Honeywell
THE POWER OF CONNECTED

Industrial Cyber Security

Honeywell Helps New Energy Facility Proactively Integrate Industrial Cyber Security Controls, Improving Productivity and Security

Application Note

A major energy facility engaged Honeywell CyberVantage Security Consulting Services for the specialized expertise needed to proactively design-in multiple risk reduction measures to meet its industrial cyber security policy and related standards.

Background

A large North American energy company needed to expand its mining and extraction capabilities by building a new facility.

In existing plants, a previous cyber security assessment had already uncovered multiple high risk areas. As planning cycles for the new facility began, the leadership team needed specialized technical capabilities to ensure the issues in older facilities were not repeated in new build specifications.

In the light of advice of specific threats against energy facilities, the leadership hoped to meet and even exceed best practices for industrial cyber security layers of defense.

Challenge

Finding experts with the right level of skills was a key challenge for the company, as it sought to design a robust network architecture from the outset. Evaluating technical service partners, it became clear that point product service teams could not deliver the multi-faceted know-how needed for the facility's state-of-the-art development.

The cost and complexity of assigning multiple, distinct teams for each area of the build – such as switching equipment or wireless network surveying – was not justifiable.

In addition, the company needed strategic resources to design an architecture that could handle both current and future needs. This required experts who could foresee and spec in support for a variety of use cases.

Financial models from others in the industry showed that cyber incidents impacting production could cause multi-million dollar losses. An 8-week range maintenance window, for example, could reduce such a facility's production to around 140,000 barrels of oil per day.

This was the business case for engaging the best people and technologies for the project, to deliver a comprehensive, complex, and multi-phased effort.

Solutions and Benefits

The company had previously engaged Honeywell CyberVantage Security Consulting Services to co-develop internal policies for industrial cyber security at its brownfield operations, which consisted of four business units.

It therefore decided to engage the CyberVantage team for the new critical industrial control system design work. The scope included designing a system based on technologies multiple vendors, as well as Honeywell, from level 3.5 of the network down to level 2.

The client needed strategic resources who could design an architecture to handle both current and future needs; those who could foresee and spec in support for a variety of use cases.

Financial models from others in the industry revealed that cyber incidents impacting production at a new plant would cause multi-million dollar issues. This business case allowed for engaging the best people and technologies for the project.

About CyberVantage Security Consulting Services

The CyberVantage Security Consulting Services provide capabilities to enable safer connected plants, digital transformation, and Industrial Internet of Things (IIoT) efforts. Delivered by consultants with expertise in both operational technology (OT) and industrial cyber security, the services help organizations reduce the risk and possible impact of incidents by helping them improve industrial cyber security maturity levels.

Since CyberVantage Security Consulting Services were brought in early, the security specialists were able to complete a proper review of the planned facility's architecture, zoning, segmentation, solution choices, and integrated design requirements.

In addition to increasing production, the new facility was also designed to lower emissions in support of environmental goals. Understanding these needs, and with experience across multi-vendor plant environments, Honeywell CyberVantage consultants were able to explicitly identify and implement necessary security controls and counter measures. Based on intimate knowledge of the company's internal policies, which Honeywell's CyberVantage team had co-authored, and the latest IEC-62443 recommendations, they were able to identify how and where to augment risk reduction.

Another outcome of the work has been to reduce the security overhead for the company's system administrators. In the past, for example, different firewall approaches made it time-consuming and complicated to support different business units (BUs). A standardized design across them ensured similar firewall set-ups that allows a single central unit to handle cross-BU security operations work.

Beyond the design stage, the CyberVantage Security Consulting Services team commissioned the industrial control system, performing technical implementation of virtualization, networking, security, firewall, patch management, and anti-virus technologies. It also implemented people and process best practices.

With its their deep experience of both operations as and cyber security, as applied to control systems, the team was able to safely handle the extensive technical needs of the customer throughout the two-year project.

A key outcome of Honeywell's work has been to increase both security and productivity at the site. Increased automation and new secure remote access capabilities, allow third party or internal staff to safely troubleshoot issues without leaving their desks. Software to automate and simplify daily operational work, such as patching to close vulnerabilities or updating anti-virus, has made common tasks faster to complete, which also permits more frequent updating, critical in a dynamic threat landscape.

After start-up, Honeywell CyberVantage consultants were further engaged for on-demand expertise, as new personnel learned the systems and threat advisories emerged. While detailed documentation and deliverables were part of the service engagement, the ongoing service commitment addressed any unforeseeable requirements for specialized operational or industrial cyber security expertise.

The new facility is now successfully producing and contributing significantly to the company's overall performance, according to independent analysts, and has surpassed forecasted production. Moreover, the company has advanced its cyber security maturity significantly, moving from ad hoc, zero level security to a proactive and repeatable level to protect and mitigate threats.

A formerly flat network, where technology use was minimal and attackers could easily bypass existing firewalls, has been replaced with a defense-in-depth design and segmentation that better protects assets based on risk prioritization. The new facility has a demonstrable and repeatable security framework, and industrial cyber security processes are monitored, enforced, and constantly updated following best practices.

Summary

This new facility for a large North American energy company benefited from Honeywell CyberVantage Security Consulting Services that enabled it to improve both productivity and security.

Our consultants proactively designed-in multiple risk reduction measures, enabling the company to meet and exceed requirements. Detailed design work, meanwhile, spanned cyber security, virtualization and networking domains, with the Honeywell CyberVantage team integrating cross-vendor security technologies on time and on budget for comprehensive implementation.

For More Information

To learn more about Honeywell Cyber Security Solutions, visit www.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

AP-18-13-ENG
September 2018

Honeywell