

## SERVICES

# SECURE DESIGN & DEPLOYMENT SYSTEM HARDENING & COMMISSIONING



## SECURE FROM THE FIRST SWITCH ON

Commissioning new OT systems often involves default configurations, unnecessary open services, insecure or default passwords, or weak protocol settings. If devices are deployed without hardening, they become easy targets once in operation.

Arista Cyber brings hardened standards and secure baseline practices into your commissioning process. From disabling unneeded services to enforcing least-privilege and secure patching practices, we ensure that system setup is secure from day one. We work side by side with your engineering, commissioning, and operations teams, reviewing device specifications, firmware and service settings. We validate configurations in approved environments before deployment and help you build commissioning practices that maintain security over time. Our collaborative approach ensures that hardening is practical, aligned with functionality, and sustainable.

## KEY BENEFITS

- Reduced attack surface and prevent exploitation from day one of system use.
- Standardize secure configurations across OT assets.
- Enhanced consistency and repeatability across sites and devices.
- Faster, safer deployments that support compliance with industry standards.
- A stronger foundation for ongoing security posture improvement.

## DELIVERABLES

- Secure commissioning checklists & baseline configurations.
- Review and hardening of protocols, patching, and default credentials.
- Hardening guidelines for PLCs, HMIs, RTUs, and servers, network devices.
- Implementation to support compliance with industry standards
- Procedures for secure deployment & commissioning.
- Implementation plan with milestones, testing, and validation.
- Final Hardening Report

**PARTNER WITH ARISTA CYBER TO DESIGN, DEPLOY, AND  
PROTECT YOUR OT OPERATIONS WITH BUILT-IN SECURITY  
AND LASTING CONFIDENCE.**



## HAVE A QUESTION?

[Contact](#) our industrial cybersecurity professionals for more information.

[REQUEST A CONSULTATION](#)

LOCK DOWN YOUR OT SYSTEMS—MINIMIZE WEAKNESSES, MAXIMIZE RESILIENCE. HARDENED OT ENVIRONMENTS THAT ATTACKERS CAN'T EASILY EXPLOIT

**VISIBILITY. INTEGRITY. RESILIENCE.**

Let's Fortify Your Future.

**More information**

Email us: [info@aristacyber.io](mailto:info@aristacyber.io)  
Or visit [aristacyber.io](http://aristacyber.io)