

CorreLog for NERC

NERC, the North American Electric Reliability Corporation, is tasked with ensuring the reliability and safety of the bulk power system in North America. As of 2010, NERC regulations regarding Cyber Security are enforceable, including possible fines of up to \$1 million each day!

NERC is a non-government organization, which has statutory responsibility to regulate bulk power system users, owners, and operators through the adoption and enforcement of various standards, including comprehensive Cyber Security guidelines and regulations.

In 2008, The U.S. Federal Energy Regulatory Commission (FERC) granted NERC the legal authority to enforce standards for users, owners, and operators of U.S bulk power systems. FERC has made compliance with those standards mandatory and enforceable by June of 2010.

Bulk power providers have a strong tradition of hardware safety and reliability. With information broadly held and transmitted electronically, the NERC security standards furnish clear rules for the protection of the electrical grid, and all participants.

Q: What are the NERC controls for Cyber Security?

A: NERC establishes a variety of regulator requirements and specifications, and enforces these standards in its capacity as a non-government organization under a grant of the U.S. Federal Energy Regulatory Commission (FERC). The particular requirements for computer security are similar to those found in other standards, such as FISMA and others. By 2010, bulk power providers must employ asset and security management, secure perimeters, and incident reporting for their network assets. These specifications are embodied in a series of regulations numbered CIP-003 through CIP-009. Cardholder data is any personally identifiable data associated with a cardholder. This could be an account number, expiration date, name, address, social security number, etc. All personally identifiable information associated with the cardholder that is stored, processed, or transmitted is also considered cardholder data.

Critical Infrastructure Protection (CIP) Standards

NERC Standards CIP-002 through CIP-009 provides a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.

Ship's Log: True Tales of NERC

CIP-002 Critical Cyber Asset Identification

Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System.

CIP-003 Security Management Controls

Standard CIP-003 requires that Responsible Entities have minimum-security management controls in place to protect Critical Cyber Assets, including the ability to track user access, determine security status, monitor policy changes, and other controls.

CIP-004 Personnel & Training

Standard CIP-004 requires that personnel having authorized cyber access to Critical Cyber Assets have personnel risk assessment, training, and security awareness.

CIP-005 Electronic Security Perimeter(s)

Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. These requirements cover firewalls, VPN access, and other access points.

CIP-006 Physical Security of Critical Cyber Assets

Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets.

CIP-007 Systems Security Management

Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s).

CIP-008 Incident Reporting and Response Planning

Standard CIP-008 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets.

CIP-009 Recovery Plans for Critical Cyber Assets

Standard CIP-009 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices.

CorreLog Support For NERC Standards

CorreLog Security Correlation Server provides specific elements needed to support the NERC CIP requirements in a highly cost-effective and secure manner, using standards based protocols, extensible architecture, and simplicity of operation to insure long life cycles and high rates of returns without sacrificing functionality.

Configuration Assessment.

With configuration assessment, CorreLog Enterprise can proactively test and assess a server environment against pre-configured, out-of-the-box policies, helping to enable a minimal deployment window. CorreLog leverages industry standards and benchmarks formulated for the Center for Internet Security (CIS), the National Institute of Standards and Technology (NIST).

Change Detection and Reporting.

CorreLog monitors file integrity and file structures on information systems, including hardware, software, network, and security infrastructure. It then provides detailed change audit information to enable agency staff to quickly pinpoint, analyze, and recover from any undesirable change. CorreLog delivers assurance that authorized changes are completed. With a verifiable audit trail, staff can then document every step to auditors or assessors and provide them with detailed reports that demonstrate changes made to information systems.

Automated Security Compliance.

By combining change detection and reporting with configuration assessment, CorreLog assesses every change as authorized, within policy and compliant, ensuring systems achieve a known and trusted state. CorreLog then helps maintain that known and trusted state by establishing a secure baseline to measure change against.

Secure Perimeter Policy Enforcement.

Monitor and control transfer of federal agency data from all desktops and laptops regardless of where users and data go, and even when users are not connected to the corporate network. Control the transfer of corporate data to removable media. Regulate how users copy federal agency data to removable USB drives, CDs, DVDs and other external storage devices. Direct whether and how users may access, print, and send federal agency data over the network. Ensure that data only goes to authorized recipients such as contractors or government agencies.

User Training, Monitoring, and Education.

Improve user awareness and reinforce appropriate behavior with custom and automatic notifications, which help maintain the information security policy that NERC requires. CorreLog is specifically designed to leverage the existing paradigms and ways of doing things found throughout industry, without undue burden on security personnel. Ease of usage and ergonomic design minimize training. Passive monitoring eliminates specific requirements of users except to obey established security practices. The result is fast deployment, intuitive design features, allowing users to refocus on the actual security processes rather than the tools.

Security Policy Maintenance and Test.

An organization cannot claim to have a comprehensive information security policy without monitoring the security message being constantly logged on platforms within your enterprise. An enterprise that installs CorreLog, with no other action, takes a major step forward in creating and maintaining an enterprise security policy. CorreLog interfaces easily with common, security-test software, including port scanners, to verify that CorreLog is successfully monitoring system security. CorreLog has a self-test associated with AES encryption that permits users to verify that CorreLog encryption is working.

Incident Reporting and Workflow Management.

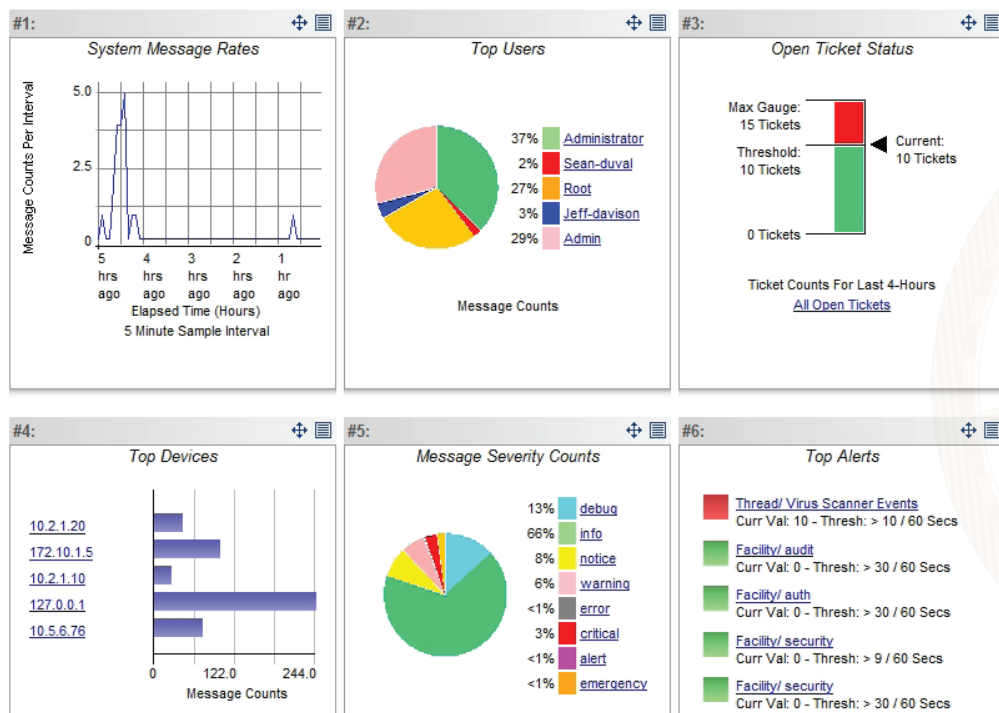
Incident management is the highest level of correlation for any organization. CorreLog incorporates a flexible ticketing interface that tracks problems and provides searchable resolutions. As part of this process, CorreLog creates actionable data based upon pre-defined or user specified conditions, ensuring the identification, classification, proper response, and reporting of Cyber Security Incidents. The CorreLog “Ticket” interface works with all popular third-party incident management systems, including an interface to BMC Remedy, and to Heat. Automatic incidents contain a detailed record of the particular messages and parameters that caused the ticket to be opened. The result is more thorough tracking of incidents, and more effective workflow for security personnel.

Failover, Recovery, and Redundancy.

CorreLog provides a distributed, highly hardened environment that includes continuous check pointing of data, automatic external backups, buffering of data and retransmission during network failures. The program is designed for mission critical environments, where message loss is not an option. Using CorreLog, you can easily configure multiple failover strategies that prevent loss of data and provide quick disaster recovery.

CorreLog NERC Highlights:

- Monitor security and diverse performance metrics for all network and perimeter assets.
- Manage all devices, including meters, servers, collectors, routers, firewalls, and infrastructure
- Follow the Federal Information Processing Standard (FIPS). CorreLog includes full AES-256 encryption and TLS internal security.
- Easy to deploy, scale and adapt. CorreLog reduces NERC security training compliancy costs



Sample of CorreLog Custom NERC Dashboard Reporting

Navigate Your Way to NERC Compliance Today

CorreLog, Inc. delivers security information and event management (SIEM) combined with deep correlation functions. CorreLog's flagship product, the CorreLog Security Correlation Server, combines log management, auto-learning functions, neural network technology, proprietary semantic correlation techniques and highly interoperable ticketing and reporting functions into a unique security solution.

CorreLog furnishes an essential viewpoint on the activity of users, devices, and applications to proactively meet regulatory requirements, and provide verifiable information security. CorreLog provides auditing and forensic capabilities for organizations concerned with meeting requirements set forth by NERC and others.

To learn more about how CorreLog can help, contact CorreLog toll-free in the US at 877-CorreLog or 239-514-3331 or visit www.correlog.com.

Installation Requirements

The CorreLog Security Server system requires Windows Vista, XP, 2003, or 2000 workstation or server platforms. There are no hard limits on CPU, disk space, or memory resources. The CorreLog Security Server download package incorporates the Apache HTTP server, easy, Windows-based installation dialog, a ready-to-run configuration, and an encompassing user manual. The system also includes a copy of the CorreLog Syslog Windows Tool Set and manual so users can easily add Syslog capability to an existing Windows platform, making the CorreLog Security Server full-enterprise capable.

Free, 30-Day Evaluation

Download CorreLog for Windows 200x, XP, and Vista systems. NOTE: the CorreLog server system is designed for easy installation. A typical installation does not require the host platform to be rebooted and can be performed in less than five minutes. Download a free evaluation at: www.correlog.com/download.html.

About CorreLog, Inc.

CorreLog, Inc. delivers security information and event management (SIEM) combined with deep correlation functions. CorreLog's flagship product, the CorreLog Security Correlation Server, combines log management, Syslog, Syslog-NG, SNMP, auto-learning functions, neural network technology, proprietary semantic correlation techniques and highly interoperable ticketing and reporting functions into a unique security solution. CorreLog furnishes an essential viewpoint on the activity of users, devices, and applications to proactively meet regulatory requirements, and provide verifiable information security. CorreLog automatically identifies and responds to network attacks, suspicious behavior and policy violations by collecting, indexing and correlating user activity and event data to pinpoint security threats, allowing organizations to respond quickly to compliance violations, policy breaches, cyber attacks and insider threats. CorreLog provides auditing and forensic capabilities for organizations concerned with meeting SIEM requirements set forth by PCI/DSS, HIPAA, SOX, FISMA, GLBA, NCUA, NERC and others. Maximize the efficiency of existing compliance tools through CorreLog's investigative prowess and detailed, automated compliance reporting. CorreLog markets its solutions directly and through partners. Visit www.correlog.com for more information.

1004 Collier Center Way, Suite 103 • Naples, Florida 34110 • 1-877-CorreLog • 239-514-3331 • info@correlog.com