ConsoleWorks
Cybersecurity Operations Platform

NERC CIP-005

Secure Interactive Access

Monitors, manages, logs, reports and secures access to managed assets in all machine states

1 All privileged user activity from users, 3rd-party vendors and contractors is logged as a forensic record of activity performed on assets.

2 Maintains a persistent connection to ensure nothing is missed. No buffers; no polling cycles.

3 Provides comprehensive security model with granular permissions for access control.

To effectively secure electronic assets (PLCs, RTUs, servers, switches, etc.), access must be controlled and all activity must be automatically logged to provide a forensic record of activity performed of users, 3rd party vendors, and contractors.

ConsoleWorks controls access by allocating specific permissions/ privileges to a user based on the role based permission model. The permission model specifies which assets a user, vendor, or contractor may access and at what level of privilege. ConsoleWorks supports command-by-command privilege grants for absolute control over electronic access.

The ConsoleWorks solution supports integration with Active Directory or LDAP server. The product was designed with the open ability to integrate its authorization/authentication services with multi-factor and other authentication technologies, as well.

ConsoleWorks is designed to minimize operational disruption and mean-time-to-repair.

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

- Secured Role-Based Account Control (RBAC) for asset-specific, task-based, user privileges
- Agentless, persistent monitoring ensuring no gaps in monitoring
- Capture complete recording and playback capabilities for user sessions, across RDP/VNC and even web applications.
- Scanning of incoming data streams for pre-defined text patterns such as failed login attempts
- Appropriate, customizable, log-on splash screen
- All log-ons, log-offs, and failed log-on attempts are captured, logged, and alerted
- All changes – down to the keystroke are captured, logged, and alerted
- Complete intelligence gathering, including source and account IDs, incident context, and commands executed and their results
- Centralized command and control for physical, logical and virtual console connections, Syslog messages, SNMP traps, and other streams of information

- Connections secured using SSL and SSH encryption
- All asset activity logs digitally secured for easy detection of modifications
- Color-coded logs from different information sources facilitating drill-down analyses in aggregated log views
- Events consolidated from all data sources using a common natural time, independent of asset vendor or type
- Sub-second timeframe for more insightful granularity
- Multiple users granted simultaneous remote access to a single asset
- Integrated incident recognition and response
- Complete event lifecycle management: Recognition, Notification, and Remediation
- Events prioritized by severity, set initially by OEMs and 100% customizable by users
- Real-time, customizable graphs and charts for NERC CIP audit reporting and business intelligence