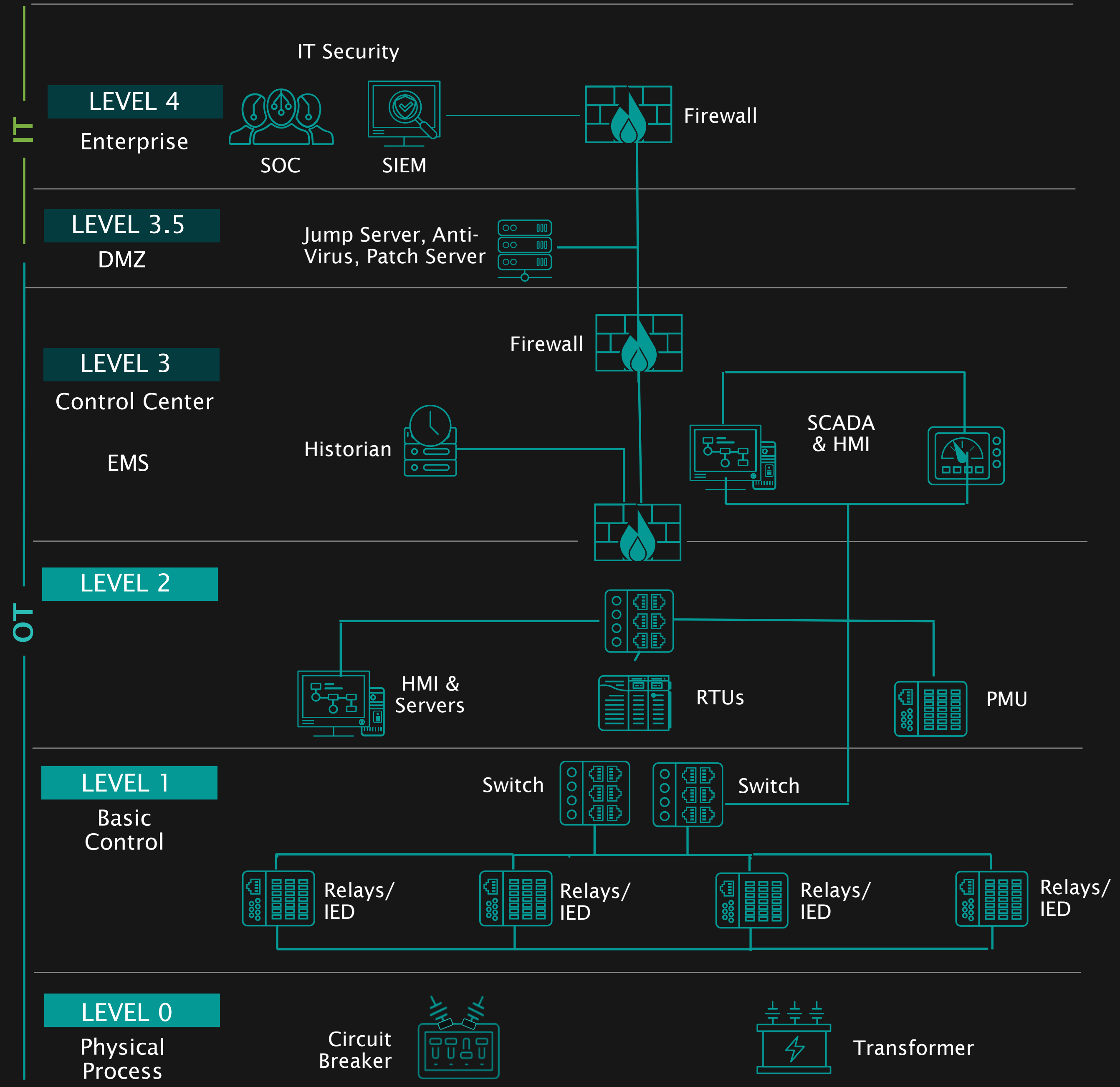
3rd Requirement

Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to **protect internal network security monitoring data** collected in support of Requirement R1 and data retained in support of Requirement R2 to mitigate the risks of unauthorized deletion or modification.

Why INSM is Critical

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

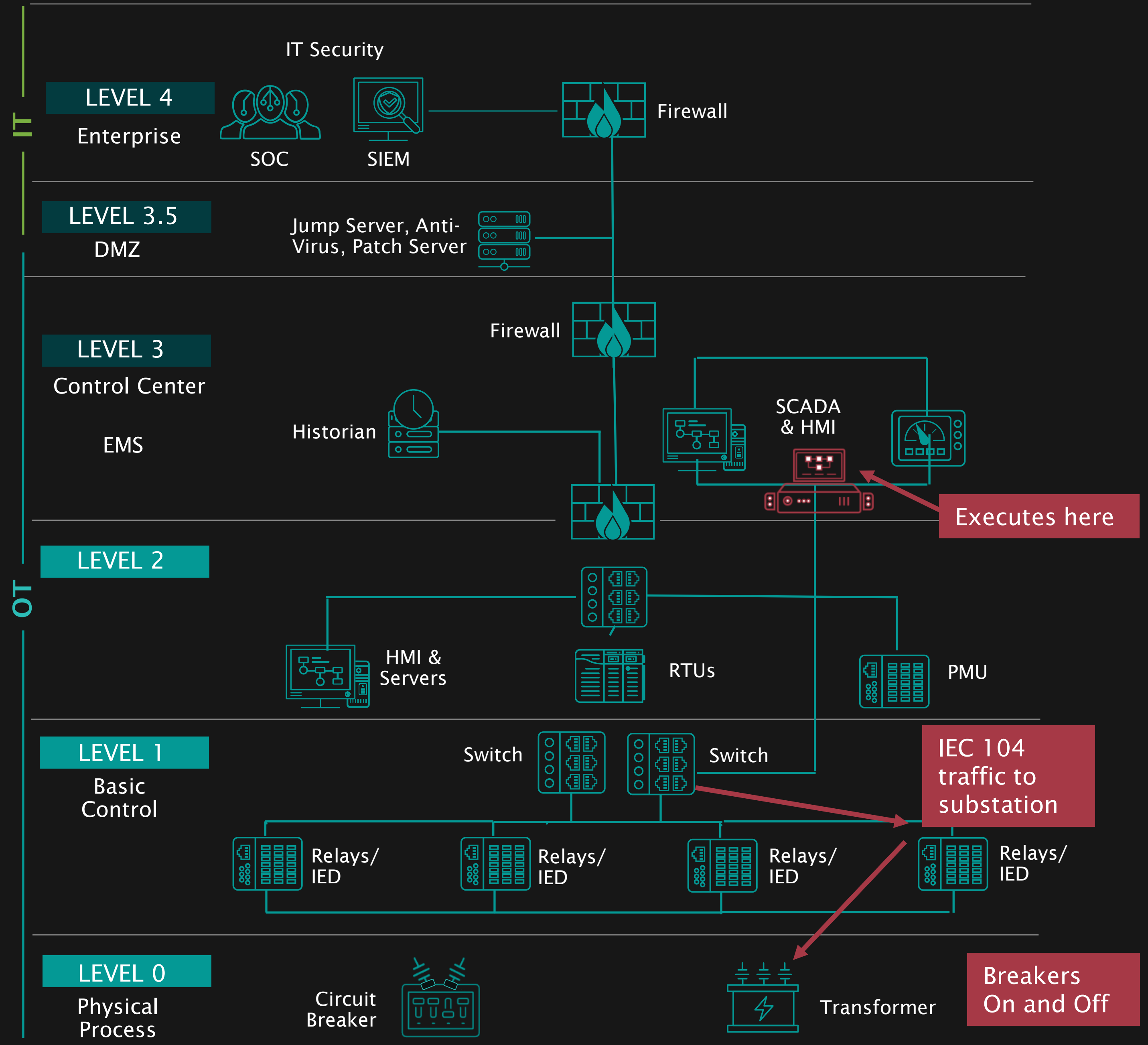
Utilizing techniques that circumvent traditional network perimeter-based security controls aimed at detecting the initial stages of an attack.



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.



Dragos Platform Satisfies INSM Requirements

Monitor

OT-Native Passive Network Monitoring (Dragos Sensors)

- Single-Sensor and Multi-Sensor Threat Analytics
- Edge-Compute-Enabled East-West Monitoring
- Active Scanning

Detect

Anomaly-Based Detections

- Modeling Detections
- Configuration Detections

Intelligence-Driven Detections

- Indicators/IOC Detections
- Threat Behavior Detections

Evaluate

- Case Management for IR
- Notification Triage
- Raw Historical Evidence
- OT Watch
- Neighborhood Keeper
- Expert Response Playbooks
- ICS/OT Threat Intelligence

Early Adopter Incentives

Early starters benefit from quicker financial returns

FERC issued Order No. 893 in 2023:

- Provides deferred cost recovery incentives to help utilities invest in advanced cybersecurity technology
- Includes commission-approved cybersecurity-related CIP Reliability Standards before they become mandatory and enforceable
- Incentive available until the utility's next rate case
- After the incentive period, cybersecurity investments can be included in the rate base for cost recovery through future rate cases
- Early starters benefit from quicker financial returns

INSM Implementation Timeline

May 9, 2024	June 24, 2024	T$_0$	T + 36 Months October 2027 or January 2028	T + 60 Months
NERC Board of Trustees adopted CIP-015-1 – Cyber Security – Internal Network Security Monitoring	NERC Submitted a Petition for Approval of Proposed Reliability Standard CIP-015-1 (RM24-7-000)	FERC Order Approving Reliability Standard CIP-015-1	CIP-015-1 goes into effect for all High and Medium w/ ERC Control Centers	CIP-015-1 goes into effect for all other Medium BES Cyber Systems with ERC

Dragos Services

Dragos Enables Organizations to Prepare and Execute Plans for NERC CIP Requirements

- Sensor Placement Studies
- Network Vulnerability Assessments
- Tabletop Exercises
- Incident Response
  - Plan Development Workshops
  - Rapid Response Retainers
- OT Threat Hunting with OT Watch

Protect Electric Sector While Meeting Compliance

Trusted
in the electric industry with influence into requirements and implementation of CIP-015

Collect and Monitor
native network visibility and monitoring solution built for OT protocols down in E/W traffic

Detect
comprehensive threat detection injected with Dragos OT CTI outside of just anomaly detections or AI use

Analysis & Response
manage and triage with response playbooks to aid forensics and investigations + OT Watch Threat Hunting

Thank You

DRAGOS

Phil Tonkin
Shelby Brooks