ConsoleWorks

Cybersecurity Operations Platform

THREAT ACTIVITIES - OBSERVED TACTICS, TECHNIQUES, AND PROCEDURES	CONSOLEWORKS STAUNCH DEFENSE TO SECURE OT/ICS ASSETS VIEW CONSOLEWORKS SCREENSHOT
Spearphishing to obtain initial access to the organization’s information technology (IT) network before pivoting to the OT network.	With ConsoleWorks, all communications to an OT network must come through ConsoleWorks. It provides the protocol break between the user accessing ConsoleWorks (HTTPS in this case) and assets which they want to access. Access to those assets utilizes their native interactive protocol (SSH, Telnet, RDP, etc.). The protocol break created by ConsoleWorks prevents viruses and malware from moving through ConsoleWorks, adding a disconnected layer of security via protocol changes.
Deployment of commodity ransomware to encrypt data for impact on both networks.	Because of ConsoleWorks' protocol break, Ransomware, viruses, malware will never make it through ConsoleWorks to the endpoints on the OT network. In order for it to encrypt data, it would require privileged credentials on the endpoint as well as a path there, both controlled and managed by ConsoleWorks.
Connecting to internet accessible PLCs requiring no authentication for initial access.	With ConsoleWorks, there are no internet accessible PLCs. Access to PLCs through ConsoleWorks requires the appropriate role and access control rules to be defined. ConsoleWorks handles the authentication through either local username / password combination or through standard Active Directory and multifactor authentication methods and technologies.
Utilizing commonly used ports and standard application layer protocols, to communicate with controllers and download modified control logic.	All interactive access is forced through ConsoleWorks eliminating the ability for actors to scan for open ports and services, much less actually connect to them. This minimizes the required open ports to the outside to only https and that can be on any defined port. Once ConsoleWorks collects the configuration and settings of managed assets and they are approved by the asset owner, it establishes a firm configuration (baseline). ConsoleWorks collects baselines on a user defined schedule and compares the current set of baseline information to the approved set and, if changed, sends notifications to the appropriate personnel that an unauthorized configuration change occurred and is opened for further investigation.
Use of vendor engineering software and program downloads.	Customers generally place vendor engineering software and program downloads behind ConsoleWorks creating a role-based access, audit and log of who can use the software. It also prevents the software from being infected on a remote workstation, eliminates the need to patch multiple workstations when updates come out and standardizes the version of Vendor software being used for each asset or set of assets. Use of those applications is based on a person's Role and associated access credentials. Access to ConsoleWorks by a bad actor would require multiple methods of authentication enforced by ConsoleWorks.
Modifying control logic and parameters on PLCs.	With ConsoleWorks in place, the likelihood of an outside, bad actor gaining access to a PLC is extremely low. In the event that someone did make a change to the control logic or parameters, ConsoleWorks Baseline capability would have already collected and logged configuration, settings and logic of each PLC. As such, it knows the correct control logic, settings, firmware, and configuration for each asset under management. ConsoleWorks will check the approved configuration settings against the current settings. If a difference is found it will alert and notify the appropriate personnel to investigate the changes that occurred. That device / PLC could then be restored to the authorized configuration as ConsoleWorks knows it and has record of it in its logs.

HAVE A RESILIENCE PLAN FOR OT	CONSOLEWORKS STAUNCH DEFENSE TO SECURE OT/ICS
Immediately disconnect systems from the internet that do not need internet connectivity for safe and reliable operations. Ensure that compensating controls are in place where connectivity cannot be removed.	ConsoleWorks removes the need for specific PLCs and the like to be accessible directly from the Internet. ConsoleWorks acts as the Electronic Access Control and Monitoring System (EACMS) where all human activity initiates through ConsoleWorks. With ConsoleWorks, there are no direct connections to any device. Every interactive access session initiated through ConsoleWorks and then ConsoleWorks makes the actual connection to the PLC based on the actor's role and access capabilities defined by the role. ConsoleWorks provides the compensating controls such as username / password and multi-factor authentication for the actor to access ConsoleWorks first (these are not the username / password of the asset). Then, ConsoleWorks uses credentials only it has securely stored for the asset to create an authenticated session to the asset. Then ConsoleWorks allows the actor access to the session ConsoleWorks created by brokering access to it, effectively becoming an authorized "Man-In-The-Middle". ConsoleWorks can be configured, for an added layer of security where the user does not need to know the username / password for the asset, allowing more complex password rules to be utilized and minimizing sharing of passwords.
Plan for continued manual process operations should the ICS become unavailable or need to be deactivated due to hostile takeover.	With ConsoleWorks installed at each facility (such as substation, plant, pumping station, etc.) even if the facility is disconnected from outside access, ConsoleWorks can remain the method by which local access is managed and controlled. ConsoleWorks will continue to log, audit and continue to operate as before. Just because someone is inside, access is treated as though they are outside. The same business and cyber security process is followed. Everyone is authenticated, audited and logged and no one is trusted.
Identify system and operational dependencies.	Because ConsoleWorks understands each asset in the network in order to control access and it has the ability to collect each asset's configuration information, it creates an automatic system of record for the network. User defined or system defined Meta data may also be applied to assets that would pair or identify an asset to a system or business process for the purpose of describing the operational dependencies across assets.
Restore OT devices and services in a timely manner. Assign roles and responsibilities for OT network and device restoration.	Since ConsoleWorks has the most recent and historical configuration for every device managed by ConsoleWorks, confidence that the restoration of devices to their approved configuration is 100%. ConsoleWorks can enforce assigned Roles of individuals responsible for performing restoration activities. At the same time, ConsoleWorks logs all activity (down to the keystroke and response), records Graphical sessions for review or forensic purposes, if required, later.
Backup "gold copy" resources, such as firmware, software, ladder logic, service contracts, product licenses, product keys, and configuration information. Verify that all "gold copy" resources are stored off-network and store at least one copy in a locked tamperproof environment (e.g., locked safe).	ConsoleWorks is continually collecting current configuration for firmware, software, ladder logic, ports, services, users and groups, security settings, for all devices it manages (and saves historical configuration information), it always knows what the approved configuration should be. Additionally, ConsoleWorks' backup feature can be configured to ensure backups are taken and stored offline. These backups can be pushed offsite for storage, per the business continuity and security policy.

Test and validate data backups and processes in the event of data loss due to malicious cyber activity.	ConsoleWorks may be configured to run regular checks making sure configuration data is good (ensure current configuration and settings matches the approved configuration settings). As a reference, historical configurations are kept as well.
HARDEN YOUR NETWORK	**CONSOLEWORKS STAUNCH DEFENSE TO SECURE OT/ICS** VIEW CONSOLEWORKS SCREENSHOT
Remote connectivity to OT networks and devices provides a known path that can be exploited by cyber actors. External exposure should be reduced as much as possible.	With ConsoleWorks, all communications to an OT network must come through ConsoleWorks. It provides the protocol break between the user accessing ConsoleWorks (HTTPS in this case) and assets which they want to access. Access to those assets utilizes their native interactive protocol (SSH, Telnet, RDP, etc.). The protocol break created by ConsoleWorks prevents viruses and malware from moving through ConsoleWorks, adding a disconnected layer of security via protocol changes. This also limits the need to only expose one PORT or SERVICE to the outside, HTTPS which may be defined on a non-standard port.
Remove access from networks, such as non-U.S. IP addresses, if applicable, that do not have legitimate business reasons to communicate with the system.	ConsoleWorks may be configured with IP address controls, security certificate requirements, username / password, multifactor authentication methods to prevent access to all but those who have a legitimate reason to gain access. And that's just to ConsoleWorks - then the actors role controls where they may go - so they are also limited.
Fully patch all Internet-accessible systems.	ConsoleWorks understands device configurations down to and including installed software, ports, services, users and groups, patch level including what is available versus what is installed. ConsoleWorks works with a defined operational patch process maintaining human oversight and control of the activity. During the process, ConsoleWorks continues to log all activity and record all sessions for audit and forensic purposes. After a patch is installed, new baselines are checked and the asset owner is made aware of the changes made on the asset such as firmware, version, settings, ports, services program or image files and protections. Each new configuration requires approval from the asset owner as a result.
Segment networks to protect PLCs and workstations from direct exposure to the internet. Implement secure network architectures utilizing demilitarized zones (DMZs), firewalls, jump servers, and/or one-way communication diodes.	After connecting through a VPN, generally interactive access is routed directly to ConsoleWorks vs dropping someone on a jump box or network. ConsoleWorks then enforces user authentication, 2FA and with its protocol break between the user and asset, there is a physical separation from the outside world to ConsoleWorks, and from ConsoleWorks to the inside/OT network. There is no access to the OT network without going through ConsoleWorks as ConsoleWorks is the originator of all access inside the Network.
Ensure all communications to remote devices use a virtual private network (VPN) with strong encryption further secured with multifactor authentication.	In addition to the VPN, ConsoleWorks also implements a protocol break preventing malware, viruses from penetrating into the OT network. Access to ConsoleWorks supports standard multifactor authentication technologies.
Check and validate the legitimate business need for such access.	ConsoleWorks has the capabilities to support / enforce policies set by the business for access control.

Filter network traffic to only allow IP addresses that are known to need access and use geo-blocking where appropriate.	ConsoleWorks may be configured with IP address filters and controls, security certificate requirements, username / password, multifactor authentication methods to prevent access to all but those authorized users who have legitimate reason to gain controlled access.
Connect remote PLCs and workstations to network intrusion detection systems where feasible.	Events generated from Network Intrusion Detection systems can be sent to ConsoleWorks for immediate investigation to facilitate human response (faster MTTR). When events occur, they should be investigated. This generally requires human access to a sensor or to the network where cyber security controls are enforced. Thus, using ConsoleWorks for this access creates the oversight of changes to the cyber sensors and configurations of end point assets.
Capture and review access logs from these systems.	ConsoleWorks may be configured to monitor logs from network intrusion detection systems and look for patterns of interest or Events. In addition, Events generated from Network Intrusion Detection systems can be sent to ConsoleWorks for immediate investigation to facilitate human response (faster MTTR). This generally requires human access to a sensor or to the network where cyber security controls are enforced. Thus, using ConsoleWorks for this access creates the oversight of changes to the cyber sensors and configurations of end point assets.
Ensure all communications to remote devices use a virtual private network (VPN) with strong encryption further secured with multifactor authentication.	In addition to the VPN, ConsoleWorks also implements a protocol break preventing malware, viruses from penetrating to the OT network. Access to ConsoleWorks supports standard multifactor authentication technologies.
Secure all required and approved remote access and user accounts.	This is the most basic use case for ConsoleWorks Secure Remote Access.
Prohibit the use of default passwords on all devices, including controllers and OT equipment.	ConsoleWorks may be configured to check whether vendor default passwords exist on any device, including controllers and alert / notify appropriate personnel. It also has the capability to change passwords on assets to enforce their maximum complexity based on a user defined schedule.
Remove, disable, or rename any default system accounts wherever possible, especially those with elevated privileges or remote access.	ConsoleWorks may be configured to check for default vendor accounts on all devices and alert / notify appropriate personnel. Default accounts and password may be automatically check for and disabled and/or simply alerted on when found.00.01.0
Enforce a strong password security policy (e.g., length, complexity).	ConsoleWorks may be configured to enforce the maximum complexity of passwords supported by a device. Many OT devices have limited password security support. With ConsoleWorks controlling access, the security is strengthened because a user is required to enter ConsoleWorks first using multiple authentication methods including AD, multifactor authentication and they would not need or know the credentials to access a device. ConsoleWorks would provide the necessary credentials when it establishes the connection on behalf of the actor.

Require users to change passwords periodically, when possible.	ConsoleWorks enforces (and can automate) changes to passwords on a regular cadence defined by security or compliance policies.
Enforce or plan to implement two-factor authentication for all remote connections.	ConsoleWorks supports two-factor authentication for interactive sessions to ConsoleWorks. Utilizing 2FA to OT assets is not always supported by the asset. However, when it is supported or if PKI is supported, ConsoleWorks will utilize the most secure capability supported by the asset or intermediate assets to remote connections.
Harden or disable unnecessary features and services (e.g., discovery services, remote management services, remote desktop services, simulation, training, etc.).	Once devices are hardened and unnecessary features and services are disabled, ConsoleWorks can be used to perform regular checks (daily, weekly, etc.) to ensure the configuration does not change. It does this be establishing the approved configuration as the baseline. Also, subsequent checks are compared to the approved baseline. If differences are detected, appropriate personnel are immediately notified.
CREATE AN ACCURATE "AS-OPERATED" OT NETWORK MAP IMMEDIATELY	**CONSOLEWORKS STAUNCH DEFENSE TO SECURE OT/ICS**
Use vendor-provided tools and procedures to identify OT assets.	ConsoleWorks integrates with Asset Discovery tools, where discovered assets may be quickly onboarded to enable secure remote access, as appropriate. Where discovery provides information such as configuration, make, model, vendor etc that information is gathered by ConsoleWorks and may be also compared to the information collected by ConsoleWorks via a different method. Having two or more sources of the same information about an asset is critical in today's cyber world. Comparing the same information from all sources creates confidence in the information.
Use publicly available tools, such as Wireshark, NetworkMiner, GRASSMARLIN, and/or other passive network mapping tools.	ConsoleWorks integrates with Asset Discovery tools, where discovered assets may be quickly onboarded to enable secure remote access, as appropriate. Where discovery provides information such as configuration, make, model, vendor etc that information is gathered by ConsoleWorks and may be also compared to the information collected by ConsoleWorks via a different method. Having two or more sources of the same information about an asset is critical in today's cyber world. Comparing the same information from all sources creates confidence in the information.
CREATE AN ASSET INVENTORY	**CONSOLEWORKS STAUNCH DEFENSE TO SECURE OT/ICS** VIEW CONSOLEWORKS SCREENSHOT
Include OT devices assigned an IP address.	Because ConsoleWorks requires knowledge of an asset in order to control access, IP address is a part of the meta data stored in ConsoleWorks. This information is also gathered with the baseline collections for the asset.
Include software and firmware versions.	ConsoleWorks configuration monitoring collects the software and firmware version for a given asset. Getting the information directly from the asset prevents manual entry inconsistencies.

Include process logic and OT programs.	ConsoleWorks configuration monitoring can be configured to collect process logic and OT program information for a given asset. Getting the information directly from the asset prevents manual entry inconsistencies.
Include removable media.	ConsoleWorks may be configured to alert when removable media is being used or has been enabled on an asset.
Include standby and spare equipment.	Standby and spare equipment is configured in ConsoleWorks just as active equipment. In this case, they are disabled until which time they are needed. Since they are configured in ConsoleWorks, they would be included in the asset list, but tagged with the appropriate status. Should a major failure occur, ConsoleWorks would see the failure and could automatically start the backup system if that is the business process.
IDENTIFY ALL COMMUNICATION PROTOCOLS USED ACROSS THE OT NETWORKS	**CONSOLEWORKS STAUNCH DEFENSE TO SECURE OT/ICS**
Investigate all unauthorized OT communications.	CW controls all human access of OT communications. ConsoleWorks can alert on an actor performing unauthorized activity. ConsoleWorks also has the ability for an authorized user to disconnect a session that might be performing activity that is not authorized.
Include all business, vendor, and other remote access connections.	ConsoleWorks should be the only method of access for all business, vendor and other remote access needs (contractor). Privileges for each of these types of users is controlled through Roles. All activity is recorded for forensic and audit purposes. Before a user gains access to a device, ConsoleWorks may be configured to collect the current configuration from the asset. Once a user logs out, another configuration can be collected and compared to the previous version to determine what changes were made during their interactive session.
Review service contracts to identify all remote connections used for third-party services.	Vendors, Contractors and Employees are connected through ConsoleWorks for all OT asset access without impacting the vendor's ability to do their job. At the same time, ConsoleWorks is monitoring what they have done, changes made, etc. for audit and forensic use.
UNDERSTAND AND EVALUATE CYBER-RISK ON "AS-OPERATED" OT ASSETS	**CONSOLEWORKS STAUNCH DEFENSE TO SECURE OT/ICS** VIEW CONSOLEWORKS SCREENSHOT
Vendor-specific cybersecurity and technical advisories.	Security benchmarks, baselines of configuration, patches, nvd, cve, access roles and limitations, and other integrated other systems that collect data such as discovery, nmap, grassmarlin, etc.
National Institute of Standards and Technology – National Vulnerability Database. Available at https://nvd.nist.gov.	TDi Technologies and ConsoleWorks is a NIST / NCCoE NCEP partner and has been included and participated in over 10 cybersecurity user cases.
Implement mitigations for each relevant known vulnerability, whenever possible (e.g., apply	ConsoleWorks supports organizations process for mitigating known vulnerabilities. ConsoleWorks has the ability to evaluate current device configuration for current software and notify users if security patches are

software patches, enable recommended security controls, etc.).	available. ConsoleWorks can also collect security configuration information on assets to determine the security vulnerability / risk score.

IMPLEMENT A CONTINUOUS AND VIGILANT SYSTEM MONITORING PROGRAM	**CONSOLEWORKS STAUNCH DEFENSE TO SECURE OT/ICS** VIEW CONSOLEWORKS SCREENSHOT
Log and review all authorized external access connections for misuse or unusual activity.	ConsoleWorks logs all activity down to the keystroke and records all user RDP sessions. Upon detection of misuse or unusual activity, ConsoleWorks has the ability for a user with authority to disconnect a session in question.
Monitor for unauthorized controller change attempts.	Once an approved baseline has been established for a PLC's controller process logic, ConsoleWorks can run integrity checks and notify appropriate personnel if changes are detected. Other automated actions may also be defined.
Implement integrity checks of controller process logic against a known good baseline.	Once an approved baseline has been established for a PLC's controller process logic, ConsoleWorks can run integrity checks and notify appropriate personnel if changes are detected. Other automated actions may also be defined.
Where possible, ensure process controllers are prevented from remaining in remote program mode while in operation.	Once ConsoleWorks knows that the process controller should not remain in remote program mode while in operation (sets the operation baseline), it will check to ensure the mode has not been changed. If a difference is detected notifications are sent to the appropriate personnel. In some cases, ConsoleWorks can be configured to automate some activities.
Lock or limit set points in control processes to reduce the consequences of unauthorized controller access.	ConsoleWorks can use a few of its capabilities for locking or limiting set points in control processes. In some cases, RBAC can be used to limit who has the ability to access the controller. ConsoleWorks configuration monitoring can be used to perform regular checks as well.