WHITE PAPER

SUPPORTING NERC CIP COMPLIANCE

Mapping Features of The Claroty Platform to Standard Requirements for NERC CIP Compliance

CLAROTY

CONTENTS

INTRODUCTION

Electric industry asset owners in North America are subject to mandatory cybersecurity regulations developed by the North American Electric Reliability Corporation (NERC). The regulations, known as the NERC CIP standards, carry the force of law in the United States, based on their approval by the Federal Energy Regulatory Commission (FERC), and in Canada, based on provincial authorities. In addition, many countries in Latin America are adopting the NERC CIP standards on a voluntary basis, with possible future government mandates.
These standards impose a wide range of technical and procedural requirements on industry asset owners (commonly known as Registered Entities). To meet the requirements, Registered Entities typically deploy a variety of technical security controls that directly address the requirements, or indirectly support compliance with the requirements. Also, some requirements may be imposed on security technology used within NERC CIP regulated environments.

This paper describes how Claroty's fully integrated platform supports entities' compliance efforts while helping to improve the cybersecurity and operational reliability of power generation and transmission systems. We will map NERC CIP requirements to specific functionality provided by Claroty's solutions and provide answers to the most common questions asked by utilities regarding NERC CIP compatibility.

WHY READ THIS PAPER?

- Understand how the Claroty Platform can help meet NERC CIP requirements
- Obtain answers to key questions needed to ensure compatibility with the CIP standards

SUPPORTING CIP COMPLIANCE

Electronic Security Perimeters

NERC standard CIP-005 specifies requirements for Electronic Security Perimeters (ESPs), secure networks containing Cyber Assets that are in-scope for CIP requirements. Claroty's platform assists with the design and verification of these networks by identifying and mapping all assets communicating on control networks (Field Bus / Serial & IP Networks). This information is used to construct network diagrams identifying all external routable communication paths and access points.

This standard also requires monitoring of inbound and outbound access to the ESPs for the purpose of detecting malicious activity. Claroty is well-suited to meet this requirement via its unique combination of signatures, purpose-built OT behavioral models, and proprietary anomaly detection capabilities. This can immediately detect and provide actionable information on malicious activities. Most importantly, CTD can identify potentially malicious communications within OT protocols that may not be understood by traditional security tools, filling a potential gap in compliance.

Interactive Remote Access

CIP-005 R2 requires entities to implement secure remote access mechanism that meet strict requirements. Claroty Secure Remote Access (SRA) system meets these requirements and provides a robust method to allow secure access to protected assets when needed.

This system meets all three core requirements of CIP-005 R2:

- SRA prevents a device that initiates a connection from directly accessing a protected asset. Remote access is securely proxied through SRA, ensuring that only the authorized user on the originating device has access.
- SRA provides encryption between originating devices and the remote access server. Access to SRA is provided via HTTPS, an industry standard protocol for secure web access.
- SRA supports 2-factor authentication. User accounts can be configured to require a one-time password (OTP) in addition to the required user password. SRA supports Google Authenticator and similar OTP systems.

SRA also supports the new requirements enacted in the supply chain standards. CIP-005 R2, Parts 2.4 and 2.5 require entities to have the ability to identify active vendor remote access sessions and be able to terminate those sessions if needed. SRA provides active monitoring of all sessions and the ability to disconnect any session at any time.

System Security Management

CIP-007 establishes several requirements related to system management. The Claroty Platform can assist with many of these.

Port and Services
CIP-007 R1 requires entities to disable unnecessary "logical network accessible ports". CTD monitors network communications and identifies ports on which devices are communicating. This can be used to identify necessary ports for this requirement, or as an additional control to identify misconfigured devices or potential security incidents.

Patch Management
CIP-007 R2 establishes requirements for the management of security-related patches. CTD can assist with this process by identifying specific hardware and firmware versions for devices on networks it monitors. This can provide an inventory that can be used to establish and track patch sources. This inventory can also be used when evaluating

specific patches for applicability to determine which specific devices may require the patch. Additionally, Claroty automatically generates a comparison between the patch policy set by the organization and the actual list of installed patches on hosts, thereby identifying and reporting the list of missing patches per host. This acts as an additional control to ensure patches are installed.

Malicious Code Prevention
CIP-007 R3 requires entities to implement controls that deter, detect, or prevent malicious code on their in-scope systems. For devices that do not have commercially available anti-malware software available, the standard allows for network-based detection. CTD is a perfect solution for these situations.

CTD's security fabric can monitor all network traffic within a protected network. With its advanced deep packet inspection (DPI) capabilities, built specifically for ICS networks and protocols, and its advanced machinelearning algorithms, CTD automatically whitelists legitimate baseline activities and alerts on any changes or anomalies. These features provide a robust capability to detect malware activity occurring on the network.

Password Guessing Attacks
CIP-007 R5 requires entities to limit the number of unsuccessful login attempts allowed. The standard permits alerting to be used to meet this requirement. CTD's monitoring process can detect unsuccessful login attempts passively throughout the ICS network.

Security Event Monitoring

CIP-007 R4 requires entities to log system events related to cyber security. Many ICS devices have limited logging capabilities, but this can be address through CTD's ability to identify security-related events through its inspection of ICS network traffic. If a Cyber Asset is not capable of logging an event type, CTD may be able to identify the event through its deep packet inspection capability. This includes Cyber Asset communication connections, user login/logouts, baseline network configuration, firmware changes, types of commands and registers used, and the values of the responses.

Events identified by CTD for monitored assets can be reviewed as needed via management reports. CTD can also be configured to capture and store network traffic to support after-the-fact investigations of security incidents. CTD provides real-time, actionable alerts on known and unknown threats, suspicious activity, failure of event logging, and changes that pose a risk, so organizations can protect their resources against threats on the OT network.

Using DPI, CTD can detect unsuccessful login attempts passively throughout the ICS network. By using WMI, SNMP, and log collection, CTD is able to detect unsuccessful login attempts that occur locally to the asset. CTD provides alerting when the number of defined consecutive invalid access attempts is exceeded. This is an effective additional control for many devices and may be the only control available for some OT devices.

Configuration Change Management and Monitoring

CIP-010 R1 requires entities to document baseline configurations for in-scope assets. This includes operating system or firmware, installed software and patches, and open ports. CTD can identify and document these baseline configurations for devices using both passive monitoring and active detection.

CTD documents the configuration baseline of assets on the ICS network. Historical data is stored for each individual asset, allowing organizations to review and report on changes that deviate from the authorized baseline. Reports can be executed on the assets to verify accepted changes. These reports can be routed to designated approval authorities and the documentation then placed in the organization's change control database. These functions support answers to auditor evidence requests during NERC CIP audits.

CIP-010 R2 requires monitoring of baseline configurations and investigation of any detected, unauthorized changes, CTD provides alerts when it detects that an asset has deviated from its documented, approved baseline. If unauthorized components are connected to the ICS Network or unauthorized communications take place on the ICS network, CTD creates alerts for designated officials.

Incident Response

CIP-008 requires entities to develop Cyber Security Incident Response Plans that include processes for the identification of and response to security incidents. CTD assists with the identification of potential Cyber Security Incidents via its many capabilities for monitoring, analyzing, and reporting on network communications and system activity, including the generation of alerts for suspicious, unauthorized, or known malicious activity.

Response to incidents is supported by the ability of CTD to quickly and easily report on communications and actions taken within systems it monitors, providing tremendous insights to investigators. CTD can export information for use in investigations and integrates with other tools, such as SIEMs, to support investigations. CTD can also support active response via integration with firewalls or Network Admission Control (NAC) technology.

Vulnerability Assessments

CIP-010 R3 requires entities to perform vulnerability assessments. Through passive and active monitoring and detection techniques, CTD obtains detailed knowledge of the configuration of networks, the devices on those networks, and the communications between those devices. This provides a rich set of information from which to conduct vulnerability assessments.

CTD has several capabilities to support vulnerability assessments:

- CTD's built-in Attack Vector Simulation identifies the highest risk attack vectors based on analysis of devices and vulnerabilities.
- CTD generates numerous "insights" from its analysis of network traffic. These are prioritized and made available via a number of standard reports. These insights identify potential vulnerabilities or weak spots in system design or defenses such as unpatched vulnerabilities, insecure protocols, and external communications.
- CTD can also generate a summarized Risk Assessment Report which provides a quick and easy overview of system security.
- With deep insights into the ICS environment, CTD enables users to proactively identify and fix configuration and other network hygiene issues that can leave your network vulnerable to attacks. Leveraging proprietary intelligence, the system continuously monitors the network for new known vulnerabilities – providing precise CVE matching down to the firmware versions for industrial devices.

Using precise asset inventory and sanitized CVE database, CTD is the only solution that presents "actual" conclusive vulnerabilities. Other solutions either fail to collect the full asset context (e.g. model and firmware) or fail to thoroughly sanitize their CVE databases. This in turn increases alert fatigue and results in precious time and money spent chasing false alarms.

NERC CIP COMPATIBILITY

Although the NERC CIP standards are designed to protect devices used directly in the real-time operation of the Bulk Electric System, certain other devices deployed in such an environment can be in-scope for some requirements. For example, devices used for electronic access control or monitoring, remote access, or simply installed onto a protected network that contains other in-scope devices.

All of Claroty's solutions are designed to be compatible with the NERC CIP standards. This means that capabilities exist that allow entities to easily comply with the requirements, and that Claroty provides the information that entities need to document and apply these capabilities. The following sections outline these areas.

Port and Services

CTD makes compliance with CIP-007 R1 easy. By default, CTD requires only port 22 (SSH) and port 443 (HTTPS) to be open and accessible via the network.

Security Patch Management

As a fully supported, turnkey system, CTD simplifies compliance with the patch management requirements of CIP-007 R2. Claroty provides all necessary patches, including security patches, for its software and the underlying operating system platform. These cover system functionality and operating system security. Patches for Red Hat Linux or CentOS are tested by Claroty in-house prior to release to customers. Updates are provided in standard Redhat Package Manager (RPM) format, providing ease of installation, tracking, and security.

Malicious Code Prevention

CTD easily supports compliance with CIP-007 R3 malicious code prevention requirements. As permitted by the standard, malicious code risks are addressed via security hardening of the CTD platform. Claroty has documented a full hardening procedure as part of the system deployment process (see attached hardening procedure guidelines for additional information). Additionally, Claroty encrypts and signs all software updates and new software versions prior to being sent to customers. This provides strong security and supports the new supply chain requirements in CIP-010 R1, Part 1.6, effective July 1, 2020.

Security Event Monitoring

Claroty's platform provides strong logging features[1] and compatibility with modern Security Information and Event Management (SIEM) systems, making it easy to meet the requirements of CIP-007 R4.

Claroty provides broad and robust logging capabilities, including support for the ubiquitous syslog protocol, allowing easy integration with enterprise SIEM deployments. Claroty, as a primary function, can generate numerous security relevant log events and alerts that exceed the requirements of the CIP standards and fully support the underlying objective of detecting cybersecurity incidents. Claroty's log message format is well-documented[2].

Claroty has robust alerting capabilities. Alerts can be generated for a wide range of security relevant events detected are monitored networks. These alerts can be sent directly via email or can be forwarded to a SIEM for centralized alerting and response. Claroty can alert when a monitoring interface goes down, supporting the requirement to alert on loss of logging under CIP-007 R4.2.2.

Claroty is capable of retaining logs for the required 90 day interval. By default, Claroty compresses and encrypts all local log files and retains them for a minimum 5-year time period. Additionally, since all logs can be sent to a SIEM, log retention can be centrally maintained for easy compliance.

Log review requirements can be met in two ways. By taking advantage of Claroty's SIEM integration, log review can be performed on a single pane of glass by an entity's analyst team. Additionally, Claroty can generate reports itself that highlight specific events relevant to

the operational environment. This allows operational technology staff to easily review security events, providing an appropriate level of expertise for this critical task.

Account Management

Claroty's platform is well positioned to meet the requirements of CIP-007 R5, which contains several account management and password related items:

- **User Authentication**[3] – Claroty contains a built-in capability to authenticate users against an internal user database. Claroty is also capable of integrating with Microsoft Active Directory[4] to support centralized administration of user accounts, user authentication, and authorization permissions.

- **Default Accounts** – Claroty's platform has four default accounts. A built-in administrator account[5] (admin) exists. During the initial setup phase, Claroty will prompt and allow this account to be renamed and a new password to be set. Claroty's database and web front end have three built-in accounts[6], a root database account, a system database account, and a web front end account. Claroty allows an administrator to easily change the passwords for these accounts during system setup.

- **Password Controls**[7] – Claroty's platform enables strong password controls. For deployments that leverage Active Directory, password controls are automatically provided based on the entities' configuration. For builtin accounts within the Claroty system, strong controls are supported. Administrators are able to set a password expiration (in days) to ensure passwords are changed at regular intervals. Administrators can also expire all passwords with the push of a single button, requiring all passwords in the system to be changed. CTD leverages the Linux Pluggable Authentication Modules (PAM) system to enforce password requirements. The CTD hardening guide includes steps to require CIP compliant password length, complexity, and change intervals.

- **Account Lockouts**[8] – Claroty's platform supports controls to deter password guessing attacks. For deployments that leverage Active Directory, account lockout settings are automatically provided based on the entities' configuration. Additionally, Active Directory logging can support alerting for multiple failed login attempts. For built-in accounts within the Claroty system, administrators can configure accounts to lock after a configurable number of failed logins using Linux PAM settings[9]. Failed login attempts are logged, supporting the alternative alerting approach to this requirement.

Backup and Recovery

CIP-009 requires entities to develop recovery plans for all systems in-scope for NERC CIP. The Claroty Platform easily supports these plans with a preconfigured backup and restore scripts[10] that make recovery a snap. All information needed to restore an installed instance is easily saved to a single file which can then be archived to an entity preferred backup media. Restoration is a one-step process. Simply run the provided restoration script against the previously backed up file and the system is restored. Additionally, Claroty supports virtualized environments[11], making recovery even easier.

Change Management

CTD's software installation leverages the Linux RPM system, the standard for ease, security, and manageability of software on Linux systems. Claroty provides all required packages and runs on a hardened, minimized Redhat or CentOS platform making change management a snap.

CONCLUSION

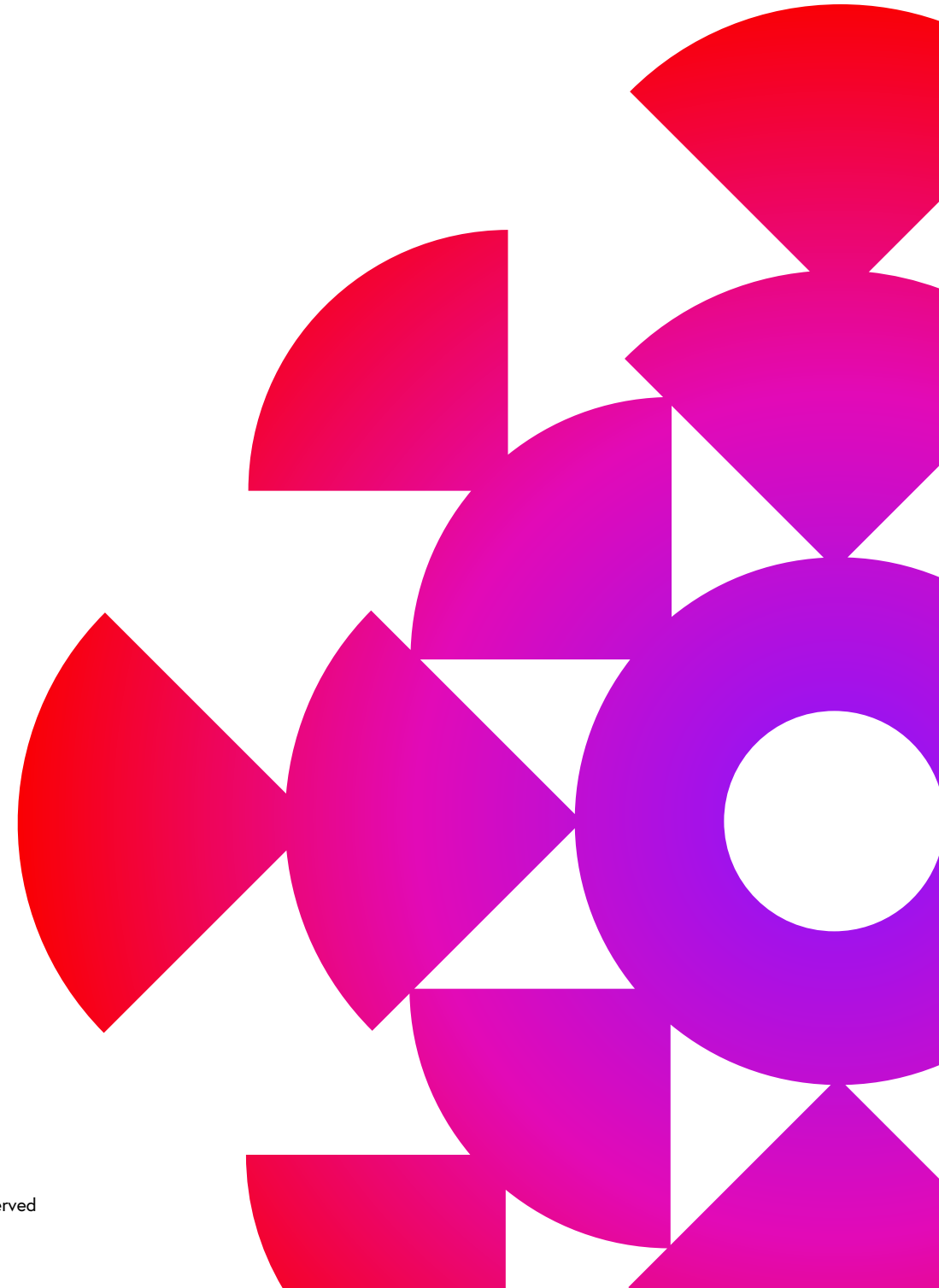
Many electric utilities are seeking to strengthen cybersecurity in their ICS environments, which are susceptible to today's sophisticated attacks. Many of these environments are subject to the mandatory NERC CIP standards, making it critical that deployed solutions are compatible with and support compliance with the CIP requirements. An important part of this effort is the implementation of innovative solutions that improve cyber resiliency without creating compliance risks. When considering a solution, seek one that provides both strong security features and full support for regulatory mandates.

About Claroty

Claroty is the industrial cybersecurity company. Trusted by the world's largest enterprises, Claroty helps customers reveal, protect, and manage their OT, IoT, and IIoT assets. The company's comprehensive platform connects seamlessly with customers' existing infrastructure and programs while providing a full range of industrial cybersecurity controls for visibility, threat detection, risk and vulnerability management, and secure remote access—all with a significantly reduced total cost of ownership. Claroty is backed and adopted by leading industrial automation vendors, with an expansive partner ecosystem and award-winning research team. The company is headquartered in New York City and has a presence in Europe, Asia- Pacific, and Latin America, and deployments on all seven continents.

To learn more, visit www.claroty.com.

1 CTD Admin Guide section 12
2 CTD Admin Guide section 12.2
3 CTD Admin Guide section 5.3.2
4 CTD Admin Guide section 5.3.2.3
5 CTD Admin Guide section 5.2.2.2
6 CTD Admin Guide section 5.2.3.4
7 CTD Admin Guide section 5.3.2.5
8 CTD Admin Guide section 5.3.2.5
9 CTD Admin Guide section 5.3.2.5
10 CTD Admin Guide section 3.4
11 CTD Admin Guide section 3.3



CLAROTY