

NERC CIP Compliance

Introduction

LogRhythm’s NERC CIP Compliance Package provides out-of-the box assistance in addressing numerous NERC CIP requirements. As part of the NERC CIP Compliance Package, the enterprise assets are categorized according to NERC CIP-002-1 Critical Cyber Asset Identification standards: Electronic Security Perimeter, Incident Reporting and Planning, Critical Cyber Assets, Malware Systems, Vulnerability Detection, Disposal Logs, and Patch Compliance.

The collection, management, and analysis of log data are integral to meeting many NERC CIP requirements. IT environments consist of heterogeneous devices, systems, and applications all reporting log data. Millions of individual log entries can be generated daily if not hourly. The task of assembling this information can be overwhelming in itself. The additional requirements of analyzing and reporting on log data render manual processes or home-grown remedies ineffective and cost-prohibitive.

A fundamental component of an effective NERC CIP strategy is an automated Log Management and SIEM platform providing enterprise-class capabilities for security, operations and compliance requirements.

Requirements

The North American Electric Reliability Corporation (NERC) is a nonprofit corporation designed to “ensure that the bulk electric system in North America is reliable, adequate and secure.” As the federally designated Electric Reliability Organization (ERO) in North America, NERC maintains comprehensive reliability standards that define requirements for planning and operating the collective bulk power system. Among these are the Critical Infrastructure Protection (CIP) Cyber Security Standards, which are intended to ensure the protection of the Critical Cyber Assets that control or affect the reliability of North America’s bulk electric systems.

In 2006, the Federal Energy Regulatory Commission (FERC) approved the Security and Reliability Standards proposed by NERC, making the CIP Cyber Security Standards mandatory and enforceable across all users, owners and operators of the bulk-power system. After going into effect in June 2006, initial compliance auditing began in June 2007.

Solution Summary

LogRhythm has extensive experience in helping organizations improve their overall security and compliance posture while reducing costs. Log collection, archive, and recovery are fully automated across the entire IT infrastructure. LogRhythm automatically performs the first level of log analysis. Log data is categorized, identified, and normalized for easy analysis and reporting. LogRhythm’s powerful alerting capability automatically identifies the most critical issues and notifies relevant personnel.

Automated Compliance Support for NERC CIP

- **Demonstrate Compliance**
Ensures that Critical Cyber Assets operate within the requirements of applicable policies, legislation and regulations.
- **Enhanced Risk Management**
Provides an essential contribution to the mitigation of risks to the confidentiality, integrity and availability of information assets processed by Critical Cyber Assets.
- **Reporting and Continuous Improvement**
Contributes to mandatory reporting and process requirements of NERC CIP.
- **Situational Awareness**
Provides a real-time feed of information regarding the current status and threats to Critical Cyber Assets, ensuring incidents are detected, investigated and effectively remediated.
- **Enables Accountability**
Ensures that Critical Cyber Assets are used within the parameters defined and not used for wasteful or unlawful purposes.
- **Complements Network Defense**
Enhances other security countermeasures, providing a complete “defense in depth” approach and facilitating automated responses to threats to Critical Cyber Assets.



NERC CIP Reporting Package

The table below shows how LogRhythm and its NERC CIP Compliance Package address the nine sections of the standard and additional benefits gained.

NERC CIP Requirement		Solution	LogRhythm Offering
CIP-001-1a:	Sabotage Reporting	Identifies attacks in real-time by monitoring, classifying and alarming on events, supporting the reporting process of CIP-001a in requirements 2 and 3.	Maintains a digital chain-of-custody, ensuring that log evidence and supporting reports are validated as unaltered.
CIP-002-3:	Cyber Security - Critical Cyber Asset Identification	Provides support for identifying systems and their roles that might not have otherwise been accounted for, especially covering requirements 2 and 3 that provide support for critical assets.	Intelligently identifies critical assets with geolocal awareness and risk and threat level properties, with a 100-point Risk Based Prioritization to help identify when critical assets are at risk of attack.
CIP-003-3:	Cyber Security - Security Management Controls	Supporting tool for Security Management decision making. The assigned Compliance Monitor will be able to validate controls using LogRhythm.	Provides executive-level reporting to help management with operations, security and compliance-related decision making.
CIP-004-3:	Personnel & Training	Augments personnel training by providing additional "eyes" on organization activities. 24x7 monitoring provided by LogRhythm covers areas of awareness that personnel normally cannot.	Automated reports and easy-to-create saved investigations provide managers with a simple and effective way of tracking employee activity.
CIP-005-3:	Cyber Security - Electronic Security Perimeter(s)	Directly supports monitoring of the ESP and Critical Cyber Assets, and other security and organizational access controls. Identifying configuration changes on ESP devices augments strict security configuration requirements, while correlating detected vulnerabilities with other data enhances Cyber Vulnerability Assessments and protection.	Works with all security devices, enhancing ESP protection by providing a centralized view within a single console. All information is available via automated reports, simple-yet-powerful investigations and real-time automated alerts.
CIP-006-3:	Cyber Security - Physical Security of Critical Cyber Assets	Augments existing physical access controls by monitoring logs generated by electronic access systems.	Correlates physical and digital access logs with network activity and user information for comprehensive security auditing and enforcement. For example, a badge reader alerting on an attempted entry by a user only authorized to access another location.
CIP-007-3:	Cyber Security - Systems Security Management	Provides oversight for almost all requirements of the Systems Security Management standard, directly meeting many of the challenges of implementing an effective NERC CIP compliant solution.	Correlates log and event data across all devices, enhancing Systems Security Management and providing a centralized, comprehensive view of an organization's security posture.
CIP-008-3:	Cyber Security - Incident Reporting and Response Planning	Provides a centralized system for collecting, reporting and alarming on critical events from network and host security systems. Centralization of incident response management and reporting is a key component for an effective IRR plan.	Incident Response Management tool can automatically track and report on the status of alarms. Reports track detailed information about response trends and resolution history for more effective planning.
CIP-009-3:	Cyber Security - Recovery Plans for Critical Cyber Assets	Provides early warning system failures that can improve response time and diagnostic abilities, reduce downtime and alarm on failures to augment disaster recovery.	Offers flexible High Availability Solutions for meeting business continuity, information assurance and disaster recovery requirements.

LogRhythm Headquarters

3195 Sterling Circle
Boulder, CO 80301
303-413-8745

LogRhythm EMEA

Siena Court, The Broadway
Maidenhead Berkshire SL6 1NJ
United Kingdom
+44 (0) 1628 509 070

LogRhythm Asia Pacific Ltd.

8/F Exchange Square II
8 Connaught Place, Central
Hong Kong
+852 2297 2812