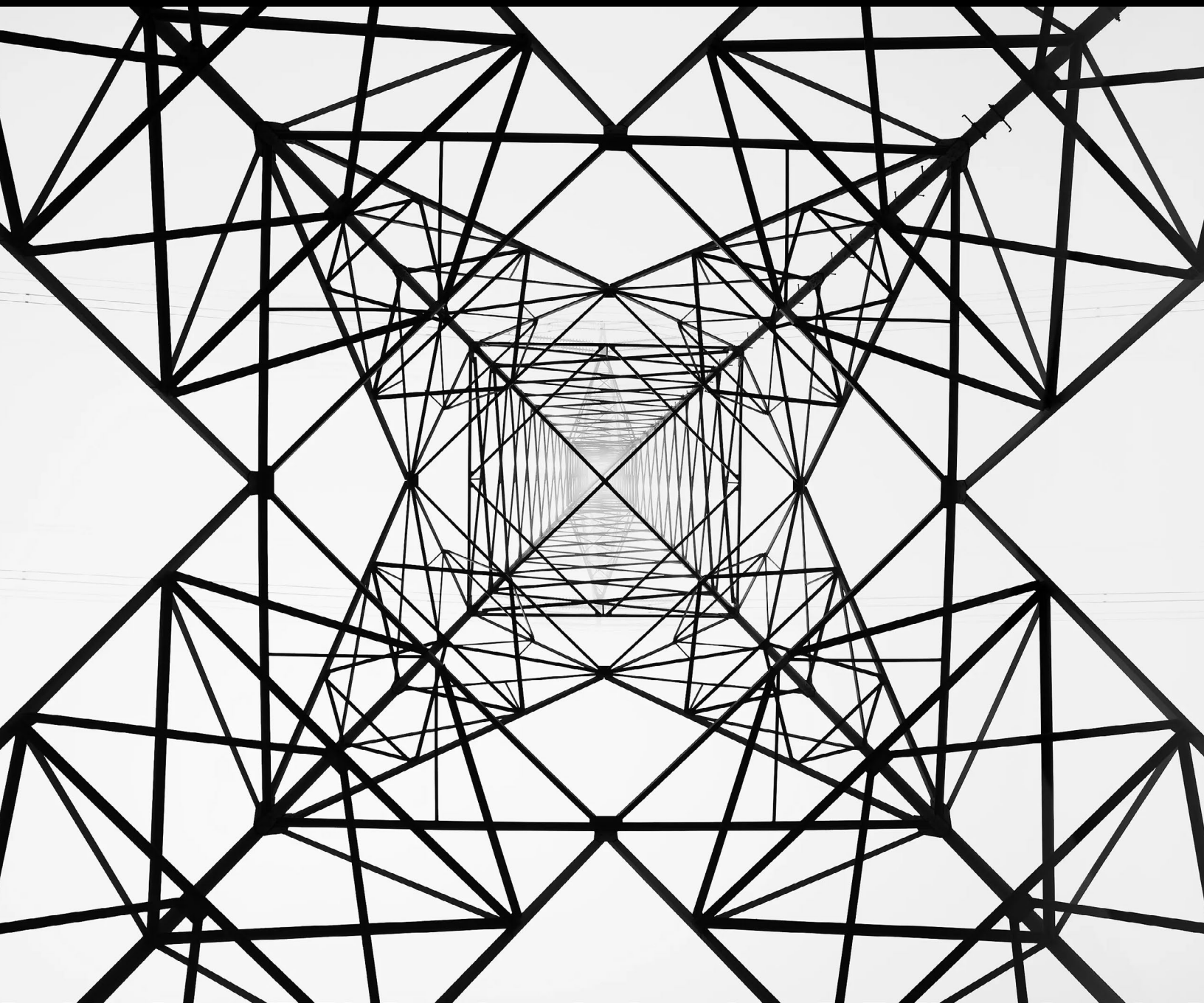
DRAGOS

SOLUTION BRIEF

How Dragos Supports NERC CIP Reliability Standards

The Dragos Platform and Services



Overview:

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
- Advanced threat detection and vulnerability management
- Rapid investigation and response capabilities
- Weekly Knowledge Packs, Dragos-authored content releases that deliver new detections, IOCs, and response playbooks directly to the platform
- Integrated findings from adversary threat hunters and service engagements

The Dragos Services team complements the Dragos Platform with expertise in OT security maturity assessments, incident response planning, and OT security practices, empowering organizations to make informed decisions about their security posture.

CIP-002

BES Cyber System Categorization

Platform:

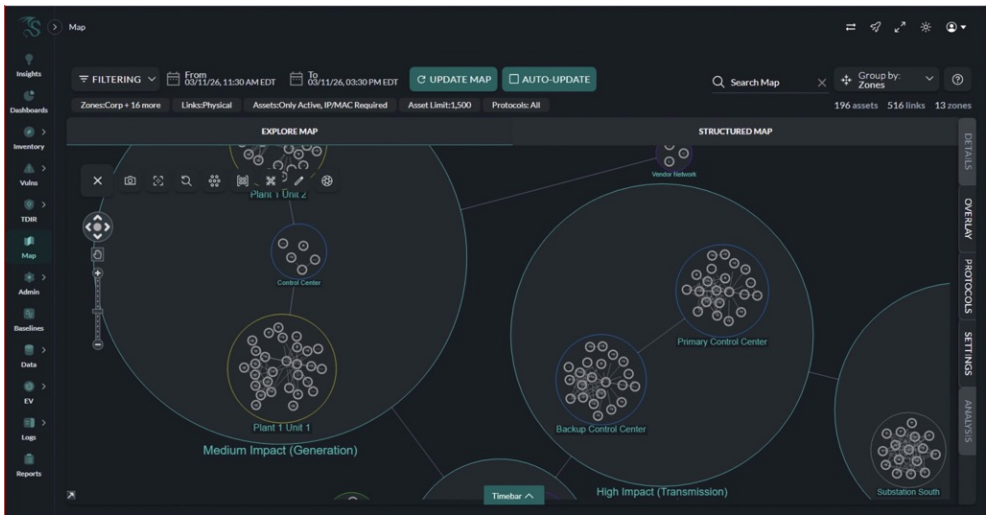
The Dragos Platform employs passive monitoring techniques to observe and identify devices connected to the network. The platform offers several capabilities, including alerting on assets within the Electronic Security Perimeter(s) (ESP) not listed in the asset inventory system via export and/or API integration,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

For controlled environments, the platform also offers active collection capabilities through the **Extended Visibility Agent** that safely queries devices without disrupting operations, enabling organizations to validate asset inventories against authoritative records and confirm configuration integrity. Active collection helps identify unauthorized or rogue devices, detect misconfigurations, and verify firmware versions, supporting NERC CIP requirements for asset management. By combining active collection with passive monitoring, the platform provides a layered approach to visibility and security, reducing blind spots, and strengthening the overall security posture.

Additionally, Dragos Platform provides visual network maps that clearly depict network zones, helping organizations understand traffic flows and dependencies. As illustrated in *Figure 1*, entities can create zones and parent zones that correspond to their facility's designated impact ratings, allowing clear visualization of traffic flows between High, Medium, and Low impact sites. The maps show how assets and components relate to one another, providing a clear view of device interconnections and communication pathways.

Figure 1

Asset Map



NP-View:

Building on the zoning and impact-based network views illustrated in Figure 1, NP-View provides a complementary, architect-grade representation of these same environments, enabling deeper validation and documentation of BES Cyber System boundaries and dependencies.

NP-View extends the Dragos Platform's support for CIP-002 by providing visualization of OT network architecture and asset relationships. Using OT-aware network diagrams, NP-View enables organizations to model and document BES Cyber System environments, including substations, control centers, and supporting communication paths. These visualizations help clearly delineate BES Cyber Systems and associated assets, supporting accurate impact categorization and scoping decisions under CIP-002.

Services:

Dragos Architecture Reviews and Cybersecurity Architecture Design Reviews (CADR), delivered as part of Dragos OT Cybersecurity Assessment services, help organizations assess the defensibility of their OT network and cybersecurity program against evolving threats. These reviews include detailed topology analysis, evaluation of network segmentation and data collection strategies, and compromise assessments to identify potential adversary activity and architectural weaknesses. The process examines critical assets, communication paths, and trust boundaries, and may incorporate asset inventory validation, indicator-of-compromise analysis, and threat discovery using the Dragos Platform. The outcome is a set of prioritized, actionable recommendations to harden OT architectures, improve resilience, and support alignment with regulatory frameworks such as NERC CIP.

CIP-003

Security Management Controls

Platform:

The Dragos Platform provides OT-aware visibility and detection capabilities to help organizations monitor for, and detect, known or suspected malicious communications associated with vendor electronic remote access. By leveraging deep packet inspection and Dragos' four types of threat detection, the platform enables defenders to observe remote connectivity patterns and identify activity that deviates from expected operational behavior. These capabilities are presented through dashboards that support investigation and response within industrial environments.

Dashboards and interactive network maps provide centralized visibility into remote access communications and associated assets, enabling teams to understand how external connections traverse the OT network. Sensors deployed at key network boundaries support visibility into ingress and egress traffic and generate alerts to assist with timely response to suspicious behavior. In addition, the platform's Communications Hub surfaces detailed communication context, such as source and destination assets, protocols, and session characteristics, to support focused investigation of remote access activity.

Additional capabilities include analytics for commonly observed remote access tools and protocols, extended asset context derived from passive monitoring and OT-safe active collection, and baselining of normal communications and behaviors. Baselines allow organizations to establish expected patterns for remote access and system interactions, and highlight deviations that may indicate unauthorized activity, misuse of access, or emerging threats. Together, these capabilities enhance situational awareness, support security operations, and assist organizations in meeting operational and compliance objectives, including those associated with NERC CIP.

The Dragos Platform also helps organizations support Transient Cyber Asset (TCA) requirements under CIP-003 by providing OT-aware visibility into devices that connect to BES Cyber System environments. Using passive monitoring, the platform can identify transient devices as they appear on the network and associate observed communications with the relevant assets and network zones. This information can be compared against approved TCA Plans to help verify that TCAs used are authorized.

NP-View:

NP-View helps organizations document how remote access is permitted within the OT environment by modeling vendor remote access paths, trust boundaries, and electronic access controls. These network views support policy enforcement, change management, and internal oversight by enabling stakeholders to visualize and validate remote access architectures against established security management controls. NP-View diagrams can be maintained as living documentation, helping to support CIP-003 requirements related to vendor electronic remote access.

Services:

Standards & Regulations Reviews are included in Dragos' Cybersecurity Architecture Design Review (CADR) to help organizations evaluate their OT cybersecurity program against recognized standards such as NERC CIP. These reviews assess governance structures, policies, procedures, technologies, and resources used to manage and protect OT and BES Cyber Systems. The assessment identifies capability gaps, evaluates the effectiveness of existing practices, and provides prioritized recommendations to improve program maturity and consistency.

CIP-004
Personnel & Training

Community Resources:

To support requirements related to personnel awareness and training for individuals with access to critical assets, Dragos provides a set of community and intelligence resources focused on OT cybersecurity. These resources are designed to complement, not replace, entity specific training and compliance programs.

Dragos Academy:

Dragos Academy is an OT focused cybersecurity training program that delivers education based on the same skills and methodologies used by Dragos analysts, consultants, and practitioners in real world industrial environments. Training is available through self-paced, on-demand courses as well as instructor-led sessions delivered by Dragos experts. Course content covers ICS/OT fundamentals, threat detection, vulnerability management, and effective use of the Dragos Platform, while structured learning paths and certifications support workforce development and skill validation.

While Dragos Academy should not be relied upon as the sole mechanism to meet CIP-004 requirements, it serves as a valuable supplement to organization specific training programs.

Operational Technology – Cyber Emergency Readiness Team (OT-CERT):

OT-CERT provides complimentary resources to the ICS/OT community to help organizations build and mature OT cybersecurity programs. OT-CERT offers free access to threat advisories, best-practice guidance, templates, tabletop exercise materials, and educational content designed to improve baseline awareness, preparedness, and resilience across operations, engineering, and security teams.

CIP-005
Electronic Security Perimeter(s)

Platform:

The Dragos Platform helps support CIP-005 by providing OT-aware visibility and detective controls for communications entering and exiting defined network boundaries including Electronic Security Perimeters (ESPs). Dragos Sensors can be deployed inside and outside of the network boundary to provide ingress and egress visibility, helping organizations observe and investigate known or suspected malicious communications. Through deep packet inspection, protocol-aware analytics, and behavioral analysis, the platform identifies suspicious activity within OT environments without disrupting operations.

Passive monitoring provides continuous, non-intrusive visibility into OT assets and communications as they naturally occur, establishing baselines and supporting anomaly detection. In addition, the platform supports controlled, OT-safe active collection in appropriate environments to selectively enhance visibility, where passive monitoring alone may be insufficient. Active collection is deliberate, read-only, and protocol-aware, with data requests executed during planned windows. These capabilities help clarify asset attributes, support validation of observed communication paths, and improve understanding of remote access mechanisms, complementing passive monitoring without introducing operational risk.

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 platform also 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.

NP-View:

NP-View complements the Dragos Platform by providing OT-specific network architecture and access-path analysis that helps support the design and review of CIP-005 Electronic Security Perimeters (ESPs). By modeling network topology, firewall rules, and routing configurations, NP-View enables organizations to visualize potential communication paths into, out of, and within the ESP, including pathways that may exist outside of designated Electronic Access Points (EAPs).

These offline, non-intrusive analyses help support validation of segmentation design, identify unintended or undocumented access paths, and assist with documentation of ESP boundaries and Intermediate Systems, such as Electronic Access Control or Monitoring Systems (EACMS).

NP-View's maintained diagrams and reports, updated as network and configuration data changes, provide defensible architectural evidence to support CIP-005 audit activities, architecture reviews, and compliance assessments conducted by the asset owner.

Services:

To help organizations in understanding the security of their ESPs and support secure remote access principles, Dragos offers a suite of specialized services:

- **Sensor Placement Studies:** Comprehensive analysis to determine optimal sensor locations inside and adjacent to critical networks such as an ESP, supporting ingress and egress visibility aligned with monitoring objectives. These studies help organizations improve visibility coverage and support validation of sensor deployment strategies within OT environments.
- **Architecture Reviews:** Detailed evaluation of OT network architecture, segmentation, and perimeter design to assess network boundaries, access points, and remote access pathways. Reviews identify architectural weaknesses, support validation of segmentation intent, and provide actionable recommendations to strengthen perimeter defenses and remote access controls.

- **Tabletop Exercises:** Scenario-based exercises that simulate realistic OT cyber incidents, including remote access compromise scenarios. These exercises test incident response processes, decision-making, and coordination across technical and leadership teams, helping identify gaps and improve response readiness.
- **Rapid Response Retainer:** Ongoing access to Dragos OT incident response experts for rapid support during cybersecurity events such as those involving network boundary violations or remote access compromise. The retainer includes onboarding to document the environment and provides priority access to responders for containment, investigation, and recovery activities.

CIP-007
Systems Security Management

Platform:

The Dragos Platform supports system security management in OT environments by providing continuous, OT-aware monitoring and threat detection for assets where traditional antivirus solutions cannot be deployed, such as protection relays and RTUs running real-time operating systems (RTOS).

Using deep packet inspection and four types of OT threat detection, configuration analysis, anomaly detection, threat behavior analytics, and indicators of compromise (IOCs), the platform identifies malicious activity and abnormal behavior with high fidelity and low noise, enabling timely investigation and response in operationally sensitive environments.

The platform generates alerts for security-relevant network activity, including malicious indicators, anomalous authentication-related behavior, and suspicious access attempts detectable through OT traffic analysis. Log retention settings are configurable to support retention periods consistent with CIP-007 requirements (e.g., minimum 90-day log availability, where applicable), and events can be exported via centralized logging integrations to external systems such as SIEM solutions or Syslog for correlation and analysis.

In addition to passive monitoring, the platform supports controlled, OT-safe active collection in appropriate environments to enrich asset context and improve vulnerability identification. Asset data collected through active collection, such as operating system versions, firmware details, software context, and hardware relationships, enhances vulnerability matching and prioritization. Together, passive monitoring and active collection help strengthen overall OT security posture and support CIP-007 requirements.

Community Resources:

Dragos WorldView delivers OT exclusive threat intelligence through a secure portal, providing actionable insight into emerging threats, vulnerabilities, and adversary activity targeting industrial environments. WorldView content is updated regularly and includes analysis of adversary tactics, techniques, and procedures (TTPs) mapped to MITRE ATT&CK for ICS, indicators of compromise (IOCs), and OT-specific vulnerability analysis with operational context.

WorldView also publishes advisory alerts and in-depth vulnerability and incident reports with defensive recommendations tailored for OT systems. Intelligence from WorldView integrates directly into the Dragos Platform to continuously update detections and response guidance. Combined with OT-CERT resources, WorldView empowers security teams to anticipate threats and prioritize defenses more effectively.

CIP-008

Incident Reporting and Response Planning

Platform:

The Dragos Platform provides a centralized incident management dashboard where security teams can view, triage, and prioritize alerts, incidents, and ongoing investigations. Predefined response playbooks are integrated into the platform and outline step-by-step procedures and workflows for responding to different types of incidents, helping ensure consistent and effective response actions.

Incident response is further streamlined through integrated case management capabilities that allow teams to document investigation context, analyst decisions, and remediation actions in a single system of record. Artifacts associated with a case including alerts, playbooks, packet captures (PCAPs), and other forensic data, are retained to support audit readiness, incident review, and long-term forensic analysis.

The Dragos Platform also integrates with Security Information and Event Management (SIEM) solutions and Security Operations Center (SOC) automation tools to support rapid investigation and coordinated response across enterprise security workflows. Together, these capabilities enhance incident reporting and response planning by combining OT-aware detection, centralized management, guided response workflows, forensic visibility, collaboration features, and support for continuous improvement.

Services:

- **Rapid Response Retainer:** The Dragos Rapid Response Retainer provides 24/7 access to OT-specialized incident responders to support preparation, response, and recovery during cybersecurity incidents affecting industrial environments. The retainer pre-establishes agreements and documents the customer environment to reduce response timelines and includes expert-led forensic analysis, containment guidance, recovery support, and stakeholder reporting. For organizations using the Dragos Platform, the retainer enables priority, SLA-backed response and more effective investigation using historical OT telemetry. Retainer hours may also be applied to proactive preparedness services.

- **Tabletop Exercises:** Dragos Tabletop Exercises are scenario-based engagements that test OT incident response capabilities using realistic industrial threat scenarios. These exercises evaluate decision-making, coordination, and response workflows across technical and leadership teams, helping organizations identify gaps, validate response plans, and capture lessons learned to improve readiness.

- **Incident Response Plan (IRP) Workshops:** Incident Response Plan Workshops are structured, collaborative sessions designed to review, develop, or refine OT-specific incident response plans. Using Dragos incident response expertise and OT threat intelligence, these workshops assess response workflows, clarify roles and escalation paths, and align plans with operational constraints and current threat scenarios. IRP Workshops may be delivered independently or as part of a Rapid Response Retainer engagement.

- **OT Watch:** Dragos OT Watch delivers expert-driven, proactive threat hunting for OT environments. Dragos analysts continuously investigate identified suspicious activity using the Dragos Platform, OT-specific threat intelligence, and insights derived from incident response, compromise assessments, and Neighborhood Keeper community data. OT Watch integrates with existing security teams and processes to enhance visibility, reduce dwell time, and improve detection maturity without adding internal operational burden.

- **OT Watch Complete:** Dragos OT Watch Complete extends OT Watch by providing full-service managed monitoring and operational support of the Dragos Platform. This includes 24/7 alert triage, advanced threat hunting, asset visibility and rogue device identification, vulnerability management support, and continuous security hardening recommendations. OT Watch Complete embeds Dragos incident response expertise directly into ongoing operations, providing deeper engagement and sustained risk reduction for critical infrastructure environments.

CIP-009

Recovery Plans for BES Cyber Systems

Platform:

The Dragos Platform includes backup and restore capabilities designed to help support recovery planning and execution under CIP 009. The platform enables administrators to back up and restore configuration settings and core application state for key components, including the SiteStore and Sensors, to support recovery or rebuild activities following a system failure or cyber event.

Backup and restore events are recorded within the Platform UI and audit logs, providing visibility into if they are successful and unsuccessful. These capabilities help organizations validate recovery procedures, test restore processes in non production environments, and maintain readiness to restore monitoring functionality following a cyber security incident.

Services:

- The services described under CIP-008 Incident Reporting and Response Planning also support CIP-009 Recovery Plans for BES Cyber Systems by enabling organizations to prepare for, execute, and validate recovery activities following a cybersecurity incident. **Rapid Response Retainers, Tabletop Exercises, and Incident Response Plan (IRP) Workshops** help organizations test recovery procedures, clarify roles and responsibilities, capture lessons learned, and improve recovery readiness in alignment with CIP-009 requirements.

CIP-010

Configuration Change Management, Vulnerability Assessments, and Transient Cyber Assets

Platform:

The Dragos Platform provides OT-specific vulnerability management by combining passive monitoring with controlled, OT-safe active collection to enrich asset context and identify vulnerabilities across industrial environments. The platform aligns hardware, software, and OS vulnerabilities to assets, and applies OT-specific context and prioritization, informed by Dragos Threat Intelligence and delivered through weekly Knowledge Packs.

Dragos' "Now, Next, Never" methodology helps organizations focus remediation efforts on vulnerabilities that pose the greatest operational risk, while supporting operationally safe mitigation strategies appropriate for OT systems. These capabilities complement existing vulnerability assessment and secure configuration management processes.

The Dragos Platform helps organizations support Transient Cyber Asset (TCA) requirements under CIP-010 by providing OT-aware visibility into devices that connect to BES Cyber System environments. Using passive monitoring, the platform can identify transient devices as they appear on the network and associate observed communications with the relevant assets and network zones. This information can be compared against approved TCA Plans to help verify that TCAs used are authorized.

To support regulatory programs such as NERC CIP, the platform includes dashboards that assist in identifying assets and communications. These views help track change-related activities and provide contextual evidence to help support compliance workflows associated with CIP-010 and related standards.

The platform's Insights Hub consolidates vulnerability, asset, and threat information into a single, prioritized view that accelerates decision-making across security workflows. By leveraging vulnerability analysis and risk-weighted prioritization authored by Dragos OT cybersecurity experts, Insights Hub helps teams efficiently prioritize and coordinate response actions in alignment with broader enterprise security and configuration management programs.

Services:

Dragos Network Vulnerability Assessments are expert-led evaluations designed to identify security weaknesses within OT networks and assess the effectiveness of existing technical controls. These assessments use a collaborative, OT-safe approach that combines passive observation with targeted information gathering and configuration review to identify vulnerabilities that could potentially be exploited by adversaries for initial access, lateral movement, or privilege escalation. Leveraging the Dragos Platform for network telemetry analysis and asset context, the assessment produces a prioritized set of findings and actionable recommendations to strengthen OT network defenses and improve overall security posture.

CIP-012

Communications between Control Centers

Platform:

When encryption is used to protect communications between Control Centers, the Dragos Platform provides OT-aware network visibility that can help identify communication paths and protocols used to transmit real-time monitoring and assessment data. Through passive inspection of network traffic, the platform can highlight the use of protocols or sessions that may appear unencrypted or misaligned with documented security protections, providing visibility that supports validation and investigation activities related to CIP-012 requirements.

CIP-013

Supply Chain Risk Management

Resources:

Dragos supports NERC CIP013 Supply Chain Risk Management through documented contractual, administrative, and security commitments designed to help entities assess and manage vendor-related cyber risk. Dragos addresses supply-chain risk considerations applicable to Dragos offerings used by entities subject to the NERC CIP Standards in the Dragos NERC CIP-013 Addendum. The addendum outlines Dragos' obligations related to secure access controls, personnel authorization, vulnerability remediation timelines, and protections against the introduction of malicious code through software or third-party components.

Entities can reference this addendum as part of their CIP 013 vendor risk assessments and procurement documentation to support evaluation of supplier controls and risk management practices in alignment with CIP 013 requirements. Dragos also provides responses to vendor supply chain risk questionnaires upon request.

CIP-015

Internal Network Security Monitoring

Platform:

The Dragos Platform supports Internal Network Security Monitoring (INSM) by providing continuous, passive visibility into network traffic within trusted zones such as Electronic Security Perimeters (ESPs), and adjacent networks that include EACMS, PACS, and SCI. While Internal Network Security Monitoring can be achieved through passive, protocol-aware monitoring, the Dragos Platform also supports optional, OT-safe active collection in appropriate environments to selectively enrich asset context and validate inventory details without disrupting operations.

Anomalous activity is evaluated using a layered detection model that incorporates the Dragos Platform's four types of OT threat detection. Baseline and anomaly detection identify deviations in east-west communications and asset behavior, while configuration analysis highlights changes to assets, services, or protocols that may indicate misconfiguration or unauthorized modification.

Baseline development is supported through an initial learning period during which the platform observes normal network communications and asset behaviors within the monitored zone. After this learning phase, ongoing monitoring focuses on identifying deviations from the established baseline, enabling detection of potentially suspicious internal activity without disrupting operations.

Threat behavior analytics assess observed activity against known adversary tactics and techniques relevant to OT environments, and indicator-based detections, informed by Dragos Threat Intelligence and IOCs, provide validation against known malicious artifacts. By correlating results across the Dragos Platform's four types of OT threat detection, the platform supports consistent evaluation of anomalous internal network activity and enables informed investigation and response aligned with CIP-015 requirements.

To support CIP-015 data retention requirements, the Dragos Platform retains internal network security monitoring data associated with anomalous activity, including network traffic metadata, alerts, detection artifacts, and investigation context based on entity-defined retention settings. Data can be preserved within the platform and, where appropriate, forwarded to external systems such as SIEM solutions to align with organizational retention policies and incident response requirements.

To support CIP-015 requirements to protect INSM data, the Dragos Platform implements protective and detective controls designed to safeguard monitoring data from unauthorized access or modification. These controls include role-based access control (RBAC), data access controls, user activity logging, and support for multi-factor authentication.

NP-View:

NP-View complements the Dragos Platform by providing network architecture and segmentation visibility that helps to support validation and documentation of internal network design. By analyzing router, switch, and firewall configurations, NP-View creates accurate topology maps and access-path models that show how zones are interconnected and how traffic is permitted to flow within and between trusted network segments.

When used alongside the Dragos Platform's monitoring and detection capabilities, NP-View helps teams to correlate observed anomalous traffic identified by the Dragos Platform with intended network design. This helps to support verification of internal segmentation, identification of unintended access paths, and validation of zone boundaries. NP-View's configuration-based analysis and reporting provide documentation to help support CIP-015 compliance activities, architecture reviews, and audit readiness by providing point-in-time, configuration-based evidence without impacting live operations.

Services:

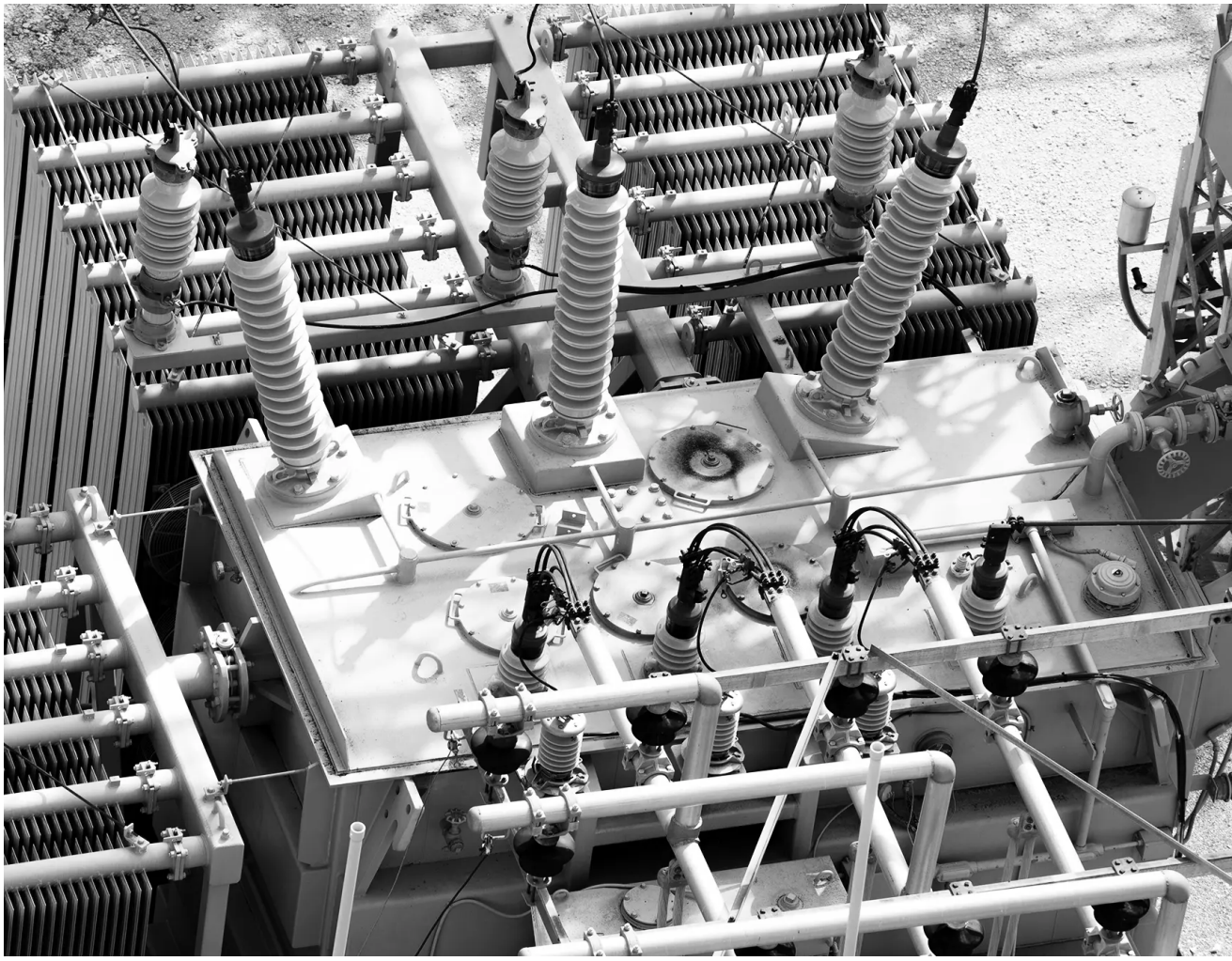
Dragos offers Sensor Placement Studies as a services engagement to help organizations determine optimal Dragos Sensors locations for OT-safe, passive monitoring and stronger visibility of internal network traffic. The study is typically driven by a review of existing network documentation (e.g., diagrams, segmentation strategies, and asset inventories) and interviews with subject matter experts to understand operational workflows, critical assets, and key communication paths. Findings focus on identifying visibility gaps and producing deployment recommendations that maximize coverage of trusted zones (including within ESPs where applicable) and critical traffic flows, helping organizations improve monitoring outcomes and supporting regulatory objectives by improving visibility into internal network traffic and INSM/CIP-015 planning and evidence alignment.

Call to Action

Meeting NERC CIP requirements requires more than point solutions or periodic compliance activities. It requires sustained visibility, defensible architecture, actionable intelligence, and operationally safe security practices purpose built for OT environments.

As outlined throughout this document, the Dragos Platform, NP-View, Dragos Community Resources, and Dragos Services can be used together to help organizations strengthen cybersecurity resilience and support NERC CIP use cases, from asset identification and perimeter protection to monitoring, and incident response. By aligning technology, intelligence, and expert services to the realities of BES operations, Dragos enables organizations to reduce risk while building durable, audit ready compliance programs.

To take the next step, engage with Dragos to assess your current environment, identify and prioritize gaps, and develop a roadmap that advances both regulatory compliance and real-world cyber resilience for your critical infrastructure.



Appendix A:

Summary Mapping of NERC CIP Standards to Dragos Capabilities

NERC CIP Standard	Primary Objective	Dragos Technology (Platform & NP-View)	Dragos Services & Resources
CIP-002 BES Cyber System Categorization	Identify and categorize BES Cyber Systems based on impact (Low, Medium, High) to determine applicable security controls.	**Platform:** OT-aware passive and controlled OT-safe active asset discovery; asset inventory validation; custom asset tagging (e.g., EACMS, PACS, BES Cyber Systems); visualization of zones and impact ratings; network flow visibility. **NP-View:** OT network diagrams and dependency mapping to document BES Cyber System boundaries, supporting impact categorization and scoping decisions.	Architecture Reviews; Cybersecurity Architecture Design Reviews (CADR); OT Cybersecurity Assessments
CIP-003 Security Management Controls	Establish governance, policies, and oversight to manage and enforce cybersecurity practices. Low Impact Cyber security program requirements.	**Platform:** Monitoring and detection of vendor and remote access activity; behavioral baselining; intelligence-driven alerts; centralized dashboards for investigation and oversight; Monitoring and detection of TCAs; Comms Hub. **NP-View:** Documentation of vendor remote access paths, trust boundaries, and electronic access controls to support policy enforcement and change management.	Standards & Regulations Reviews (via CADR)

NERC CIP Standard	Primary Objective	Dragos Technology (Platform & NP-View)	Dragos Services & Resources
CIP-004 Personnel & Training	Ensure personnel with access to BES Cyber Systems are properly trained, vetted, and authorized.	**Platform / NP-View:** None	Dragos Academy training and certifications; OT-CERT community resources, advisories, templates, and tabletop materials
CIP-005 Electronic Security Perimeter(s)	Define and protect network boundaries (ESPs) and control electronic access to BES Cyber Systems.	**Platform:** Ingress and egress traffic monitoring; detection of suspicious boundary communications; visibility into remote access paths and EACMS usage; OT-safe validation of observed communications. **NP-View:** Architecture-based access-path analysis to validate ESP boundaries, Electronic Access Points (EAPs), and Intermediate Systems; identification of unintended or undocumented access paths.	Sensor Placement Studies; Architecture Reviews; Tabletop Exercises; Rapid Response Retainer
CIP-007 System Security Management	Secure BES Cyber Systems through technical controls like patching, ports/services management, malware protection, and logging.	**Platform:** OT-aware threat detection where traditional AV is not feasible; anomaly, behavior, configuration, and IOC-based detections; configurable log retention; SIEM/Syslog export; vulnerability enrichment using OT-safe active collection.	Dragos WorldView threat intelligence; OT-CERT resources

NERC CIP Standard	Primary Objective	Dragos Technology (Platform & NP-View)	Dragos Services & Resources
CIP-008 Incident Reporting and Response Planning	Detect, classify, report, and respond to cybersecurity incidents.	**Platform:** Centralized incident management; alert triage; case tracking; forensic artifact retention; integrated response playbooks; enterprise security tool integrations.	Rapid Response Retainer; Tabletop Exercises; IRP Workshops; OT Watch; OT Watch Complete
CIP-009 Recovery Plans for BES Cyber Systems	Ensure systems can be restored following a cyber incident or disruption.	**Platform:** Backup and restore capabilities; audit logging of backup and restore events	Rapid Response Retainer, Tabletop Exercises, IRP Workshops
CIP-010 Configuration Change Management and Vulnerability Assessments	Control system changes and identify vulnerabilities to maintain a secure baseline.	**Platform:** OT-specific vulnerability management; passive monitoring combined with OT-safe active collection; risk-based prioritization ("Now, Next, Never"); compliance dashboards; Insights Hub; Monitoring and detection of TCAs. **NP-View:** Configuration-based visibility to support architectural validation during change reviews.	Network Vulnerability Assessments
CIP-012 Communications Between Control Centers	Protect the confidentiality and integrity of real-time operational communications between control centers (e.g., via encryption).	**Platform:** Passive visibility into communication paths and protocols; identification of sessions that may appear unencrypted or misaligned with documented protections.	None
CIP-013 Supply Chain Risk Management	Identify, assess, and manage cybersecurity risks associated with vendor and supplier relationships.	**Platform / NP-View:** CIP-013 is addressed through contractual and administrative controls rather than technical platform features.	Dragos NERC CIP-013 Addendum; vendor risk assessment responses

NERC CIP Standard	Primary Objective	Dragos Technology (Platform & NP-View)	Dragos Services & Resources
CIP-015 Internal Network Security Monitoring	Detect and evaluate anomalous internal network activity.	**Platform:** Passive east-west network monitoring; baselining and anomaly detection; four types of OT threat detection; optional OT-safe active collection for enrichment; evidence retention and access controls. **NP-View:** Segmentation validation and access-path modeling; correlation of detected anomalous traffic identified by the Dragos Platform with intended network design; audit-ready documentation.	Sensor Placement Studies

About Dragos

Dragos is the world's leading OT cybersecurity firm headquartered in Washington DC, USA area with offices around the world. It provides the most effective OT cybersecurity technology for industrial and critical infrastructure to deliver on our global mission: safeguarding civilization. The Dragos Platform provides visibility and monitoring of OT environments for asset identification, vulnerability management, and threat detection with continuous insights generated by the industry's most experienced OT threat intelligence and services team. Dragos protects customers across the range of operational sectors, including electric, oil & gas, data centers, manufacturing, water, transportation, mining, and government.

Learn more: dragos.com