Honeywell
THE POWER OF CONNECTED | Industrial Cyber Security

Global Petrochemical Manufacturer Fuels Business Growth and Scale through Industrial Cyber Security

Application Note

This critical infrastructure company in Asia Minor worked with Honeywell industrial cyber security experts to meet industry cyber security standards' requirements. The resulting Reference Architecture, designed to its specific needs, together with clearly scoped cyber security measures, protect the provider's high-growth service delivery capabilities and open the door to future business opportunities.

Background

Specializing in petrochemical manufacturing, this 53-year-old company has grown to over a dozen manufacturing plants in Asia Minor, and continues to expand capacity. A critical infrastructure provider, it produces ethylene, polyethylene, polyvinyl chloride, polypropylene and other chemical building blocks to create plastics, textiles, and other consumer and industrial products. Products are also exported to the United States, and countries in Europe, the Middle East, Africa, and Asia.

Challenge

Scaling to support local and global markets, the manufacturer needed to safely modernize infrastructure while meeting strict regulatory requirements. As a designated critical infrastructure provider, it faces ongoing government oversight and added cyber security responsibilities to protect operations. At the same time, regionally, there is strong competition to attract global investment, so business trust and a scalable, secure architecture are vital. The company's lack of expansive industrial cyber security personnel could slow both design and implementation of required critical security controls, and worse, allow adversaries to exploit security vulnerabilities. Keeping labor costs down and increasing automation are ongoing operational challenges as the company attempts to manage profitability.

Solution & Benefits

Honeywell Account Managers recognized that, like many industrial providers, the customer needed a holistic, informed view of cyber security across its sites. With the appropriate expertise, it could move its industrial cyber security efforts forward in more efficiently, balancing both short and long-term needs across constituents.

CyberVantage Security Consulting Services were engaged to deliver a face-to-face Technical Design Workshop with key customer personnel. Key criteria for choosing Honeywell included the need to maintain Global Technical Assistance Center (GTAC) warranties, and the company's trust in Honeywell's deep expertise to avoid risk to automation systems, DCS, and operational infrastructure.

Through the collaborative design workshop, led by a highly experienced Honeywell ICS security consultant, the right experts and decision makers were able to openly discuss needs across all of the company's sites. This expedited information-sharing and informed design of the resulting Reference Architecture delivered by the Honeywell services team. As part of a comprehensive report, the Reference Architecture mapped out a potential technical path forward.

Through a collaborative Technical Design Workshop led by a highly experienced Honeywell ICS security consultant, the right customer experts and decision makers were able to openly discuss cyber security needs across all the company's sites.

The Workshop and a Reference Architecture have helped the customer simplify risk visibility, management, and control across sites to enable safe expansion of their operations.

The technical vision prompted the necessary internal discussions regarding priorities, needs, and approaches. Honeywell industrial cyber security experts answered the customer's questions and offered insights regarding the Reference Architecture, covering a range of topics including addressing advanced security level three (SL3) metrics (often relevant for those organizations defined as critical infrastructure providers) and adherence to the IEC-62443 standard. Internally at Honeywell, some of its 200+ community of cyber security experts were tapped to peer-review recommendations and comment on any latest best practices and know-how learned from other customer engagements, both ongoing and completed.

Through the industrial cyber security sessions with Honeywell, customer leaders recognized the breadth and depth of skills necessary to meet critical infrastructure provider requirements. Focused experts could help progress efforts, and remediation work was scoped and proposed for one of the priority sites. Specialized Honeywell cyber consultants, each well versed in their particular discipline, made modifications to the network to enable two-factor authentication for secure remote access, added application whitelisting, and improved access control by adding a more secure domain architecture.

Solutions identified included Pulse Secure Gateway, and implementation of third party technologies from Dell (RSA), Palo Alto Networks, Cisco, and McAfee. The customer also later visited Honeywell's Dubai Industrial Cyber Security Center of Excellence for demonstrations of Honeywell's Industrial Cyber Security Risk Manager Solution, which was added to the scope to implement standardized cyber security risk reporting and policies.

Customer feedback reports that Honeywell has vastly increased their awareness of industrial cyber security and the importance of maintaining a focus on risk reduction efforts.

The delivered Reference Architecture and detailed remediation work scoping has helped simplify risk visibility, management, and control across sites to enable safe expansion of operations. Understanding SL3 and the latest industry standards has helped clarify the path forward, preventing costly mistakes and non-compliance.

Summary

The premier petrochemical provider in Asia Minor, this designated critical infrastructure company substantially enhanced its understanding of how to safely build and scale industrial cyber security by working with Honeywell.

Honeywell's cyber security consultants delivered detailed design recommendations specific to the customer's operations, helping it identify an appropriate Reference Architecture and strategically prioritize future risk reduction investments. As a result, its operations will be able to expand and address security level three (SL3) cyber security requirements as defined by IEC-62443 once the design is built out, opening the door to additional business opportunities while protecting its high-growth service delivery capabilities.

As important, the vetted industrial cyber security documentation and Honeywell expert engagements will help it continue to advance cyber security, an issue topic important to its international investors, government constituencies, and local citizen base. Relying on skills from Honeywell also avoided the recruiting, management and overhead complications of staffing an internal team, ultimately expediting the ability to find the right technical path forward.

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-18-12-ENG
October 2018

Honeywell