ConsoleWorks
Cybersecurity Operations Platform

NERC CIP-007

Situational Awareness

Shorten Event resolution – minimizing operational disruption and downtime.

1. Immediate notification enables resources to be proactive by remediating the problem before it results in further, downstream issues.
2. View multiple log files, in context, to help in determining root cause and problem resolution.
3. Capture Event remediation down the keystroke building a client-specific best practice database.

ConsoleWorks acts in a multi-dimensional fashion by monitoring not only the applications but also the servers, virtual machines, network, PLCs, RTUs, and storage devices that run them. It provides managers and privileged users an end-to-end management solution that controls access, that monitors and manages all log files, RDP and VNC sessions, and watches for specific events that may occur across the organization. It does it in real-time and in all machine states – power on, single user, maintenance, production and failure modes. Its persistent connection also locks down the "back door" entrances that are overlooked by similar, agent-based solutions.

The end-to-end, situational awareness view, provided by ConsoleWorks, helps users understand WHY something went wrong and quickly determine and implement the resolution. During that process, ConsoleWorks captures the exact steps used by an experienced user to remediate an issue and stores it in the knowledge base for future reference and for audit purposes.

View multiple log files, in context for identifying root cause.

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

Secure Access Management – ConsoleWorks controls access by allocating specific permissions/ privileges to a user based on the ConsoleWorks role-based permission model. The permission model specifies which assets a user may access and at what level of privilege they may access those systems. ConsoleWorks supports command-by-command privilege grants for absolute control over electronic access.

The ConsoleWorks solution supports integration with an IAM solution and supports RBAC from an Active Directory server. The product was designed with the open ability to integrate its authorization/ authentication services with other technologies, as well.

GUI Capture and Monitoring – ConsoleWorks has the ability to capture complete recording and playback capabilities for privileged user sessions, across RDP/VNC and even web applications. Users gain a complete, detailed account of what happened on sensitive systems, and who performed a specific activity.

Event Monitoring – ConsoleWorks can monitor and manage almost any application or infrastructure interface – including routers, switches, servers, firewalls, virtual machines, PLCs, RTUs, appliances, applications and networks – to provide the most comprehensive record possible.

ConsoleWorks watches for messages, or Events, in the data streams of all the devices and applications it manages. When ConsoleWorks detects an Event, it alerts the appropriate personnel in real time, records the circumstances, and automatically performs the default or customer-configured response(s). Users are able to respond to the device or application error condition and immediately view the vendor-supplied explanation along with steps required to resolve the issue.

Log File Aggregation – ConsoleWorks monitors the asset logs in the context of all other managed applications or hardware. Its ability to aggregate error conditions across all log files enables users to view multiple log files, in context, to help in root cause analysis. In many cases, issues have been resolved before other solutions have been notified that an Event has occurred.

Keystroke Logging and Best Practices – ConsoleWorks captures the steps taken for Event remediation down to the keystroke, enabling any ConsoleWorks user to leverage in-house past experience and acquire proven solutions faster. In this way, ConsoleWorks builds the business's data warehouse of intellectual property related to the problem resolution.

Proof of Compliance – ConsoleWorks produces, aggregates and summarizes audit logs that record user activities, exceptions, and information security events. Log files are digitally secured for each asset, operating system, application, etc. as they are written allowing detection of line deletion, insertion or modification.