GE
Digital Energy

CyberSentry™ SEM

Security Event Manager

GE's CyberSentry SEM Security Event Manager is an integrated cyber security management and monitoring software for protection, automation and control devices. CyberSentry SEM is specifically designed to help utilities and energy intensive industrial companies manage security risks.

Standing guard 24/7, CyberSentry SEM monitors for configuration changes and cyber security issues. CyberSentry SEM also monitors and reports cyber security issues of grid automation and communications devices and to help utilities prove their compliance to North American Electric Reliability Corporation (NERC) standards.

Key Benefits

- Manages cyber security in protective relaying and automation systems with a straightforward, yet powerful set of software tools designed specifically for power systems and grid automation experts.
- Simplifies security reporting for NERC CIP audits with easy-to-use templates and workflows that document all activity, to ensure a safe and secure system.
- Modernizes security logs from aging relays and other grid automation electronics, translating events into industry standard syslog format and interfacing to the latest cyber security systems to avoiding costly and premature upgrades.
- Shields against human errors during routine protection testing and maintenance, by raising alarms when changes to relay configurations occur, preventing costly outages.
- Alerts system owners to unwanted changes in devices that could occur as the result of an insider or external cyber attack.

Applications

- Transmission and generation utilities covered by NERC CIP cyber security compliance regulations
- Industrial power producers and users with mission critical cyber assets
- Independent power producers with digital relays, grid automation devices, switches and communications infrastructure
- Municipal and co-op utilities managing power systems of all sizes

Practical Interface

- Functional tabbed structure saves users time searching for options
- Simple annunciator-style security dashboard shows alarm states for prompt response from systems experts

Customizable Logging

- Syslog security event streaming for enterprise Security Information and Event Management (SIEM) integration
- Choice of activities to log for complete control

Intelligent Monitoring

- Multiple classes of security event notices to quickly distinguish type of risk
- Simple definition of approved operations
- Predefined security event detection for common security and compliance program requirements

Alarm Activation

- Email notification for quick action and containment
- Assignment of workflows for quick action to resolve issues
- Process tracking from open to close of incidents for NERC CIP audit requirements

Audit Reporting

- Generate reports based on event type, security parameter category and open/closed status
- Selectable inclusion of action detail and history for more complete reports

imagination at work

Overview

Power and control systems experts need reliable tools to provide notification of cyber security issues. CyberSentry SEM guards assets by tracking authorized activities and logging them to fulfill audit requirements. Using industry standard syslog technology, CyberSentry SEM also modernizes security logs from aging relays and other grid automation devices, to fit into the latest cyber security system, avoiding costly and premature upgrades.

NERC CIP Compliance

Clearly defined processes, that deal with any and all events indicating a cyber security breach, establish confidence that devices are secured. Official reports which detail actions taken, should provide evidence that efforts have been made to reduce, prevent and contain security events. CyberSentry SEM provides a simple and powerful solution for managing and documenting cyber security events and actions. It delivers a system for ensuring that key equipment connected to the power grid is being effectively monitored, which is fundamental in any critical infrastructure protection and security program.

User-Friendly Security Dashboard

Designed specifically for power systems and grid automation experts, CyberSentry SEM manages cyber security in protective relaying and automation systems with a straightforward, yet powerful set of software tools. View security information in a centralized dashboard, detailing threats and risks. Navigate through data with ease. Determine what's important before it becomes an issue.

Define Legitimate Operations Through ACPs

Authorized Configuration Profiles (ACPs) let users define "normal" operations and configuration changes, to monitored cyber assets, within approved variances. ACPs allow users to perform everyday functions as they require, without triggering nuisance alarms for expected operations. When CyberSentry SEM detects a change that is not allowed within an ACP, it alerts the responsible parties that there has been some irregular behavior in the system. Irregular behaviour can be a strong indicator of a cyber attack and should be examined and corrected as part of a cyber security risk mitigation program.

Secure Configuration Management

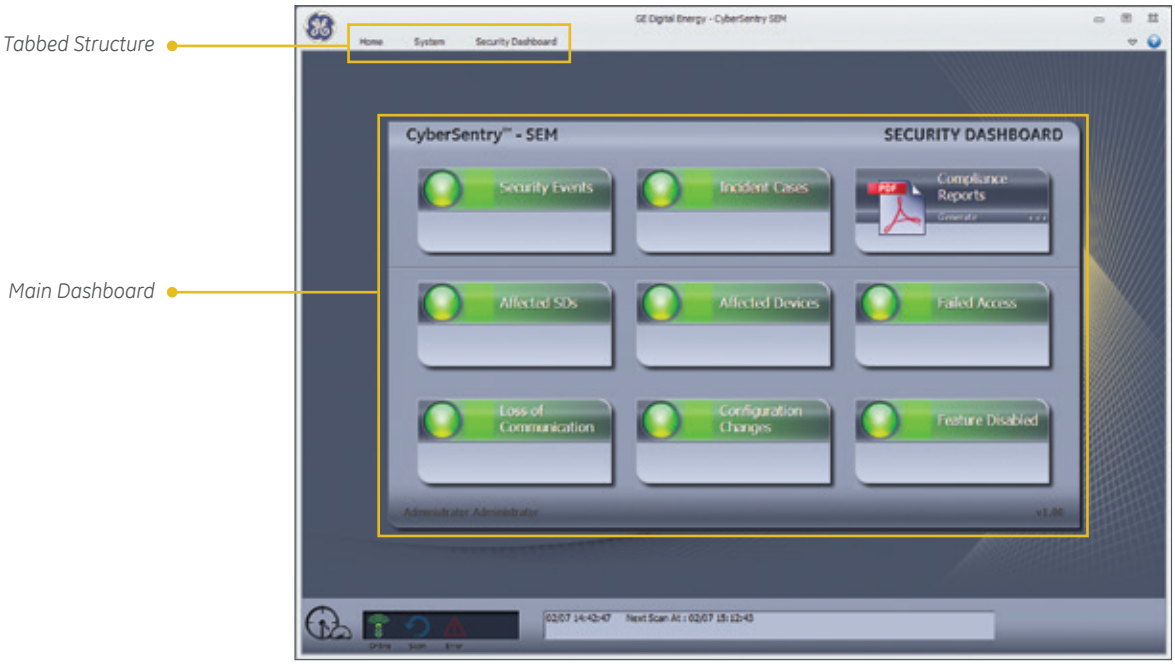
CyberSentry SEM is designed to monitor changes to device configurations. When changes are detected, a workflow and alarm can be triggered to ensure the correct steps are taken in change management. This virtual watchdog helps avoid false trips and other major power system impacts that could result from a simple mistake during necessary, but routine maintenance.

Simplified Reporting

Save time and effort with rapid security report generation and creation. These records are invaluable during security audits. CyberSentry SEM generates detailed reports related to possible threats identified by the software. These include failed logins and changes to settings related to communications or device functionality.

CyberSentry SEM Security Dashboard

The CyberSentry SEM security dashboard offers unparalleled convenience in a centralized, user-friendly environment. The tabbed structure along the top of the screen provides easy navigation to system setting options, while the main dashboard presents an uncomplicated view of system status.



Specialized Workflows and Documentation

Be ready for action when a problem occurs. Customizable workflows come pre-configured to ensure readiness for common cyber threats and audits.

The straightforward options available with CyberSentry SEM help identify processes that should be in place as well as common methods for addressing gaps. These workflows can be tailored to fit existing internal procedures or used straight out of the box.

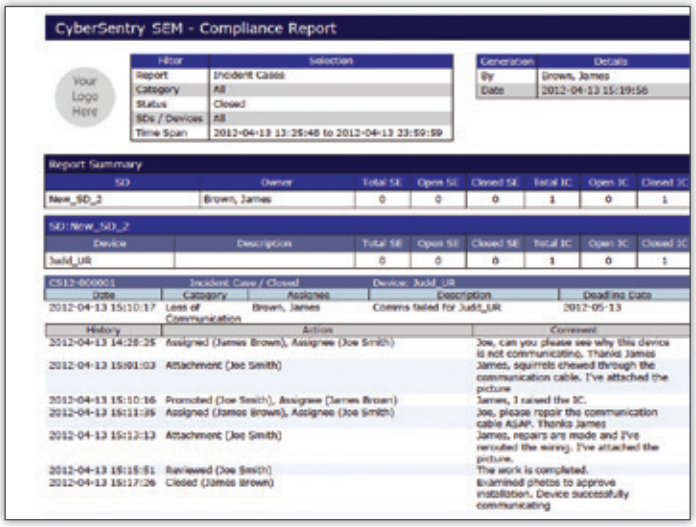
Enhanced Resolution Traceability

Prove actions have been taken and organizational commitment to security is in place through detailed records of action. Build an effective audit trail simply and effectively.

Comprehensive Security Documentation

CyberSentry SEM is a substation or control center level security solution to aid in simplifying NERC CIP cyber security compliance. It maintains a detailed history of changes to all configurations and creates audit-friendly workflows and records. Users can even customize the report with their own company logo.

The CyberSentry SEM security dashboard displays alarm notifications in a single view, enabling operators to take quick action.



This sample CyberSentry SEM report for a loss of communication event is an example of the documentation that users have, to prove they are tracking their system and know what is happening.

Technical Specifications

CyberSentry SEM Device Support

Supports enhanced integration with the following GE Multilin™ relays and networking devices:

- UR — firmware versions 5.4x to 6.0x
- UR^{Plus} — firmware versions 1.7x and 1.8x
- ML2400 — firmware version 4.01

Also supports the following third-party devices:

- Modbus devices
- Simple Network Management Protocol (SNMP) devices

Operating System

- Windows® 7 (32-bit) with the latest service pack and patches

Hardware Requirements

- 2.3 GHz (or better) Intel/AMD processor
- 4 GB RAM (minimum 2 GB)
- 1.0 GB free space on hard drive
- Minimum screen resolution SXGA
- CD/DVD drive
- Ethernet connection
- Keyboard and mouse

Ordering

CSEM	-	*	-	*	Description
		1			1 License
		5			5 Licenses
		10			10 Licenses
				025	25 Maximum Devices
				050	50 Maximum Devices
				100	100 Maximum Devices
				150	150 Maximum Devices

imagination at work

GEDigitalEnergy.com

GEA-12738A(E)
English
150211