ConsoleWorks
Cybersecurity Operations Platform

NERC CIP-010

Configuration Monitoring

ConsoleWorks helps reduce or eliminate security gaps resulting from configuration changes.

1. Maintain asset configuration in a known state with the highest level of security.
2. Address key NERC CIP regulations pertaining to notification of asset configuration changes.
3. Eliminate security gaps resulting from assets that are not properly configured.

Configuration monitoring and management is a way to reduce or eliminate security gaps resulting from assets that are not properly configured. These gaps occur when asset configuration changes are not documented, when required changes (such as security patches) are not implemented, when configuration changes are made without approval, and when configuration change mandates are not implemented on one or more assets. ConsoleWorks configuration monitoring solution addresses key security requirements pertaining to notification of those configuration changes as described in NERC CIP-010. It can be configured to monitor many things including:

- Functional settings that determine how the asset operates
- Versions of software currently installed including BIOS, firmware, operating system, applications, etc.
- Patches, including security patches that are installed
- Ports that are active and how they are configured
- Services that are enabled
- Accounts that have been added or deleted
- Asset configuration files (routers, switches, PLCs, RTUs, etc.)

Minimize the impact of intentional or unintentional configuration changes.

Configuration Monitoring & Management – The overriding purpose of configuration monitoring and management is to maintain asset configurations at a known state that have the highest level of security. ConsoleWorks automates the collection, comparison, alert/notification and auditing of any changes to configurations, eliminating the majority of human errors and minimizing the impact of intentional or unintentional erroneous activity.

Automation of the Asset Configuration Retrieval – ConsoleWorks captures, documents and secures the configuration data programmatically.

Establishing a Specific Configuration as the Baseline – Once the asset configuration is captured, it can be defined as the master or baseline configuration and used as the standard for which all other like asset configurations are compared.

Automating the Comparison of the Current Asset Configuration to the Baseline – ConsoleWorks automates the comparison and determines where differences exist.

Automated Event Detection and Alerting of Unauthorized Changes – When a difference is detected, ConsoleWorks logs that a configuration check has occurred and differences were found. It subsequently Alerts the appropriate personnel of the differences.

Notification Sent to the Trouble Ticketing System – In addition to notifying appropriate personnel, ConsoleWorks can automate the generation of a trouble ticket to start the review or resolution process.

Manual Triggering or Scheduling of Configuration Checks – At any time a baseline check can be manually executed within ConsoleWorks.

Logging of Activity over the Entire Process for All Devices – ConsoleWorks understands who changed the asset configuration outside the approved process. Identifying the person that made a change provides the opportunity for training to ensure the process is followed in the future – or to take corrective actions if such is deemed necessary and appropriate.

Secure Logs for Compliance Reporting and Forensic History – Since all activity, down to the keystroke, is logged, proof of NERC CIP compliance is as simple as executing a report. The report not only includes the dates and times that the configuration checks were run, it also includes information on when differences were found and acknowledged.

History of Asset Configurations – ConsoleWorks maintains a history of configuration baselines. Configuration checks can be executed on any of the saved configurations.

Contact Us

TDi Technologies, Inc.
www.tditechnologies.com

- Agentless Monitoring
- Scalability
- Heterogeneous Deployment
- Security
- Log File Security
- Log Aggregation
- Audit & NERC CIP Compliance Reporting
- Session Management
- Command Control
- Intelligent Event Modules
- Event Management
- Automated Actions
- Event Remediation
- Log Forwarder
- Multiple User Management
- Logical & Hierarchical Grouping
- Multi-Connect

Integrated CIP Compliance ➤ Bridging IT and OT