Honeywell
THE POWER OF CONNECTED | Industrial Cyber Security

System Hardening to Optimize Process Control Network Security

Service Note

Expert system hardening provides the configurations, updates, and compliance benchmarking that will optimize security across your process control network and related operational systems. Reduce vulnerabilities and security risks, improve compliance with industrial cyber security standards, and safely execute IT-OT convergence with hardening tailored to the operational environment.

Software systems behave differently depending on how they are configured and integrated with other systems in your industrial control system environment. Honeywell CyberVantage Security Consulting Services provide hardening for process control network (PCN) and related networks hardening services, performed by skilled industrial cyber security consultants. Leveraging the Center for Internet Security (CIS) industry standard, our customized hardening services eliminate or reduce system vulnerabilities, and develop your industrial control system security policy – while catering for the unique requirements of your operational environment.

Safety and Compliance

The CIS standard provides important benchmarks for operating system (OS) cyber security, but applying all standards without regard to the needs of an industrial setting can increase the risk of operational failure.

Operational facilities often specify individualized policies, sometimes with unique configurations for each OS, based on their deep knowledge of what impacts critical processes.

Customer requirements are diligently integrated into each hardening service, prioritizing plant safety and uptime.

FEATURES & BENEFITS

FEATURES

- System hardening for process control network systems and software
- Customized compliance benchmarking prioritizing safety and uptime
- Delivered by consultants with deep technical expertise in both operations and industrial cyber security
- Experience from 5000+ PCN engagements
- Safe-on-site personnel
- CIS benchmarking
- Independent opinions
- Detailed reports

BENEFITS

- Reduced security vulnerabilities from new or changed systems and software on the PCN
- Compliance status according to latest industry benchmarks (CIS)
- Documentation for audit and regulatory bodies (e.g. insurance)
- Validated system status

Honeywell CyberVantage industrial cyber security consultants carefully validate, adjust, and apply CSI recommendations within a control system context. Customer requirements are diligently integrated into each hardening service, prioritizing plant safety and uptime.

Highly skilled and experienced Honeywell professionals are safe on site, ensuring system hardening is safely implemented while maximizing compliance. In most cases we improve customer CSI compliance from 20-30% to 80-90%.

Reducing Vulnerabilities and Risks

System hardening eliminates potentially hazardous vulnerabilities, and implements risk-reduction measures, such as shutting down unnecessary services and properly assigning user rights.

For companies hoping to deploy IT technologies in their control system environment, OT-specific system hardening is essential to avoid inadvertent or malicious disruption to production. We ensure settings based on IT environments that are impractical for operations (which vary from endpoint to endpoint) are excluded from centrally administered compliance checks. Similarly, we account for the potential for compatibility issues later (such as with future or third party applications). Settings are carefully implemented locally at each node by skilled Honeywell CyberVantage consultants.

Supporting Evolving Networks

As organizations develop, new equipment and software is frequently introduced into the network. This can introduce or leave dangerous security vulnerabilities exposed. New vulnerabilities can also inadvertently be introduced by default incompatible with related system configurations. New equipment is often not verified holistically for operational impact, and configurations can accidentally negate related device's or system's instructions. Hardening services can mitigate these risks.

Cyber Security Remediation

Cyber security assessments are an important part of industrial network routines. They can uncover high severity security issues and scope remediation actions to reduce the risk of incidents.

Remediation work helps upgrade systems and software, and prompts necessary system hardening to limit vulnerabilities. As companies complete network or cyber security assessments, they often find the logical next step is system hardening.

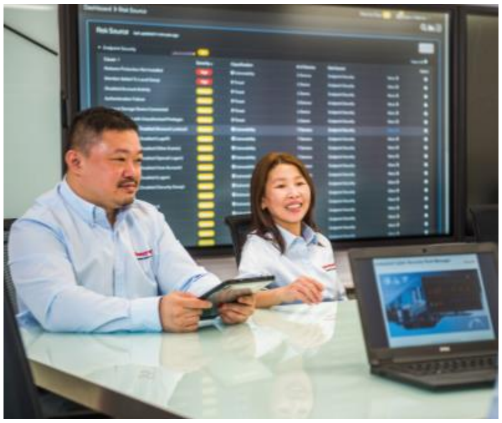
CyberVantage Hardening Options:

Process Control Network (PCN) Security Hardening

These services target domain based Windows operating systems prevalent across the ICS, from Windows 2016 to Windows 7. While CIS hardening benchmarks and evaluation tools form the basis of the policies and configurations, the baselines are reviewed and tailored for VRF's Process Control Networks and are tested by Honeywell CyberVantage consultants for compatibility with Experion PKS applications.

Network Hardening

These services target networking devices, leveraging CIS device configuration recommendations, carefully customized for operational environments. Devices commonly include switches and routers.



Engaging highly skilled and experienced Honeywell CyberVantage professionals for system hardening ensures compliance measures are safely implemented and improved, in most cases enhancing customer CSI compliance from 20-30% to 80-90%.

Honeywell Industrial Cyber Security

Honeywell is the leading provider of cyber security solutions that protect industrial assets, operations and people from digital-age threats. With more than 15 years of cybersecurity expertise and over 50 years' industrial domain expertise, we combine proven cybersecurity technology and industrial know-how to maximize productivity, reliability and safety.

For companies hoping to deploy IT technologies in their control system environment, OT-specific system hardening is essential to avoid inadvertent or malicious disruption to production.

CyberVantage Security Consulting

Honeywell CyberVantage Security Consulting Services provide over 30 specialized industrial cyber security offerings and custom consulting to help process control industries safely operate and connect.

Honeywell CyberVantage consultants are versed in both industrial operations and cyber security to help companies best assess their risks, design robust architectures, protect networks and endpoints, and improve situational awareness and incident response. Customers can leverage Honeywell Centers of Excellence to safely simulate, validate and accelerate their cross-vendor industrial cyber security solutions in state-of-the-art facilities staffed by Honeywell CyberVantage experts.

Where Innovation Meets Implementation to Drive Industrial Cyber Security Excellence

Honeywell CyberVantage Security Consulting Services provide 30+ specialized industrial cyber security offerings and custom consulting to help process control industries safely operate and connect. Honeywell CyberVantage consultants are versed in both industrial operations and cyber security to help companies best assess their risks, design robust architectures, protect networks and endpoints, and improve situational awareness and incident response. Consultants can help customers leverage any of nine Honeywell Centers of Excellence to safely simulate, validate and accelerate their cross-vendor industrial cyber security solutions in state-of-the-art facilities staffed by experts.

For More Information

Learn more about how Honeywell's Cyber Services can improve your enterprise security, visit becybersecure.com or contact your Honeywell Account Manager.

Honeywell Process Solutions

1250 West Sam Houston Parkway South
Houston, TX 77042

Honeywell House, Skimped Hill Lane Bracknell,
Berkshire, England RG12 1EB UK

Building #1, 555 Huanke Road, Zhangjiang Hi-Tech Industrial Park, Pudong New Area,
Shanghai 201203

www.honeywellprocess.com

SV-18-05-ENG
October2018

Honeywell