Honeywell | OT Cybersecurity

PROCESS CONTROL NETWORK HARDENING SERVICE

SERVICE NOTE

With the assistance of Honeywell's experienced cybersecurity engineers, a customer's industrial facilities can reduce cybersecurity risks by applying fundamentally secure settings to existing assets across process control networks, increasing resiliency against cyber attacks.

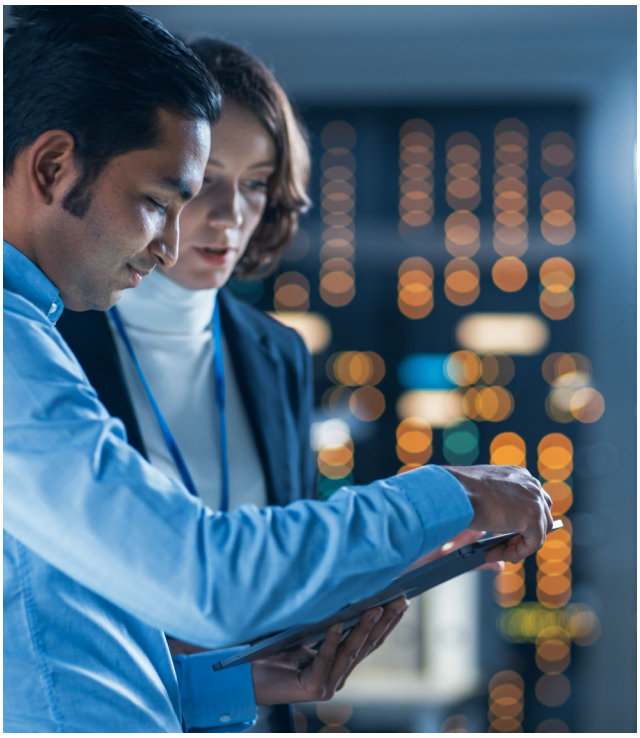
Cyber threats targeting industrial control systems continue to grow. Hardening - one of the key countermeasures - helps reduce the attack surface by applying and enforcing more secure settings to existing systems and network devices.

Need for Hardening

The backbone of an industrial facility is the process control network (PCN) and its safe operation. Unfortunately, many systems and network devices used on the PCN can have several weaknesses, such as less secure device configuration, unmanaged access privileges, and unused services. These insecure settings can act as a backdoor for attackers to cause significant damage to the systems. Honeywell's PCN Hardening Service is designed to help reduce the overall risk of cybersecurity incidents by auditing and enforcing secure settings.

Hardening for Industrial Environments

The PCN Hardening Service from Honeywell, based on Center of Internet Security (CIS®) guidelines, Honeywell best practices, and 3rd party recommendations, is a methodical approach to hardening and is engineered for operational technology (OT) environments. Our PCN Hardening Service is a standardized process with tools and techniques that are continuously improved as new technologies are adapted by industrial operators. The process starts with an audit to identify the facility's deviations from Honeywell's PCN Hardening Service guidelines. For Honeywell's Experion PKS systems and devices on the Fault Tolerant Ethernet (FTE) network, this audit includes an assessment against configuration rules specific to Honeywell's control systems.



Honeywell's PCN Hardening Service is designed to reduce available attack vectors for industrial control systems by applying more secure configuration settings on the assets in the process control network.

Working closely with the facility and taking the company's policies into account, Honeywell proposes hardening rules that are designed to increase the site's cybersecurity without negatively impacting the operations: a top requirement from operators. The hardening rules are then applied to the site's PCN systems and networking equipment.

The hardening can be deployed on L2 to L3.5 domain-based systems with Windows operating systems. For network devices on L2 to L3.5, the hardening settings have been qualified for Cisco switches, routers and firewalls. In addition, Honeywell can develop hardening configurations for other network equipment as needed.

For Experion PKS systems and FTE devices, deviations from their applicable policies are addressed. All other systems and networking devices are hardened based on the latest industry standards available in PCN Hardening.

How the Solution Works

The PCN Hardening Service reduces the OT attack vectors by applying secure settings on the existing systems and network equipment. As an example, PCN Hardening Service is designed to improve security through:

- Implementing group policies and procedures for users and computers
- Enabling use of modern protocols and security settings
- Shutting down unused and legacy services
- Enabling centralized management of systems
- Disabling unused ports.

The PCN Hardening Service includes the following activities:

- Assessing the site environment, security policies and procedures
- Integrating industry-recommended hardening practices with existing site policies
- Testing and reviewing the hardening policies
- Deploying the policies in the production environment to lock down the systems
- Validating the applied policies with the customer for acceptance
- Providing documentation for the customer, including user guide and compliance report.

Cyber Care for PCN Hardening Service

To help ensure the continued benefits of PCN Hardening in the long run, Honeywell offers annual, proactive maintenance through the Honeywell Cyber Care service program. This includes scheduled onsite visits by Honeywell's OT cybersecurity professionals, who will assist the customer by reviewing the as-is security settings against the latest PCN Hardening policies. If any gaps are found, Honeywell can help by updating the settings according to the latest, validated recommendations. This helps the site maintain the achieved hardening benefits and stay better protected against cyber incidents.

Compliance with Industry Standards

Honeywell has adapted the CIS Benchmarks for industrial control systems and uses a customized CIS profile to allow for accurate compliance evaluation. Being able to get a reliable measure of the PCN's hardening score is important for many companies as they work to meet compliance expectations. And after Honeywell's completion of the PCN Hardening project, many of our customers have been able to report a compliance score increase from less than 30% to over 90%.

Most industrial companies see the need for improving cybersecurity but are often limited with what safeguards can be applied without compromising the operations. Thoughtfully done hardening is a key tool in any industrial company's arsenal and an essential component in their OT defense-in-depth strategy.

FEATURES AND BENEFITS

- Essential component in OT defense-in-depth strategy
- Reduces cyber attack vectors by applying and enforcing more secure settings designed for industrial control systems
- Well-suited for environments where the ability to update the systems is limited

- Developed based on CIS® guidelines, Honeywell best practices and 3rd party recommendations
- Deployed by experienced Honeywell OT cybersecurity engineers to meet specific customer needs
- Vendor-agnostic solution suitable for Honeywell and non-Honeywell systems alike

- Integrates site-specific policies as part of the design process
- Supports pre-hardened Experion® PKS R500 and later
- Supports compliance with standards requiring proof of secure system and network equipment settings

About Honeywell's Professional OT Cybersecurity Services

Honeywell's Professional Cybersecurity Services provide over 30 specialized OT cybersecurity offerings and custom consulting to help process control industries safely operate and connect. Honeywell consultants are versed in both industrial operations and cybersecurity to help companies best assess their risks, design robust architectures, better protect networks and endpoints, and improve situational awareness and incident response. Companies can leverage Honeywell OT Cybersecurity Centers of Excellence and Innovation to safely simulate, validate and accelerate their cross-vendor industrial cybersecurity solutions in state-of-the-art facilities staffed by highly-skilled professionals.

Why Honeywell?

Honeywell has more than 100 years of industrial experience and over 20 years of industrial cybersecurity domain expertise. We are the leading provider of cybersecurity solutions, protecting the availability, safety and reliability of industrial facilities worldwide. Honeywell's complete portfolio includes cybersecurity software, managed security services, industrial security consulting, and integrated security solutions. We combine industry-leading expertise in cybersecurity and decades of experience in process control, for the best solutions in an operational technology environment.

For More Information

To learn more about Honeywell's Professional Cybersecurity Services, visit www.becybersecure.com or contact your Honeywell Account Manager.

Honeywell Connected Enterprise

715 Peachtree Street NE
Atlanta, Georgia 30308

www.honeywellforge.ai

SV-18-05-ENG
April 2024

Honeywell