

Power and Water Cybersecurity Suite – Security Incident & Event Management

Features

- Logs security collections from various sources and time horizons
- Aggregates and normalizes events
- Enables real-time analysis for security incidents through correlation
- Generates reports for compliance
- Configures views for detailed analysis
- Retains original logs for forensic analysis

Overview

Identifying a security incident in a distributed control system can be very challenging. A degraded control function could indicate the occurrence of a security incident. However, an intact control function does not guarantee system integrity. In most cases, security events may not be visible or dramatic. For example, repeated attempts to log into a control system by brute-forcing passwords presents no real harm to the system. However, repeated illegal login attempts using various methods could pose a significant threat that would require immediate recognition.

While an individual device may not have noticeable security events by itself, comparing multiple events from a collection of devices could reveal additional information on current or past security incidents. A powerful engine that correlates and analyzes events from multiple sources at different time horizons addresses this issue. The authenticity and integrity of archived security logs needs to be confirmed and maintained. Long-term storage of security logs



provides valuable information for forensic analysis or as evidence that an event has occurred, even if the information is required well after the event happened.

Solution

Security incident & event management is a Power and Water Cybersecurity Suite module that provides system-wide event management not inherently available in most control systems. The module operates at high throughput, with multiple concurrent sessions. A real-time user interface quickly returns queries and analytics in seconds, even on massive amounts of historical data.

Security incident & event management module collects security events from workstations running Microsoft® Windows® operating systems, as well as switches, firewalls and routers. The module also gathers events from other data sources via the simple network management protocol (SNMP) or system log messages (Syslog).

Security incident & event management normalizes data collected across numerous devices from multiple vendors into a single manageable module.

The aggregated data is correlated by a high-performance engine that manages thousands of events per second; providing an in-depth view into potential security incidents.

The module's embedded log management function along with an external network attached storage device collects and saves security logs for future forensic analysis or court evidence. The logs are digitally signed for integrity checks.

Two views are available for examining and analyzing specific events. Event views provide device event information and compliance views assist regulation compliance activities.

Reports can be created to show events in custom or predefined layouts and sent in PDF, HTML, or CSV format.

Alarm conditions can be configured such that real-time alarming occurs when defined conditions are met. In addition to alarming, other actions can be taken such as sending an email notification or creating a case for further investigation.

Operation

The security incident & event management module is accessible through the Power and Water Cybersecurity Suite's user interface browser and contains a dashboard with the following functions:

- **System navigation toolbar:** Access to general setup functions such as username, password, time zone and default system view
- **Icons:** Access to frequently used pages
- **Actions toolbar:** Selects functions to add, configure or view each device or system
- **System navigation pane:** Views, organizes and manages system devices
- **Alarms and cases pane:** Views alarm notifications and assigned open cases
- **Views pane:** Observes event, flow and log data
- **View toolbar:** Creates, edits and manages views
- **Filters pane:** Selects specific criteria for querying events of interest

Compliance Summary

NERC Standard	Requirement	Emerson Response
CIP-007-6 R4 Part 4.1	Log events at the bulk electric system (BES) cyber system level (per BES cyber system capability) or at the cyber asset level (per cyber asset capability)	Login records, successful or failed, are collected from the system domain controller and network devices
CIP-007-6 R4 Part 4.2	Generate alerts for security events As defined and determined by responsible entity	Alarm notifications can be sent to the SNMP server using the SNMP protocol or to a mail server
CIP-007-6 R4 Part 4.3	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP	Parsed logs are retained more than 90 days. Raw logs can be retained for years if security incident & event management is used in conjunction with network attached storage.
CIP-007-6 R5 Part 5.7	Generate alerts after a threshold of unsuccessful authentication attempts	Alerts on failed authentication attempts can be generated from the detection policy

©2017-2018 Emerson. All rights reserved. The Emerson logo is a trademark and service mark of Emerson Electric Co. Ovation™ is a mark of one of the Emerson Automation Solutions family of business units. All other marks are the property of their respective owners. The contents of this publication are presented for information purposes only, and while effort has been made to ensure their accuracy, they are not to be construed as warranties or guarantees, express or implied, regarding the products or services described herein or their use or applicability. All sales are governed by our terms and conditions, which are available on request. We reserve the right to modify or improve the designs or specifications of our products at any time without notice.