Compliance Brief

Corelight Open NDR Platform Supports Upcoming FERC 887 INSM Requirements

On April 10, 2023 the Federal Energy Regulatory Commission (FERC) Final Rule (Order No. 887) took effect. The order was issued in January 2023, and directs the North American Electric Reliability Corporation (NERC) to develop new or modified reliability standards requiring internal network security monitoring (INSM) for high-impact bulk electric system (BES) cyber systems and medium-impact systems with high-speed internet connections.
The final rule directs NERC to complete a feasibility study on low- and medium-impact BES cyber systems not covered under the new INSM standards to determine potential threats to the security and reliability of the Bulk Power Systems.

FERC 887 Timeline	Deliverable
January 19, 2023	FERC issues Order No.887 to NERC
April 10, 2023	Rule takes effect
Within 15 months of the effective date of final rule	NERC must submit new or modified standards for FERC approval
12 months from issuance of final rule	NERC must submit results of feasibility study of all low-impact BES cyber systems with and without external routable connectivity and medium-impact BES cyber systems without external routable connectivity
TBD	Implementation deadline for responsible entities

Current NERC Reliability Standards focus on perimeter-based security controls, but excludes monitoring anomalous activity within the network. The implementation of INSM facilitates the detection of anomalous network activity indicative of a threat in progress, increasing the probability of early detection and allowing for quicker response to an incident.

The new or modified INSM Standards will apply to all high-impact BES cyber systems and medium-impact BES cyber systems with external routable connectivity, defined as the ability to access a BES cyber system from outside of its associated electronic security perimeter. INSM will be required in any Critical Infrastructure Protection (CIP) networked environment.

How Does Corelight Support INSM for FERC 887?

INSM enables an analyst to track and detect malicious activity that has circumvented perimeter controls and gained access to one or more vulnerable systems. INSM alerts and evidence improve the organization's ability to stop adversary campaigns before they achieve their objective.

Corelight's Open NDR platform supports these capabilities via indexed network transaction logs, intrusion detection alerts, and packet capture. Our security design employs both community-sourced and Corelight-developed content that can enumerate Indicators of Compromise (IoCs) and integrate leading threat intelligence feeds in IT and OT environments.

Network Security Monitoring (NSM) is the collection, detection, and analysis of data from a logical, virtual, or physical computer network.

Internal Network Security Monitoring (INSM) is a subset of NSM applied within a trust zone. For FERC 887 that trust zone is any CIP-networked environment.

FERC 887 Requirement	Corelight Supporting Capability
Develop baselines of network traffic inside a CIP-networked environment	Corelight's *Known Entities Collection* aids in the development of network traffic baselines. This feature summarizes current and historical activity for every host allowing analysts to answer "how many hosts were on a CIP network at a given time?", etc.
Monitor for and detect unauthorized activity, connections, devices, and software inside a CIP-networked environment	Corelight leverages a wide array of detection methodologies including machine learning models, Suricata signatures, and industry-specific threat intelligence for detection.
Identify anomalous activity to a high level of confidence by: ● Logging network traffic ● Maintaining logs and other data collected regarding network traffic ● Implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices	Corelight produces rich network metadata that can be stored for long periods of time to enable retroactive network investigations. This provides analysts context to investigate IDS alerts and the surrounding activity including packet capture, both in real and past times.

corelight		Defenders have always sought the high ground in order to see farther and turn back attacks. Corelight delivers a commanding view of your network so you can outsmart and outlast adversaries. We capture, interpret, and connect the data that means everything to defenders. **info@corelight.com | 888-547-9497**