CASE STUDY

Cyber-attacks and data breaches are inevitable. Thus, having preventative controls, visibility and effective alerts are critical.

MIDDLE EASTERN OFFSHORE OPERATOR PROTECTS ICS ASSETS USING HONEYWELL’S PCN HARDENING SERVICE.
Attacks against industrial control system (ICS) environments not only cause business disruptions and financial loss, but can also result in injury, death or an environmental catastrophe.

A major oil and gas offshore operator in the Middle East wanted to harden its ICS environment to reduce its attack surface and in turn vulnerabilities. This meant locking down the functionality of various components within the system to prevent unauthorized access or changes, removing unnecessary functions or features, and patching any known vulnerabilities.

**HONEYWELL SOLUTION**

Instead of an ad-hoc solution, the customer chose Honeywell’s PCN Hardening Service to help harden its ICS Windows nodes. Delivered by trained and certified consultants with expertise in both operational technology and industrial cybersecurity, the Honeywell PCN Hardening Service reduces cybersecurity risks by applying tested and qualified security settings to existing assets across the system and network, thus increasing system resilience against cyber-attacks.

**CUSTOMER BENEFITS**

One of the most critical aspects of the project was the ability for Honeywell’s certified cybersecurity experts to carefully validate, adjust, and apply industry benchmarks and Honeywell recommended settings on domain controllers and Experion® servers/stations.

Using standardized hardening policies, the Honeywell PCN Hardening Service was implemented in less time than other ad-hoc solutions, including restarting and testing the functionality. Normally, hardening requires several hours of work for each Windows node, but with the creation of domain policies and the ability to disable unwanted services with a single click, Honeywell’s PCN Hardening service saved the customer a significant amount of time.

The customer was able to meet regulatory requirements by following the Center for Internet Security (CIS) hardening guidelines throughout the site. During this engagement, customer requirements were diligently integrated while prioritizing plant safety and ensuring uptime.

In the end, the Honeywell security consulting services helped this customer lower the risk and possible impact of security incidents and improve its industrial cybersecurity maturity levels.

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**

2101 City West Blvd, Houston TX 77042

Honeywell House, Arlington Business Park
Bracknell, Berkshire, England RG12 1EB UK

Shanghai City Centre, 100 Zunyi Road
Shanghai, China 200051

www.honeywellprocess.com

© 2020 Honeywell International Inc.