corelight

Compliance brief

Navigating the new NERC CIP-015-2 standard

Securing the converged grid with unparalled network visibility

Overview

In 2025 alone, cyberattacks on critical infrastructure surged by 40%, exposing a variety of vulnerabilities in legacy defenses as organizations evolve to converged Information Technology (IT) and Operational Technology (OT) environments. To counter these threats, the North American Electric Reliability Corporation's (NERC) introduced the mandate of Internal Network Security Monitoring (INSM) to the Critical Infrastructure Protection (CIP) ecosystem in the summer of 2025, with the primary goal of identifying lateral movement across the network once an attacker is already inside an organization's perimeter. While CIP-015-1 focuses on collecting and analyzing network data inside the Electronic Security Perimeter (ESP) for High and Medium Impact BES Cyber Systems, the newly approved CIP-015-2 expands this to include monitoring for auxiliary systems like EACMS (Access Control) and PACS (Physical Access) that reside outside the ESP but provide critical entry points. This brief explains the evolution of this NERC directive and provides useful guidance for organizations aiming to meet the CIP-015 compliance requirements in the age of converged networks and AI-enabled adversaries.

On June 26, 2025, the Federal Energy Regulatory Commission (FERC) issued Order No. 907, directing NERC to develop modifications to its existing Reliability Standard CIP-015-1 to extend internal network security monitoring to include Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS) that sit outside of the Electronic Security Perimeter (ESP).

The Commission determined that an update was needed because CIP-015-1 was not fully responsive to the directive in prior Order No. 887, leaving a security gap by failing to include auxiliary systems from third-party vendors and contractor access in real-time, for example, that provide critical entry points into the internal network. Thus, NERC was directed to close the "visibility gap" with the updated NERC CIP-015-2 standard, which passed its final industry ballot in March 2026. Together, these standards require "responsible entities" to implement documented processes for monitoring internal network activity, detecting and analyzing anomalous network activity, as well as retaining network data associated with anomalous activity and protecting the internal network security data collected.

The stakes have never been higher with increasingly sophisticated threat actors and nation-state groups like Volt Typhoon actively pre-positioning themselves within corporate IT networks, patiently waiting for an opportunity to strike. Research shows the growing use of evasive "living-off-the-land" techniques and the abuse of legitimate, built-in network administration tools to bypass traditional endpoint security, establish a foothold, and pivot into critical OT systems to disrupt or, at least, threaten to disrupt operations. Adding to that is the increasing use of automation and AI, which allows even junior adversaries to discover vulnerabilities and create new attacks faster and easier than ever, often outpacing an organization's defenses, not to mention regulatory policies.

While NERC CIP is a North American regulatory framework, its rigorous approach to Internal Network Security Monitoring (INSM), the focus of this particular standard, is increasingly viewed as the global benchmark for critical infrastructure protection. As cyberthreats continue to flourish in volume and sophistication, we anticipate other countries' initiatives and international regulatory bodies will soon follow suit, adopting similar internal network monitoring mandates to secure their national grids.

Understanding the evolution of CIP-015-1 vs. CIP-015-2

To understand the impact of the new standard, it's helpful to look at how the requirements have expanded over time.

The initial CIP-015-1 iteration introduced a major paradigm shift by mandating INSM primarily for High and Medium-impact Bulk Electric System (BES) Cyber Systems. It legally required organizations to assume the perimeter could be breached and, therefore, mandated continuous monitoring within the Electronic Security Perimeter (ESP) to detect anomalous behavior.

The newly approved CIP-015-2 standard broadens these requirements to address the realities of a rapidly modernizing and highly distributed grid. To that end, this new standard expands the scope of monitored assets to include auxiliary systems, such as EACMS (Access Control) and PACS (Physical Access), that sit outside the ESP but provide access to it.

The shift from CIP-015-1 to CIP-015-2 reflects the evolving threat landscape, where attackers routinely exploit the convergence of IT and OT systems to infiltrate critical infrastructure via an initial IT compromise. This update ensures that organizations include these auxiliary systems in their INSM deployments to more effectively detect and respond to evolving threats.

Network Detection and Response helps address NERC CIP-015

To meet these updated standards, organizations are adopting advanced network monitoring solutions that provide complete visibility and threat detection across modern converged infrastructures. To that end, a modern Network Detection and Response (NDR) platform can provide several key elements. It should offer unified IT/OT visibility across the entire enterprise, including monitoring critical east-west traffic. Passive, non-disruptive monitoring is essential for safely inspecting OT systems and networks to ensure uptime. The solution should also provide deep parsing of industrial protocols (like Modbus and DNP3) to

Key decision and enforcement dates for the NERC CIP-015 standard for Internal Network Security Monitoring (INSM):

January 19, 2023: FERC issues Order No. 887, directing NERC to develop a new standard requiring INSM for all High-Impact and Medium-Impact (with External Routable Connectivity) BES Cyber Systems

May 9, 2024: NERC formally adopts the newly created Reliability Standard CIP-015-1

June 26, 2025: FERC issues Order No. 907 that formally approves CIP-015-1 but simultaneously directs NERC to close a critical "visibility gap" by extending INSM to include Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS) located outside the Electronic Security Perimeter (ESP)

March 5, 2026: NERC adopts CIP-015-2, expanding the INSM scope to EACMS, PACS, and Shared Cyber Infrastructure (SCI/Virtualization)

September 1, 2026: FERC deadline for the final submission and adoption of the modified CIP-015-2 standard

October 1, 2028 (Phase 1 Implementation): Mandatory Compliance Effective Date. Registered entities must achieve full INSM compliance (including the CIP-015-2 expansions for EACMS, PACS, and SCI) for all applicable High and Medium impact systems located at Control Centers and backup Control Centers

October 1, 2030 (Phase 2a Implementation): Entities must achieve INSM compliance for the remaining Medium-impact systems and supporting Shared Cyber Infrastructure (SCI) located at all other asset types (such as substations and generation facilities)

October 1, 2031 (Phase 2b Implementation): Final Compliance Deadline. Entities must achieve full INSM compliance for EACMS and PACS associated with Medium-impact systems located at all remaining non-control center asset types

enable command-level logging and detect unauthorized control commands. Furthermore, an effective solution should be able to identify threats that evade traditional monitoring tools that have become hallmarks of modern adversaries. Finally, it must provide immutable, audit-defensible evidence with long-term retention to ensure regulatory compliance and accelerate incident response.

An advanced NDR platform can not only provide effective threat protection across the converged IT and OT network and address compliance needs, but also help energy firms maintain operational resilience by optimizing availability, performance, and security. In doing so, organizations are future-proofing their environments with these strategic benefits:

- **Eliminating critical security blind spots** by providing a single, enterprise-wide source of network "ground truth" that seamlessly tracks lateral movement from the corporate cloud all the way through to the convergence point.

NERC CIP requirements and Corelight capabilities

NERC CIP-015-1 requirement	Corelight Open NDR Platform capability
R1.1 (Data Collection) Continuous collection and monitoring of network communications and traffic inside the Electronic Security Perimeter (ESP).	**Passive, protocol-aware visibility** Corelight sensors deploy out-of-band across on-premises, cloud, and ICS networks to passively capture traffic without risking operational disruption to legacy OT equipment. **Deep ICS/OT parsing & Entity Collections** Corelight's ICS/OT Collection natively decodes protocols like Modbus, DNP3, and IEC-61850. The Entity Collection automatically profiles network devices to establish a dynamic inventory of the Electronic Security Perimeter (ESP) and expose "shadow OT". **Immutable network packet data** Corelight's Smart PCAP and seamless integration with leading Network Packet Brokers enable organizations to capture and store network ground-truth data at key ingress and egress points across converged networks.
R1.2 & R1.3 (Baselining, detection, and analysis) Compare internal network traffic against baselines to detect, flag, and evaluate anomalous activity.	**Multi-layered detections, behavioral analytics, and machine learning** Corelight automatically baselines traffic and combines unsupervised machine learning (anomaly detection), behavioral analytics, curated IOCs and Suricata signatures, as well as YARA file analysis to alert on suspicious deviations. **Detecting evasive threats** Asset details, related device behavior, and advanced multi-layered detections uncover attack frameworks and known CVEs, track lateral movement across converged IT/OT networks, and identify stealthy "Living-off-the-Land" (LotL) techniques that evade traditional endpoint detection. **Agentic Triage** Corelight Investigator's AI-driven triage simplifies investigations and accelerates incident response with 10x faster triage.
R2 & R3 (Data retention and protection) Establish processes to safeguard network data and retain metadata tied to anomalous activity long enough—and in sufficient detail—to support forensic analysis and audits.	**Immutable, audit-defensible evidence** Corelight replaces assumptions with definitive ground-truth evidence, powered by rich Zeek metadata, multi-layered detections, curated threat intelligence, YARA static file analysis, and Smart PCAP, which offers a flexible lookback window configurable to meet customer needs for long-term forensics. This provides regulators with proof that internal controls are in place and helps ensure future-proof compliance. **Log reduction & storage optimization** Intelligent log filtering and data reduction ensure that only actionable, high-fidelity signals are forwarded to the SIEM/XDR, allowing utilities to meet strict data retention requirements affordably while reducing analyst alert fatigue.

- **Protecting operationally critical OT assets** by delivering passive, out-of-band monitoring that safely inspects traffic without requiring endpoint security agents, helping ensure the continuous uptime and performance of legacy OT equipment.
- **Uncovering hidden threats** by deeply parsing industrial protocols, such as Modbus, DNP3, and IEC-61850, to empower defenders to quickly distinguish between a routine operational read request and a malicious command attempting to write to a register that could disrupt operations.
- **Breaking down silos** to help foster cross-team collaboration by giving both IT and OT security teams a unified dataset and a common language for incident response.
- **Address compliance requirements** by providing audit-ready proof that internal networks are actively monitored to identify and remediate active and latent threats across the converged IT and OT infrastructure.

Corelight Open NDR

The Corelight Open NDR Platform provides unified network visibility by transforming raw traffic across IT, cloud, and OT environments into correlated, contextual evidence. This evidence-based approach leverages multi-layered detection, including AI-driven anomaly detection, behavioral analytics, signature-based detection, and curated threat intelligence, to identify sophisticated adversaries such as Volt Typhoon. By parsing specialized industrial protocols such as Modbus and DNP3, Corelight enables security teams to identify lateral movement and unauthorized command integrity compromises without disrupting critical infrastructure uptime.

As an open platform built on open-source Zeek and Suricata IDS, customers can create custom detections and parsers to support their unique environments. Open NDR gives organizations complete control over their data, enabling them to customize, create, filter, and integrate it whenever and wherever they want. With no proprietary data format, the data is fully portable and can be moved or shared across other systems and platforms, including with a wide variety of Corelight integration partners.

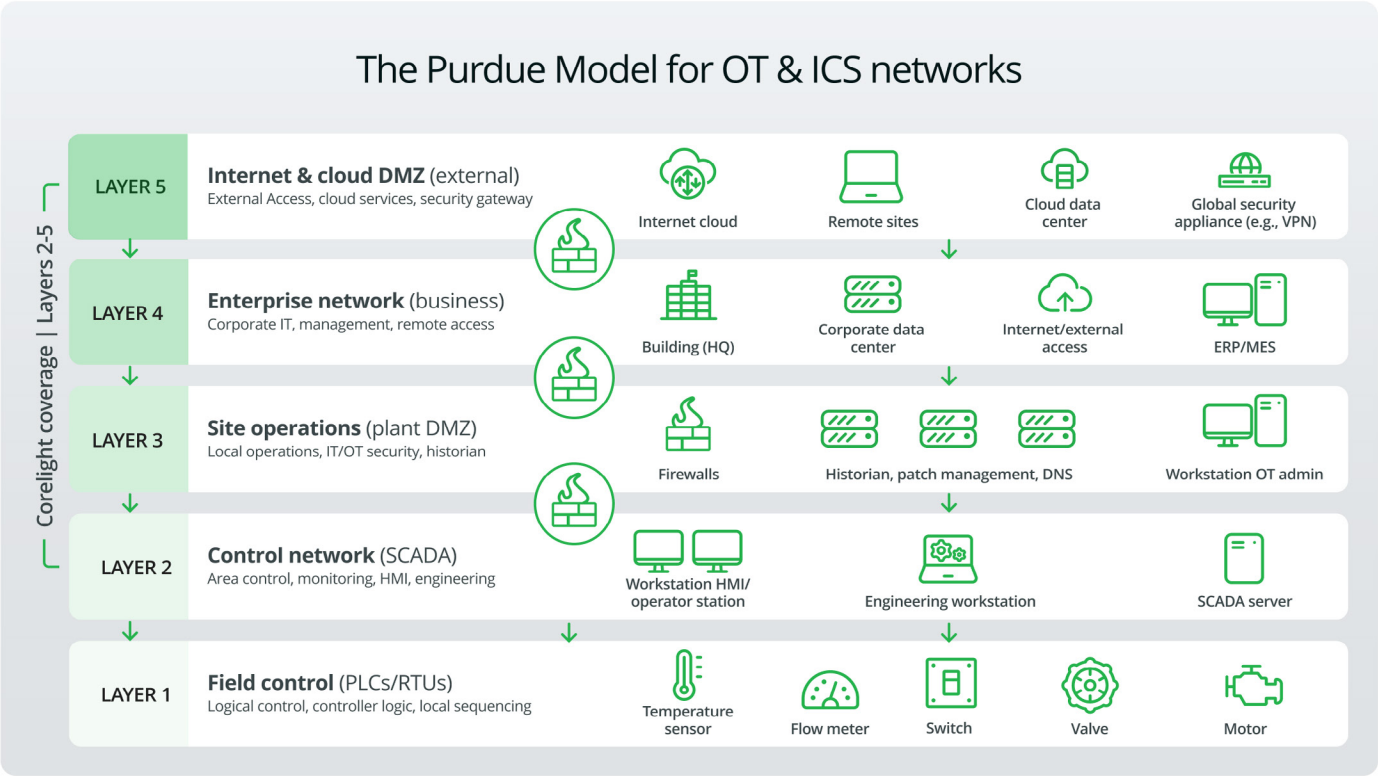
With its flexibility, full visibility, and advanced detections, Corelight empowers security teams to detect advanced threats that other tools miss, accelerate incident response, and provide the concrete proof to help address compliance requirements.

In one recent example, Corelight helped subdue a coordinated zero-day attack on a national energy consortium, where attackers bypassed their traditional firewall and EDR defenses and moved quickly inside their network, even adapting their tactics as target vulnerabilities were patched. Leveraging timely network evidence from their Corelight Open NDR solution, the organizations were able to quickly disrupt the attack and prevent a full-scale shutdown by detecting a single packet among billions that provided the critical evidence for a swift, successful response.

Mapping modern visibility to the Purdue Model

To effectively defend critical infrastructure, security teams must understand how threat actors move across the traditional boundaries separating IT and OT. The Purdue Enterprise Reference Architecture (PERA), or Purdue Model, remains the industry's foundational framework for enforcing this network segmentation and structuring data flows. Traditionally, the model isolates corporate business functions at the higher Enterprise Zone layers (Levels 4 and 5) from the sensitive physical processes at the lower Industrial Control System (ICS) layers (Levels 0 through 2). A Demilitarized Zone (DMZ), often referred to as Level 3.5, acts as the primary buffer, utilizing firewalls and proxies to restrict direct IT-to-OT communication.

However, as we discussed earlier, the trend toward IT/OT convergence renders static perimeter defenses insufficient to protect modern networks. Attackers frequently attempt to jump these zones or exploit legitimate bidirectional data paths. This is where an advanced NDR solution like Corelight becomes critical to the architecture, with the capability to monitor across Levels 2 through 5. By strategically tapping network traffic at the boundaries of Level 3 (Manufacturing Operations) and the Level 3.5 DMZ, Corelight provides comprehensive, real-time visibility into the exact protocols and data moving between IT networks and the substation. Rather than relying solely on the rigid boundary controls of the Purdue Model, Corelight infuses the architecture with unprecedented visibility and continuous monitoring across levels, transforming the static layers into an active, threat-aware ecosystem that exposes lateral movement and unauthorized traffic before it can disrupt physical operations.



Corelight identifies attacks as they move between IT and OT by monitoring all network activity across Levels 2 through 5.

corelight

To learn how Corelight Open NDR Platform can secure your converged grid and accelerate your NERC CIP-015-2 readiness, request a demo at

https://corelight.com/contact

info@corelight.com | 888-547-9497

The Z and Design mark and the ZEEK mark are trademarks and/or registered trademarks of the International Computer Science Institute in the United States and certain other countries. The Licensed Marks are being used pursuant to a license agreement with the Institute.

All rights reserved. © Copyright 2026 Corelight, Inc.