Power and Water Cybersecurity Suite – Configuration Management

Features

- Provides centralized management of control system configurations across workstations and network devices
- Monitors files and registry
- Runs commands for capturing additional data
- Real-time or manual change detection
- Assigns remediation work orders to individuals
- Generates schedules or manual reports

Overview

Configuration management is a system engineering process that establishes a baseline configuration and monitors that configuration for changes. Managing system configurations prevents unauthorized or undocumented changes that could introduce unnecessary risks to operating controls.

System configurations typically include network architectures, device functions and locations, hardware compositions, software contents and versions, as well as application programs. Original system configurations will undergo several changes throughout a regular lifecycle. Alterations can be made due to well-intended modifications, updated policies, physical rearrangements, application enhancements or content updates. Sometimes, system configuration changes can be made by an unauthorized user, malicious software or unintentional human error.

Detecting and documenting all changes through a paper trail presents great challenges where the accuracy, integrity and authenticity of these records are difficult to maintain. Malicious configuration changes are more difficult to detect and the consequences could be severe.

Proper control system configuration management establishes a baseline with all changes going through a defined proposal, approval, implementation and confirmation process. The system configuration is promptly updated after the change has been validated. Users are notified if an unauthorized change is detected.

Solution

Configuration management is a Power and Water Cybersecurity Suite module that enables effective management of control system configurations. The module supports multiple systems within a plant and focuses on Microsoft® Windows® based workstations, network devices and active directory.

A baseline is created when the system is in a known good state. The configuration management module monitors system nodes, such as workstations and network devices, and their elements such as file sizes and hash values against the baseline.

An agent is installed on each Windows-based workstation to monitor files and directories. If a change is detected, the agent reports the modification to the configuration management module through an audited event.

Network devices use rules instead of agents to detect configuration changes.

When the detected alteration is approved, a new element version is promoted which creates a new baseline. If the detected change is not approved, further actions can be taken, such as restoration or notification via email, simple network management protocol (SNMP) or system log (syslog).

Configuration management can also be used to test the compliance of corporate security policies for control systems.

The module can generate policy scores for measuring overall conformance. Failed policy tests can be remediated by using work orders.

Operation

The configuration management module includes a dashboard with the following functions:

- **Home:** Views system event alerts
- **Nodes:** Represents a monitored system, which is a file server, directory server or network device. Each node contains elements and element versions.
- **Rules:** Identifies one or more monitored objects
- **Actions:** Initiates a response to detected changes or failed policy tests. For example, if the module detects an unauthorized change, an action could send an email notification to appropriate personnel.
- **Tasks:** Runs a specific operation on a scheduled basis or in manual mode
- **Policies:** Measures the degree to which the configurations of monitored systems comply with a policy, such as an industry or corporate standard. A policy test determines if monitored systems comply with a specific policy requirement.
- **Log – Log Message:** A record of network or user created activity
- **Reports:** Compiles current monitored system data and provides information regarding the current state of a network. A dashboard is a user-defined collection of reports that may be run and viewed at the same time. By adding reports to a dashboard, you can review the latest output for all the reports in a single window.
- **Settings:** Consists of a variety of objects, system parameters and monitoring preferences

Compliance Summary

NERC Standard	Requirement	Emerson Response
CIP-010-2 R2 Part 2.1	Monitor at least once every 35 calendar days for changes to the baseline configuration. Document and investigate detected unauthorized changes	A baseline rule task can be created and run on a manual or scheduled basis on operating system, application or custom software