CASE STUDY

# Deploying the Dragos Platform to Secure Critical OT Infrastructure

## INSM Readiness as a Natural Consequence of Strong Security

Dominion Energy stands out as a forward-thinking utility that recognized the critical importance of operational technology (OT) visibility before regulatory mandates make it necessary.

As one of the nation's largest producers and transporters of electric energy, Dominion serves nearly five million customers across multiple states. The electric transmissions team developed and executed against an ambitious project—deploying over 450 Dragos sensors at facilities across three states, building a dedicated OT Security Operations Center, and establishing a specialized team to monitor their extensive network infrastructure containing approximately 16,000+ IP-enabled devices.

This case study examines how Dominion Energy transformed their security posture through a comprehensive implementation of the Dragos Platform for internal network security monitoring. What distinguishes Dominion's approach is their fundamental recognition that "being compliant doesn't equal being cyber secure."

Dominion Energy®

**5M**
customers across multiple states

**11,000**
miles of transmission lines

**27,500**
Megawatt market generation

**16,000+**
IP-enabled devices

**450+**
substations equipped with security sensors

Multiple states (primarily VA, NC, SC)

## Choosing Dragos as Their OT Security Partner

Beginning in 2019—years before FERC directed NERC to develop standards requiring internal network security monitoring (INSM)—Dominion's leadership embarked on a methodical journey to assess the OT security market, gain C-suite buy-in, evaluate vendors against stringent requirements, and implement a standardized deployment across their critical infrastructure. Rather than waiting for regulatory requirements to drive their security strategy, the team proactively identified the IT-OT security gap in their environment and pursued a solution-oriented approach focused on genuine security outcomes.

Dominion Energy partnered with Schweitzer Engineering Laboratories (SEL), a trusted industry leader in electric power systems protection, to support the implementation of controls that will ensure compliance with anticipated INSM regulations. SEL's established relationship with Dominion and deep expertise in both power systems and cybersecurity made them a natural strategic partner for this ambitious initiative.

SEL played a pivotal role in the vendor selection process, helping Dominion Energy evaluate cybersecurity solutions based on comprehensive security outcomes rather than individual product features. Their influence was instrumental in securing a partnership with Dragos. Using 70 requirements to evaluate five different vendors, the team validated Dragos's capabilities to deliver both the technology and strategic alignment needed for long-term success.

Dominion's strategic investment in comprehensive visibility, vulnerability management, and 24/7 monitoring capabilities has established a security framework that delivers tangible protection for their critical operational systems, and as a result, positioned them well ahead of regulatory compliance.

### WHAT IS NERC CIP-015?

NERC CIP-015 is a cybersecurity standard developed by the North American Electric Reliability Corporation (NERC) that focuses on Internal Network Security Monitoring (INSM) for High and Medium Impact Bulk Electric System (BES) Cyber Systems. This standard was developed in response to a Federal Energy Regulatory Commission (FERC) directive to address security gaps in existing cybersecurity measures.

The standard specifically targets "east-west" traffic monitoring within protected networks, complementing existing "north-south" protections that focus on communications entering and exiting protected networks. This approach acknowledges that adversaries may compromise an asset in an untrusted segment and then leverage approved system-to-system communications to pivot onto assets within the trusted environment.

The FERC directive requires utilities to address three key security objectives:

- **Baselining:** Develop baseline for network traffic inside the CIP-networked environment by analyzing network traffic and data flows for security purposes.
- **Monitoring and Detecting Unauthorized Activity:** Monitor for and detect unauthorized activity, connections, devices, and software inside the CIP-networked environment, as well as encompass awareness of protocols used in industrial control systems.
- **Identification of Anomalous Activity**: Identify anomalous activity to a high level of confidence by logging network traffic; maintaining those logs, and other data collected, regarding network traffic that are of sufficient data fidelity to draw meaningful conclusions and support incident investigation; and maintaining the integrity of those logs and other data by implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures (maintaining the integrity of logs and other data assures an entity that analysis and findings from incident investigations are representative of the actual incident and can aid in the mitigation of current and future similar compromises).

## Dominion Energy's Infrastructure and Goals

Dominion Energy serves nearly five million customers across several states, with its primary base in Virginia, North Carolina, and South Carolina. The company manages approximately 27,500 MW of market generation and roughly 11,000 miles of transmission lines.

Dominion Energy's primary goals for implementing internal network security monitoring with the Dragos Platform included:

- **Close the IT-OT Security Gap:** Despite having a really strong IT enterprise security program and community including phishing simulations and robust internal threat capabilities, Dominion Energy identified a gap in their OT security coverage.
- **Achieve Comprehensive Visibility:** Gain visibility across all OT assets, particularly the 13,000 IP-enabled devices in their network.
- **Move Beyond Compliance:** Transition from mere regulatory compliance to true cybersecurity, recognizing that being compliant doesn't equal being secure. Prior to implementing advanced network security monitoring, Dominion Energy relied primarily on their NERC CIP program, which included strong passwords, ports and services, annual vulnerability assessments on assets and substation systems. However, they recognized this approach just wasn't hitting the mark.
- **Implement 24/7 Monitoring:** Establish continuous monitoring capabilities for their critical infrastructure.
- **Create a Standardized Security Approach:** Execute repeatable, standardized security implementations across their infrastructure.

## Complex Implementation Requirements

SEL played a central role in deploying over 450 Dragos sensors operating on the SEL-3355 computing platform across Dominion's extensive OT infrastructure. The SEL-3355 is a versatile computing platform built to withstand harsh environments in utility and industrial applications. A wave-based deployment strategy, which prioritized medium-impact substations, critical customer assets, and other key transmission assets, ensured the most critical systems received enhanced monitoring capabilities first while maintaining operational continuity.

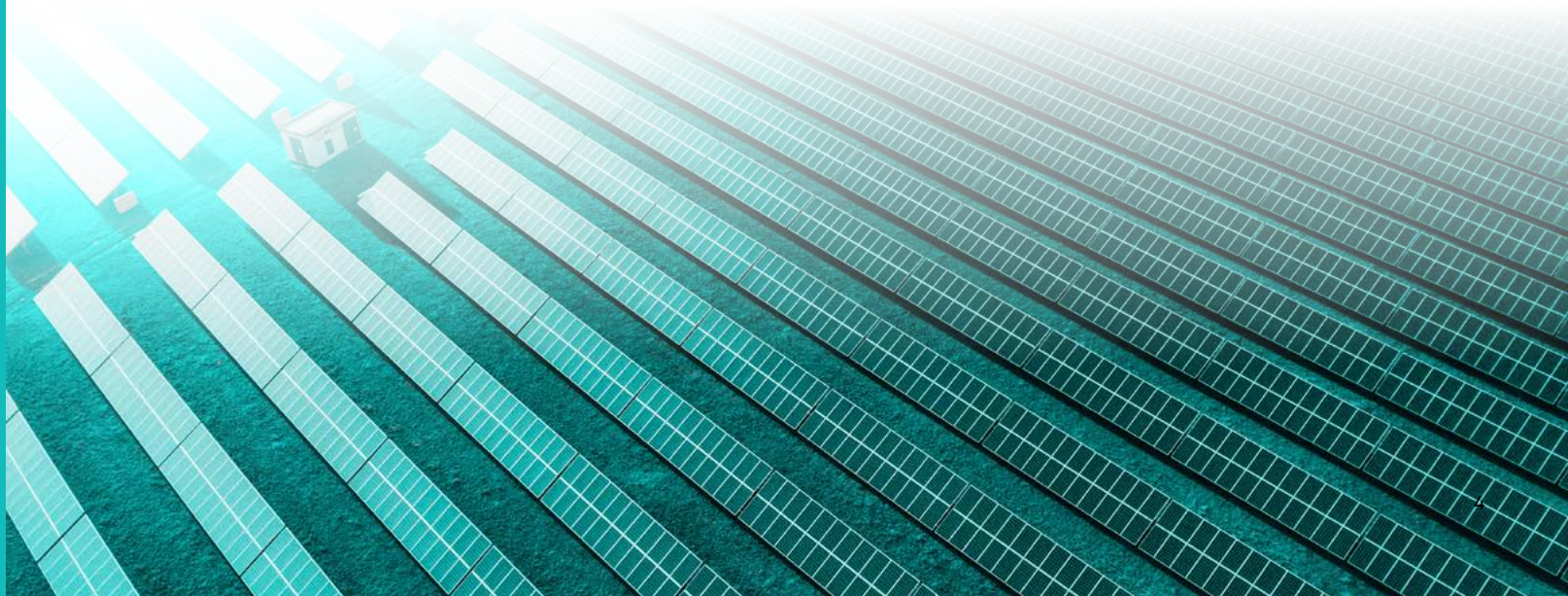
The scale and complexity of Dominion's infrastructure, spread across three states, presented significant implementation challenges, including:

- Implementing approximately 3,400 firewall rules across multiple firewall systems
- Network switches configuration for span ports across hundreds of locations
- Power and physical space requirements in substations
- Standardizing deployment across geographically dispersed locations while coordinating efforts from multiple teams

> Using 70 requirements to evaluate five different vendors, the team validated Dragos's capabilities to deliver both the technology and strategic alignment needed for long-term success."
>
> **Mike Lamb, General Manager - Electric Transmission Substation Operations • Dominion Energy**

Dominion Energy took a methodical, strategic approach to implementing the Dragos Platform:

- **They focused on outcomes.** "We envisioned a solutions-level approach. We had a goal. We wanted to have visibility, vulnerability management across multiple substations, across multiple states, covering lots of assets. We wanted to monitor these environments 24/7. What would it take to get there?"
- **They trusted vendors with proven experience in OT.** "We didn't want a typical vendor-customer relationship where you buy a couple of sensors, put them in, and deal with the mess. We wanted partners in our success, driving our decisions to trust the project to SEL and Dragos."



# Dominion's Top 5 Factors for Success

1. **Thorough FEED Study:** The comprehensive Front-End Engineering Design (FEED) study proved critical to the project's success, as it involved detailed assessment of network topologies, identification of potential bottlenecks, and thorough evaluation of existing routers, firewalls, vendor specifications, firmware versions, and span port capabilities—all essential elements without which the entire implementation would likely fail.

2. **Strategic Deployment:** Dominion Energy adopted a strategic deployment approach by prioritizing their critical infrastructure, specifically targeting medium-impact sites first. This approach aligns well when preparing for upcoming NERC CIP-015 requirements in advance of regulatory deadlines.

3. **Early Engagement with Support Teams:** SEL provided critical technical direction to Dominion Energy's IT, network, and firewall teams during the initial project setup, facilitating seamless integration between IT and OT security operations. Their experts provided data to assist in updating the implementation of approximately 3,400 firewall rules and operationalizing the Dragos Platform within Dominion's complex network infrastructure. Leveraging expertise from SEL significantly accelerated the deployment timeline and the return on Dominion's investment.

4. **Standardized Deployment with OEM Guidance:** Dominion emphasized the critical importance of standardization throughout their deployment process to ensure repeatability, cost-effectiveness, and operational efficiency, thereby minimizing unnecessary trips to substations and maximizing the return on their security investment. SEL's engineering team helped develop standardized installation specifications that ensured consistent sensor placement and panel configurations across all deployment sites. This standardization not only improved operational efficiency and reduced installation costs but also created a scalable framework that simplified future expansions and minimized reliance on external contractors.

5. **Building a Diverse Team:** To effectively operate their OT monitoring capability, Dominion assembled a diverse team comprising cybersecurity specialists, NERC CIP compliance experts, experienced field technicians, and recent college graduates, creating a blend of specialized knowledge and fresh perspectives essential for addressing complex OT security challenges. The Dominion team makes it a point to hire both active duty and retired military personnel – their commitment to the mission and ability to execute technically make the team stronger.

> The Dragos Platform's vulnerability management methodology, backed by real-time threat intelligence, gives us peace of mind. We don't have to boil the ocean – instead, we can focus on what really matters.

**Wes Futrell, Supervisor - Substation Technical Operations • Dominion Energy**

# How Dominion Energy Gets Maximum Value from the Dragos Platform

## Comprehensive Visibility

Dominion Energy uses the Dragos Platform's comprehensive visibility capabilities, encompassing all operational aspects, including the Dominion team's engineering-level access, operational data transfers, and device-to-device communications, which allows them to detect anomalous network activity and establish a complete view of their network environment.

## Using Threat Intelligence to Drive Risk-Based Decision Making

Through the Dragos Platform vulnerability management capabilities, Dominion has on-demand access to detailed insights into their asset inventory, firmware versions, and software configurations. The team relies on the fact that every vulnerability is analyzed by a Dragos expert, leveraging OT-specific mitigation guidance, corrected CVSS scores, and the Dragos Platform's now-next-never approach.

## Response Planning and Case Management

After gaining visibility across their operational technology environment, Dominion focused on developing response plans, playbooks, notification strategies, and case management processes to effectively address the security insights gathered from their monitoring systems.

## Operational Data Analysis

The operations team at Dominion comprehensively tracks all activity in their environment, including legitimate activities like engineering access and relay operations alongside potential anomalous network activity, integrating this approach into their daily security operations.

## Results from Deploying the Dragos Platform

Dominion Energy achieved significant security improvements through their implementation:

- **Enhanced Visibility.** Dominion's deployment of sensors across three states delivered unprecedented visibility into their extensive OT infrastructure containing tens of thousands of IP-enabled devices, dramatically improving their security posture.
- **Improved Threat Response.** Dominion significantly enhanced their threat response capabilities through their implementation of the Dragos Platform, which enabled them to develop comprehensive response plans, detailed playbooks, structured notification strategies, and effective case management processes, creating a cohesive framework for addressing security incidents throughout their extensive operational technology environment.
- **Proactive Security Posture:** Having been operational for over a year with many of their second-wave sites already covered, Dominion has accumulated significant operational experience and security data that informs their ongoing security improvements.
- **Standardized Security Infrastructure:** Dominion established standardized security infrastructure that benefits both existing and new facilities, ensuring that any greenfield substation projects automatically include properly configured security sensors in the correct panels.
- **Regulatory Readiness:** By proactively implementing internal network security monitoring, Dominion positioned themselves well ahead of NERC CIP-015 compliance requirements, achieving a comfortable security posture before regulatory deadlines.

## The Bottom Line

Dominion Energy's implementation of the Dragos Platform represents a comprehensive approach to securing critical infrastructure that goes beyond regulatory compliance to achieve true cybersecurity. By focusing on a solution-oriented approach rather than simply deploying a product, Dominion created a sustainable security program with standardized processes, skilled personnel, and effective technology.

The key takeaways from their experience include:

1. Invest in a thorough preliminary assessment (FEED study).
2. Develop a robust deployment strategy.
3. Standardized sensor installations.
4. Build a diverse team with complementary skills.
5. Plan for data analysis and response capabilities.

> The key to success is thinking about deployment of internal network security monitoring as a project, not a product. Take a holistic approach with trusted vendors who understand your environment – don't just buy a box and stick it in the station.
>
> **Wes Futrell, Supervisor - Substation Technical Operations Dominion Energy**

## Want to learn how Dragos can support your INSM strategy?

Now's the time to start preparing for NERC CIP-015. Schedule a personalized session with a Dragos expert to assess your current OT environment, explore network architecture considerations, and provide practical insights on how to develop an effective Internal Network Security Monitoring (INSM) strategy.

Book Your Strategy Session

### About Dragos, Inc.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

Learn more about our technology, services, and threat intelligence offerings:

Request a Demo

Contact Us