SOLUTION BRIEF

OT Cybersecurity Solutions For NERC CIP

How Dragos Supports the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)

NERC CIP is a series of standards developed to protect critical cyber assets used to operate North America's Bulk Energy Systems (BES) and associated devices from attack. Released in 2008, the standards are mandatory and enforceable.

The expansive coverage and level of detail in cybersecurity frameworks like NERC CIP can be challenging. Dragos provides the technology in the Dragos Platform to implement many of the most critical operational technology (OT) security controls contained in NERC CIP. Our Professional Services group provides the expertise to help evaluate and mature your OT security practice, while our Threat Intelligence team delivers the situational awareness on new threats and vulnerabilities.

Dragos Value Summary to OT Security Environments Leveraging NERC CIP

Dragos mission is to safeguard civilization. We deliver the critical elements crucial to implementing NERC CIP, along with a focus on making you successful in building an effective OT security program.

Complying with NERC CIP

There are thirteen domains in NERC CIP, each covering a particular type of control or capability to help build OT security programs. We've provided a summary of the domains below, along with how Dragos can help to fulfill domain requirements.

DOMAINS	DESCRIPTION	DRAGOS PLATFORM / SERVICES
CIP-002	BES Cyber System Categorization: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of security requirements.	The Dragos Platform provides asset discovery, profiling, inventory, and change tracking for OT devices. It passively monitors the network and has the capability to detect threats and support forensic analysis. The Dragos Professional Services team performs Architecture Review assessments which can assist in preliminary asset identification, categorization, and profiling.
CIP-003	Security Management Controls: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems.	Our Program Assessment Services can help identify gaps in, evaluate, and recommend steps to mature plans, procedures, and technologies. Our Capability Maturity Model Services can help track cybersecurity program management content and progress.
CIP-004	Personnel and Training: To require an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.	Dragos Academy offers training resources for ICS infrastructure and associated cybersecurity concerns, as well as access to ongoing briefings on new threat intelligence findings. This can help organizations build ICS cybersecurity training programs for their personnel.
CIP-005	Electronic Security Perimeter(s): To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter (ESP) in support of protecting BES Cyber Systems.	Dragos Platform architecture can strategically place multiple sensors in the environment to accommodate monitoring within the ESP and outside the ESP, to provide visibility to ingress and egress communications. The Dragos Platform can help entities identify external communications that may not be routed through an Electronic Asset Point (EAP) by using the Asset map and communications analysis capabilities. The Platform captures active vendor remote access sessions and identifies which connections exist. 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-006	Physical Security of BES Cyber Systems: To specify a physical security plan in support of protecting BES Cyber Systems.	N/A

DOMAINS	DESCRIPTION	DRAGOS PLATFORM / SERVICES
CIP-007	System Security Management: To manage system security by specifying select technical, operational, and procedural requirements.	Dragos Platform logs events on applicable cyber assets by detecting: • successful login attempts • failed access attempts and failed login attempts • malicious code Users can leverage case books in the Dragos Platform to track patch management cycles, testing, and mitigation resolution.
CIP-008	Incident Reporting and Response Planning: To specify incident response requirements to mitigate the risk to the reliable operations of the BES Cyber Systems.	Dragos Platform delivers alerts into incidents, integrations with SIEM and SOC automation tools, the ability to rapidly investigate incidents, integrations with firewalls and endpoint security platforms to rapidly isolate problematic endpoints, and playbooks that provide specific, best practice guidance to dealing with incidents.
CIP-009	Recovery Plans for BES Cyber Systems: To specify recovery plan requirements in support of the continued stability, operability, and reliability of the BES Cyber Systems.	Our Professional Services team, through Rapid Response Retainers, delivers capabilities to prepare for, respond to, and recover from cyber incidents. The Dragos Services team offer tabletop exercises that can satisfy the incident response plan testing requirements and provide feedback for lessons learned.
CIP-010	Configuration Change Management and Vulnerability Assessments: To prevent and detect unauthorized changes to BES Cyber Systems.	Dragos Platform provides the ability to automatically create OT asset inventories, monitor changes, visualize asset organization, and map vulnerabilities to specific asset types. • Create an asset inventory and asset profiles, including software versions • Monitors OT network activity, analyzes traffic to identify changes to the environment • Allow you to organize assets into zones to simplify visualization of assets and traffic • Map vulnerabilities to the assets • Monitor changes, communication sessions, command execution, and network telemetry and analyze that data for irregularities and threats Dragos Platform monitors OT network activity analyzes traffic and protocols to detect threats. The information logged by the system is used for in-depth forensics and root cause analysis. Additionally, Dragos Professional Services provides a suite of Architecture Review capabilities to assist in creation of inventories and identify current vulnerabilities and threats.

DOMAINS	DESCRIPTION	DRAGOS PLATFORM / SERVICES
CIP-011	Information Protection: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements.	Dragos Platform does not directly manage identities or access management policies. The following can add value to this domain: • Firewall integration to provide insights into access control policies • OT network traffic monitoring documenting network logon attempts and analyzing traffic to detect potential attacks and threat behaviors Dragos Professional Services provides best practice recommendations for securing remote access into OT environments through use of access control policy recommendations, network segmentation, multi-factor authentication, use of jump hosts, and active monitoring of OT networks and traffic.
CIP-012	Communications between Control Centers: To protect the confidentiality and integrity of real-time assessment and real-time monitoring data transmitted between Control Centers.	N/A
CIP-013	Supply Chain Risk Management: Implement security controls for supply chain risk management to mitigate cybersecurity risks to the reliable operation of the BES Cyber System.	Dragos Threat Intelligence identifies activity groups that target hardware and software, like VPNs. They can also help identify and share vulnerabilities for existing equipment architecture.
CIP-014	Physical Security: To protect the physical assets of BES Cyber Systems.	N/A

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.

To learn more about our technology, services, and threat intelligence offerings, visit **dragos.com** or connect with us at **sales@dragos.com**.