ICS/OT Security Hardening Checklist

DRAGOS

Date	**Revision #** 1.0	**Revision History** • August 2023 - Create initial draft
Process Owner:		
Author/Editor:		

1. Remove Nonessential Components

☐ Audit system(s) to identify and remove any services, applications, protocols, drivers, and other nonessential components.

☐ Disable nonessential components that cannot be removed.

☐ Disable insecure communication protocols not required for business purposes.

☐ Remove the following as applicable, where technically feasible.

- ☐ Email services
- ☐ File sharing services
- ☐ Network management tools
- ☐ Printer sharing services

☐ Disable debug mode.

☐ Ensure all configuration settings are documented.

2. Restrict Remote Access

☐ Engineering and OT teams must evaluate what systems are necessary to leverage remote access.

☐ Remote access, including process control, should be limited as much as possible.

☐ Remote access requirements should be determined, including IP address, communication types, and what processes can be monitored. All others should be disabled by default.

☐ User-initiated access should require multi-factor authentication.

☐ All remote access communication should be logged and monitored.

☐ Document the remote access mechanism, required configuration, and use case.

☐ Ensure remote access needs are periodically reviewed.

3. Change Default Passwords

☐ Change all default passwords for devices and applications.

☐ Passwords must meet organizational password requirements, where technically feasible.

☐ Change local default root/administrator username and password per application.

☐ Change local default root/administrator username and password on console/maintenance ports.

☐ Devices that can't meet organizational password requirements must be configured to the maximum password strength.

4. Access Controls/Principle of Least Privilege

☐ Devices must be configured with individual user's accounts, where technically feasible.

☐ Ensure that administration-level (privileged access) accounts are required to perform any configuration changes on the system.

☐ Separate administration-level accounts must be created for each administrator on the system.

☐ Operator accounts/user accounts are required for normal operation of the device.

☐ If the device does not support unique users' accounts, document the shared account information.

☐Utilize features such as "kiosk mode", where feasible.

5. Device Firmware Upgrade

☐ Identify the device firmware version.

☐ Check the vendor website for firmware updates.

☐ If an update is available, validate the firmware update authenticity and integrity by verifying the file hash or cryptographic key.

☐ Test the update in a lab or development environment before implementing into production.

☐ Backup the current firmware before applying the update.

☐ Retain an offline copy of the firmware and corresponding hash or cryptographic key.

☐ Annotate on the OT cyber asset inventory the current firmware version.

6. Vulnerability Identification and Patching

☐ Review OT asset inventory for identified and known vulnerabilities.

☐ Develop a method to determine if a patch is critical, high, medium, or low.

☐ Patch critically and assessment of risk will determine whether you implement a patch now, next, or never.

☐ Check vendor website for vulnerability updates.

☐ Validate each vulnerability update authenticity and integrity by validating the file hash or cryptographic key.

☐ Test functionality in a lab or development environment before implementing into production.

☐ Annotate on the OT cyber asset inventory the current patched version.

7. Additional Security Considerations

☐ Configure built-in security features such as host-based firewalls, port-security, logging, anti-virus, etc.

☐ Replace self-signed certificates with Certificate Authority (CA) signed certificates.

☐ Physically secure cyber assets.

☐ Implement network segmentation where feasible.

☐ Password protect configuration and project files.

☐ Update OT cyber asset inventory by identifying new cyber assets and documenting any configuration changes.