SOLUTION BRIEF

DRAGOS
SAFEGUARDING CIVILIZATION

How Dragos Supports NERC CIP Reliability Standards

The Dragos Platform & Services Enable Compliance

The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standards are a set of requirements designed to protect critical infrastructure vital to the reliable operation of North America's Bulk Electric System (BES) from cyber and physical security threats.

Implementing NERC CIP requirements can be challenging due to their complexity and the need for rigorous compliance across diverse operational environments. The Dragos Platform enhances the cybersecurity posture in these critical environments through comprehensive asset and network visibility, threat detection, vulnerability management, and investigation and response. It integrates intelligence from our adversary threat hunters and service engagement findings to ensure customers have the most comprehensive detections, up-to-date vulnerability guidance, and operational technology (OT) cyber threat intelligence updated weekly in the Dragos Platform.

The Dragos Services team provides expertise to help evaluate and mature OT security practices, and the Threat Intelligence team delivers contextual awareness on new threats and vulnerabilities, empowering organizations to make informed decisions about their security posture.

> We were initially focused on anomaly detection software and originally thought that we would benefit from the ability to see and react to alerts. But we quickly realized that the majority of those solutions just weren't as mature as we needed. This awareness led us to consider OT visibility platforms in general, and the conversation pretty much started and stopped with Dragos.
>
> — ELECTRIC AND WATER UTILITY CISO —

Mapping Dragos Technology & Services to NERC CIP Requirements

Below is a summary of how the Dragos Platform can be utilized in a NERC CIP program, and how the Dragos Services team can help fulfill requirements.

CIP-002 BES Cyber System Categorization

Platform: The Dragos Platform employs passive monitoring techniques to observe and identify devices connected to the network. The Dragos Platform offers several capabilities, including alerting on assets within the Electronic Security Perimeter(s) (ESP) not listed in the asset inventory system via export and/or API integration, alerting on new asset detections that require CIP-002 evaluation, asset tagging for categorization (e.g., EACMS, PACS, PCA, BCA, etc.), and out of the box integration with Configuration Management Database (CMDB), which serves as the system of record in many instances.

As shown in Figure 1, customers can create zones and parent zones that align to their facilities designated impact rating, making it easy to identify traffic between High, Medium, and Low impact sites. The Platform generates **visual maps that depict the physical and logical layout of the OT network**. The visual maps illustrate the relationships between different assets and components, which helps in understanding how devices are interconnected, their communication pathways, and dependencies between critical infrastructure components.

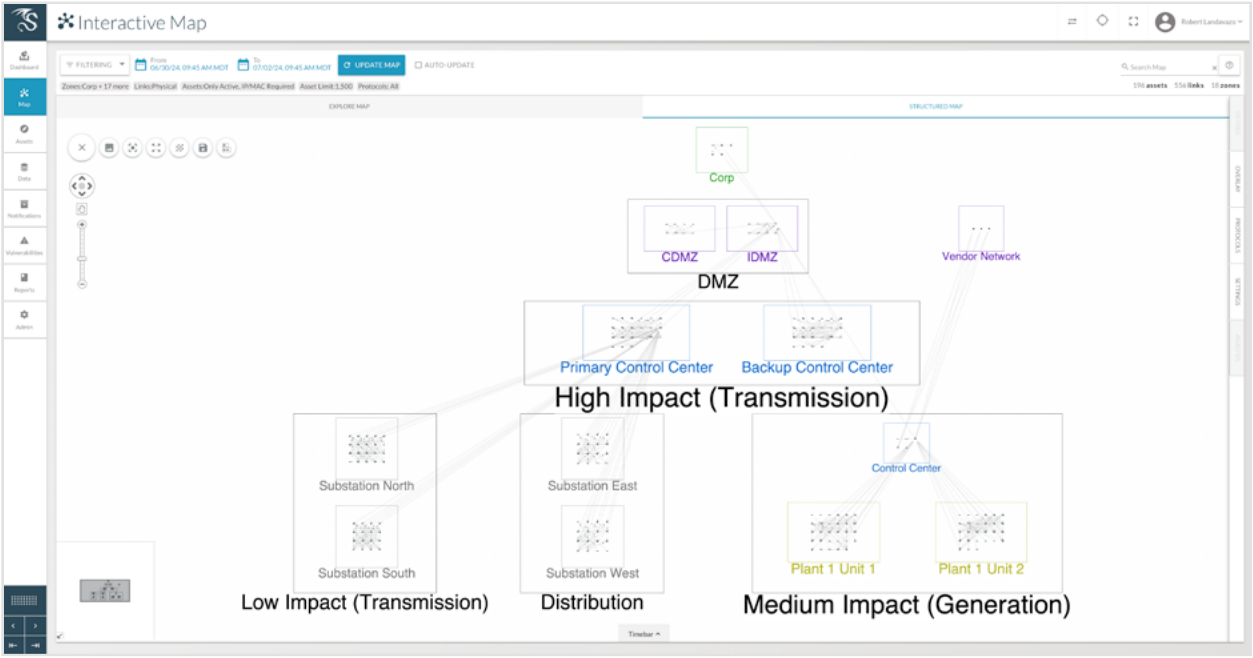


Figure 1: Dragos Platform Structured Map View

Services: Architecture Reviews assist in understanding the most critical systems, essential network infrastructure, and the potential consequences of a cyberattack on those systems.

CIP-003 Security Management Controls

Services: Cybersecurity Program Maturity Reviews, such as Cybersecurity Capability Maturity Model (C2M2), evaluate an organization's current cybersecurity posture, capabilities, and practices. This includes assessing existing policies, procedures, technologies, and resources used to safeguard assets. These reviews identify gaps, evaluate the effectiveness of plans, procedures, and technologies, and recommend steps to enhance maturity. By assessing maturity levels across various cybersecurity domains (e.g., governance, risk management, incident response), the reviews prioritize improvement efforts, enabling organizations to focus resources where they can most effectively reduce cyber risks and strengthen resilience. They provide insights that support strategic decision-making on cybersecurity investments, resource allocations, and long-term planning, empowering leadership with a comprehensive understanding of current capabilities and future needs.

CIP-004 Personnel & Training

Community Resources: To satisfy requirements that individuals with access to critical assets are properly trained, Dragos supports NERC CIP customers with the following focused on OT cybersecurity for their personnel:

Dragos Academy is a specialized OT cybersecurity training program, designed to teach the skills our analysts, consultants, and practitioners use in the field to protect industrial and operational environments. Dragos Academy should not be relied upon solely to meet CIP-004 requirements but can complement entity-specific training.

Operational Technology – Cyber Emergency Readiness Team (OT-CERT) offers complimentary resources to the community, providing members with information and materials to help build an OT cybersecurity program.

Dragos WorldView reports provide up-to-date information on emerging threats, vulnerabilities, and attack techniques that are relevant to OT environments. This includes details on adversary's Tactics, Techniques, and Procedures (TTPs), and Indicators of Compromise (IOCs). WorldView reports offer contextual analysis of cybersecurity incidents and events, highlighting the potential impact on operational continuity and safety, providing actionable insights for security teams. The reports often include recommendations and best practices for improving cybersecurity posture in OT environments. These may include defensive strategies, mitigation techniques, and steps for enhancing resilience against specific threats.

CIP-005 Electronic Security Perimeter(s)

Platform:

- Dragos Sensors can be strategically placed in the environment to accommodate monitoring within the ESP and outside the ESP, to provide visibility and enable detective controls for known or suspected malicious communications for inbound and outbound communications. The Platform offers OT-aware detections to properly identify and alert on malicious communications within the OT environment.
- The Dragos Platform can help entities **identify external communications** that may not be routed through an Electronic Asset Point (EAP) by using the asset maps and communications analysis capabilities.

- The Dragos Platform **identifies remote access session activities** and visually depicts which connections are present over time. The Platform facilitates the identification of active remote access sessions that are not utilizing Electronic Access Control or Monitoring Systems (EACMS) designated as Intermediate Systems on the interactive map. It can also provide additional displays and dashboards to indicate when an interactive session or potentially baseline routine system-to-system remote access is established.

CIP-007 Systems Security Management

Platform:

- The Dragos Platform can be deployed for detecting malicious code, utilizing sensors in environments where traditional antivirus software cannot be installed. These environments include assets equipped with a Real-Time Operating System (RTOS) like protection relays, Physical Access Control Systems (PACS) door controllers, or Remote Terminal Units (RTUs). The Dragos Platform **continuously monitors OT networks and provides real-time alerts and notifications** to cybersecurity teams when deviations from normal operations are detected, which helps in quickly identifying and mitigating any instances of malicious code. Furthermore, the **Dragos Platform firewall integration** provides automated responses to detected threats based on notification rules configured within the Dragos Platform.
- The Platform logs events and generates alerts for applicable cyber assets by **detecting malicious code, successful login attempts, failed access attempts, and failed login attempts**. Log retention can be adjusted by the administrator to meet the 90-day requirement.
- The Platform can **help identify logical ports and the associated service name** that have either initiated or received communications on Cyber Assets. This information can assist Subject Matter Experts (SMEs) in identifying logical ports that should be disabled or restricted if the Responsible Entity determines that they are not needed.

CIP-008 Incident Reporting and Response Planning

Platform:

- The Dragos Platform continuously monitors OT networks for **anomalies, suspicious activities, and potential security incidents**. It provides real-time alerts and notifications to cybersecurity teams when deviations from normal operations are detected.
- The Dragos Platform offers a **centralized dashboard for incident management**, where security teams can view and prioritize alerts, incidents, and ongoing investigations.
- The Platform also includes **predefined playbooks** that outline step-by-step procedures and workflows for responding to different types of incidents.
- The Dragos Platform integrates with various Security Information and Event Management (SIEM) solutions and Security Operations Center (SOC) automation tools to help support rapid incident investigations.
- Overall, the Dragos Platform enhances incident reporting and response planning by providing robust detection capabilities, centralized management, automated response workflows, forensic analysis tools, collaboration features, and support for continuous improvement.

Services:

Rapid Response Retainers help organizations prepare for, respond to, and recover from cybersecurity incidents by offering customized strategic and tactical recommendations that prioritize solutions aligned with their business needs. Engaging a Dragos Rapid Response Retainer ensures access to an experienced incident response team specializing in OT cybersecurity crisis management, capable of analyzing, investigating, and responding to industrial cyber events effectively. When paired with the Dragos Platform, incident responders can expedite response.

Tabletop Exercises can satisfy the incident response plan testing requirements and provide feedback for lessons learned.

An **Incident Response Plan Development Workshop** is a collaborative session focused on creating or modifying OT-specific incident response plans. Leveraging Dragos's expertise, these workshops may include developing playbooks or runbooks, assessing key plan workflows, prioritizing responses for critical systems, and aligning the incident response plan with the current cyber threat landscape.

Dragos OT Watch utilizes industrial threat hunters' expertise to investigate suspicious activity in OT environments. OT Watch conducts persistent threat hunting tailored specifically for these environments. Threat hunters leverage the Dragos Platform and the extensive Dragos ecosystem. This encompasses OT-specific threat intelligence, insights from incident response and compromise assessments, Dragos Neighborhood Keeper data, and real-time information from current events.

CIP-009 Recovery Plans for BES Cyber Systems

Services:

Rapid Response Retainers help organizations prepare for, respond to, and recover from cybersecurity incidents by offering customized strategic and tactical recommendations that prioritize solutions aligned with their business needs. Engaging a Dragos Rapid Response Retainer ensures access to an experienced incident response team specializing in OT cybersecurity crisis management, capable of analyzing, investigating, and responding to industrial cyber events effectively.

Tabletop Exercises can satisfy the incident response plan testing requirements and provide feedback for lessons learned.

An **Incident Response Plan Development Workshop** is a collaborative session focused on creating or modifying OT-specific incident response plans. Leveraging Dragos's expertise, these workshops may include developing playbooks or runbooks, assessing key plan workflows, prioritizing responses for critical systems, and aligning the incident response plan with the current cyber threat landscape.

CIP-010 Configuration Change Management and Vulnerability Assessments

Platform:

- The Dragos Platform enables organizations to develop **baseline configurations** for OT devices based on CIDR, zone, asset type, and more. It monitors network communications to identify deviations from these baselines. Detailed dashboards highlight unintended changes to baselines, facilitating effective compliance management.
- The Dragos Platform conducts **passive vulnerability assessments** on identified assets. Specifically, the Dragos Platform automatically analyzes data it receives against known IOCs provided by the Dragos Intelligence team through each new Knowledge Pack. It analyzes network traffic for atomic indicators, discrete pieces of data identifiable through exact pattern matching. The Dragos Platform also identifies vulnerabilities in assets and prioritizes them using a strategic patching approach categorized as *Now, Next, Never.*
- The Dragos Platform features a specialized NERC CIP dashboard designed to support customers. The dashboard helps identify assets and communications requiring documentation, as well as flags certain activities, such as **Transient Cyber Assets (TCAs)** that remain on the network. Additionally, the dashboard monitors the duration these TCAs have been connected.

Services:

Network Vulnerability Assessments assess the current landscape's risk and evaluate the effectiveness of existing technical security controls, proposing enhancements for the future. Through active or passive information gathering and enumeration, Dragos identifies vulnerabilities that adversaries could exploit to pivot into the OT network or escalate privileges. Dragos's Network Vulnerability Assessments exceed the requirements outlined in CIP-010 R3.

CIP-012 Communications between Control Centers

Platform: If the Responsible Entity is utilizing encryption between control centers to secure communication and reduce the risk of exposure or modification of real-time monitoring data, the Dragos Platform can quickly identify **unencrypted communication protocols** in use.

CIP-015 Internal Network Security Monitoring

Platform:

- The Dragos Platform enables organizations to develop **baseline configurations of their network traffic inside trusted zones**, such as an ESP. It monitors network communications to identify deviations from these baselines, **such as exercising new communication links or new devices**, and sends notifications, facilitating effective compliance management. Organizations can utilize two features in the Platform: **Baselines** and **Learning Mode**.
- The Baseline feature detects deviations in assets, including non-baselined communications and protocols. Learning Mode can be enabled to add all observed assets and behaviors to the baseline. Once the environment is learned, disabling Learning Mode enables detection of deviations.
- The Dragos Platform employs passive monitoring techniques **to detect and evaluate anomalous network activity**.

- The Dragos Platform conducts **passive monitoring** on identified assets. Specifically, the Dragos Platform automatically analyzes data it receives against known **IOCs** provided by the Dragos Intelligence team through each new Knowledge Pack.
- The Dragos Platform detects and alerts on **threat behaviors**, which are known adversary tradecraft and **TTPs** relevant to the OT environment. Threat behaviors abstract away individual technical elements of indicators and instead focus on the behavior. This makes threat behavior analytics used by the Dragos Platform more capable of scaling and more resilient than specific indicators.

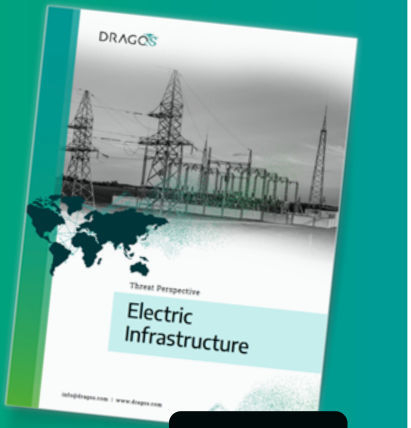
Services:

- Dragos can conduct a **Sensor Placement Study** to analyze and provide recommendations for proper Dragos Sensor placement. The goal is to analyze the necessary Sensor locations to achieve optimal visibility of internal network traffic. Sensor Placement Studies are based on network documentation and interviews with SMEs.
- Per CIP-015, any data associated with potential attempts to compromise, or a suspected cyber security event, should be retained and fed into the entity's Reliability Standard CIP-008 incident response process(es) for further investigation. **See CIP-008 Incident Reporting and Response Planning for a list of services offered by Dragos.**

OT CYBER THREAT INTELLIGENCE

ELECTRIC THREAT PERSPECTIVE

The Dragos Threat Intelligence team leads the industrial cybersecurity market as the largest private cyber threat intelligence team entirely focused on ICS/OT threats. Encompassing the consolidated knowledge and skills gained from hunting adversaries, deconstructing ICS malware, analyzing vulnerabilities, and engineering threat detections, the Dragos Threat Intelligence team, through WorldView, delivers comprehensive knowledge and defensive recommendations to stay ahead of emerging OT threats. Dragos WorldView OT Cyber Threat Intelligence is used in SOCs and board rooms down to the physical facilities that power electric grids.



Download

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