Device Hardening

Siemens Energy is proud to offer an OT Device Hardening solution that reduces the security risk to the devices by eliminating potential attack vectors and condensing the system's attack surface.

Problem	Cause	Solution	Benefit
• Insecure default configuration never adjusted • IT hardening procedures are applied without expert input, causing operational failures • Unhardened endpoints are easy attack targets • Regulatory requirements dictate hardening activities take place	• Common misconfigurations or not optimal security configurations with defaults • Common IT hardening measures may not be compatible with OT systems	• Configure settings on endpoints and other systems using "secure hardening standards" (configuring system firewall, AV, MAC address filtering, application whitelisting, etc.) • Only required software and programs are installed in the base image, others are all uninstalled	• Common misconfigurations are unable to be exploited • Attack surface reduction (limiting available and open services and ports running) • Overall security within the environment is substantially increased

What We Deliver?

- An executive summary of the hardening scope, test plan, and critical findings.
- Detailed Hardening results explaining the vulnerabilities addressed, approach, impact, and recommended countermeasures for the identified vulnerabilities.
- Identification of specific issues that cannot be addressed for whatever reason
- Hardening activities performed during the execution timeframe and recommendations.

How We Deliver?

Design	Install	Configure	Service
- Kick-off meeting - Request for documents - Review network diagrams - Update network diagrams with new components - Plan device hardening in-scope assets and timeline	- All components hardened upon delivery - Perform hardening activities on all in-scope assets - Document all changes made to in-scope assets	- Verify hardening has no negative impact on production systems - Adjust restrictions as needed	- Final report on hardening activities - Test hardening with each product release - Test hardening effects with each patch release - Update hardening guidelines as needed