Honeywell | Industrial Cybersecurity

Process Control Network (PCN) Hardening Service

Service Note

With Honeywell's expert assistance, industrial organizations can reduce cybersecurity risks by applying tested and qualified security settings and configurations to existing assets across Process Control Networks (PCNs), thus increasing their resiliency against cyber-attacks.

Today, the cyber threats to Industrial Control System (ICS) assets have never been greater. Hardening is a service intended to reduce vulnerabilities and security risks, improve compliance with industrial cybersecurity standards, enable safe Information Technology (IT)-Operational Technology (OT) convergence, and allow for the application of more secure configurations to existing systems.

The Honeywell PCN Hardening service is a driver of improved compliance and safety at today's industrial facilities. Expert industrial cybersecurity consultants carefully evaluate, customize and enforce cybersecurity recommendations for process control installations.

Need for PCN Hardening

In a typical manufacturing plant, control system networks are crucial asset. PCN hardening is a method of improving security on network devices and reducing vulnerabilities through configuration changes applied directly to the network device (e.g., a switch or router). It employs a standardized approach to implementing hardening on different networking components. This process involves denying or restricting access to unnecessary services and allowing only authorized access to necessary services.

Honeywell's Effective Approach

Honeywell is committed to optimizing the security of PCNs and related operational systems. Our Cybersecurity Hardening Service focuses on consistent and supportable policies, disabling services or features not required to perform core functions, and installing elevated security configurations.

Honeywell-certified cybersecurity staff will carefully validate, adjust and apply Honeywell recommendations within a PCN context. During this engagement, customer requirements are diligently integrated, prioritizing plant safety and ensuring uptime.

As part of the scope of work, Honeywell cybersecurity experts will:

FEATURES & BENEFITS

- Improves security consistency and manageability of OT systems
- Works with Honeywell and non-Honeywell systems
- Compatible with Experion PKS R410x, R500x and R510x
- Consistent solution, which is supportable by Honeywell
- Customizes baseline profile creation
- Provides the opportunity for future upgrades as software changes
- Optimizes cybersecurity remediation efforts
- Drives improved standards compliance and safety
- Reduces potential vulnerabilities and risks
- Safely deploys policies without impacting operations

- Integrate standard policies with the existing process control infrastructure. These policies are designed for compatibility with the PCN, including Experion PKS R410 and up, and non-Experion nodes commonly found in the PCN.
- Audit, design and remediate existing PCN equipment based on Honeywell's standard hardening specification. An audit is first conducted to identify deviations from Honeywell's standard guidelines, and the design is based on these deviations but tailored to the site with stability and availability in mind. This design will then be applied uniformly to site system and networking assets. The scope typically includes Experion and non-Experion nodes for system hardening, and routers, switches and firewalls in L2, L3 or L3.5 (DMZ) for network hardening.

The supported platforms for Honeywell's PCN hardening solution include:

- MS Windows Servers and Endpoints
- Domain-based environments
- Windows 7/2008R2 and newer operating systems (e.g., EPKS R410 and newer)

Summary

Description	Tests				Scoring		
	Pass	Fail	Error	Hotfix	Score	Max	Percent
1 Account Policies	7	2	0	0	7.0	9.0	78%
1.1 Password Policy	5	1	0	0	5.0	6.0	83%
1.2 Account Lockout Policy	2	1	0	0	2.0	3.0	67%
2 Local Policies	103	1	0	0	103.0	104.0	99%
2.1 Audit Policy	0	0	0	0	0.0	0.0	0%
2.2 User Rights Assignment	39	1	0	0	39.0	40.0	98%
2.3 Security Options	64	0	0	0	64.0	64.0	100%
2.3.1 Accounts	6	0	0	0	6.0	6.0	100%
2.3.2 Audit	2	0	0	0	2.0	2.0	100%
2.3.3 DCOM	0	0	0	0	0.0	0.0	0%
2.3.4 Devices	2	0	0	0	2.0	2.0	100%
2.3.5 Domain controller	3	0	0	0	3.0	3.0	100%
2.3.6 Domain member	6	0	0	0	6.0	6.0	100%
2.3.7 Interactive logon	7	0	0	0	7.0	7.0	100%
2.3.8 Microsoft network client	3	0	0	0	3.0	3.0	100%
2.3.9 Microsoft network server	4	0	0	0	4.0	4.0	100%
2.3.10 Network access	9	0	0	0	9.0	9.0	100%
2.3.11 Network security	10	0	0	0	10.0	10.0	100%
2.3.12 Recovery console	0	0	0	0	0.0	0.0	0%
2.3.13 Shutdown	1	0	0	0	1.0	1.0	100%
2.3.14 System cryptography	0	0	0	0	0.0	0.0	0%
2.3.15 System objects	2	0	0	0	2.0	2.0	100%
2.3.16 System settings	0	0	0	0	0.0	0.0	0%
2.3.17 User Account Control	9	0	0	0	9.0	9.0	100%
3 Event Log	0	0	0	0	0.0	0.0	0%
4 Restricted Groups	0	0	0	0	0.0	0.0	0%
5 System Services	0	0	0	0	0.0	0.0	0%
6 Registry	0	0	0	0	0.0	0.0	0%

Honeywell's Security Configuration Assessment Report captures highly detailed audit/compliance records.

How the System Hardening Works

The Honeywell PCN Hardening solution makes existing operating systems/configurations less susceptible to cyberattack by:

- Shutting down unused services or legacy services
- Creating and implementing group policies and procedures for users and computers
- Enabling centralized management of systems
- Eliminating the need for testing at the client site
- Minimizing risk of adverse effect on the OT environment

Some of the hardening activities on network devices include:

- Password protection
- Configuration of privilege levels
- Disabling unused services
- Auditing unused and open ports
- Limiting remote and local access
- Displaying log-in banner
- Configuring SNMP
- Configuring AAA

The hardening strategy is targeted to Cisco switches, routers and firewalls. However, Honeywell can develop hardening configurations for other vendors based on customer requirements.

The Honeywell PCN hardening process includes a number of key steps:

Evaluation: Evaluate customer environment, security policies and procedures. Baseline reports may be created to highlight the beginning system state.

Building: Build custom hardening policies using customer security policies, industry benchmarks and Honeywell best practices, and then integrate Honeywell's hardened policy library with the existing domain structure.

Testing: Test custom hardening policies in a simulated lab environment.

Enforcement: Deploy the policies to lock down the systems/networks.

Validation and Acceptance: Validate the applied policies in the customer environment.

Documentation: Gather pre- and post-hardening reports and provide hardening documentation to document compliance.

The primary components of Honeywell's PCN hardening approach include:

Domain Group Policy: Use Group Policy Objects (GPO) to enforce and centrally manage security policies.

Process Control Network (PCN) hardening is a method of improving security of network devices and reducing vulnerabilities through configuration changes applied directly to the network device.

The Honeywell PCN Hardening service makes existing operating systems/configurations less susceptible to cyber-attacks.

Disabling Services: Disable unwanted services.

User Rights Assignments: Create user access control based on least privilege access policies.
All components are standardized according to Honeywell's best practices to provide repeatability and improved support.

Compliance with Industry Standards

In developing an effective PCN hardening solution, Honeywell reviewed and compiled settings from multiple sources, including vendor recommendations, third-party hardening recommendations and its own best practices on configuring industrial control networks. These settings provide measurable compliance with industry-recognized standards such as Center for Internet Security® (CIS) benchmarks and are tailored for industrial networks. They are specifically designed for process control systems, including compatibility with various ICS nodes.

Honeywell customizes the CIS profile for standardized hardening packages, ensuring accurate compliance evaluation. These packages, covering hardening on both Fault Tolerant Ethernet (FTE) and non-FTE switches, take into account the impact of hardening on critical networking nodes.

Honeywell certified Cybersecurity experts work closely with customers to validate, adjust and apply best practices for PCN hardening.

Why Honeywell?

Honeywell has more than 50 years of industrial experience and know how to optimize IT/OT convergence. We are the leading provider of cybersecurity solutions, protecting the availability, safety and reliability of industrial facilities worldwide, and helping securely deploy the Industrial Internet of Things (IIoT).

Our company has over 340 dedicated cyber experts, thousands of successful multi-vendor installations, and 500+ Managed Security Service (MSS) sites.

Honeywell's complete portfolio includes cybersecurity software, MSS solutions, industrial security consulting, and integrated security solutions. We combine industry-leading expertise in cybersecurity and decades of experience in process control, for the best solution in an OT environment.

For More Information

Learn more about how Honeywell's PCN Hardening solution can improve cybersecurity, visit www.becybersecure.com or contact your Honeywell Account Manager, Distributor or System Integrator.

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
March 2020