HONEYWELL FORGE

A SAFER SUPPLIER CYBERSECURITY ECOSYSTEM

Honeywell Helps Better Secure Leading Pharmaceutical Company's Suppliers with a Cybersecurity Vulnerability Assessment

TOO SERIOUS TO DABBLE– CALL THE EXPERTS

Cybersecurity threats targeting organization's industrial control system (ICS) are not always direct. Instead, the most vulnerable entries to an ICS can start with external partners, like suppliers and vendors.

Our customer, a global pharmaceutical company, realized that potential vulnerabilities like these might be in its partner ecosystem. Therefore, the pharmaceutical company wanted to get ahead of a potential breach so they trusted Honeywell to do a thorough assessment of its suppliers' operational technology (OT) cybersecurity gaps.

Why did our customer choose Honeywell? First, because our OT cybersecurity experts took the time to understand the customer's processes at more than 100 sites around the globe. Second, because our Honeywell experts used their knowledge and experience along with the customer process insight to conduct assessments that met their unique needs. Many of our competitors are simply IT vendors dabbling in the world of OT. Honeywell , however, has the knowledge and the experience to better meet the demands of OT.

The pharmaceutical company chose Honeywell over the competitors based on the quality and wealth of OT knowledge our experts provided.

SPREADING SECURITY

This was not to be a small or limited undertaking. In fact, this Cybersecurity Vulnerability Assessment is a part of a global two to three-phase project that covers more than 100 sites. The first assessment was completed for the company's site in India with other sites being covered in later phases.

Honeywell's OT cybersecurity experts conducted the vulnerability assessment to help capture the customer's control system vulnerabilities and potential weak spots. The assessment performed was a holistic technical review of the ICS infrastructure. It focused on analyzing their cybersecurity processes, procedures, and safeguards to better protect their industrial control systems (ICS) from internal and external threats.

Because Honeywell focuses on OT as opposed to IT only, our experts are skilled in considering the entirety of an ecosystem. This means including people, processes and any technical issues that can impact the ICS cybersecurity posture.

DIGGING IN

The Honeywell team has deep expertise across IEC 62443 standards and other industry-specific guidelines, as well as invaluable experience with control systems. Because of this expertise, our team was able to holistically assess the customer's ICS environment, documenting observations and recommendations to help reduce cybersecurity risks.

Our team first conducted a physical site review to perform the assessment to uncover issues such as control room doors left unlocked, passwords in the line of sight, and other security compliance violations.

The team also reviewed the customer's network equipment from third parties such as switches, routers, and firewalls; reviewed the infrastructure configurations; and checked installation processes.

All the vulnerabilities, severity levels, and remediation details were included in the Cybersecurity Vulnerability Assessment report. The report also detailed best practices and site-specific recommendations to help the customer help mitigate and prioritize any identified threats or vulnerabilities and notes regarding how and where each step can serve as a foundation for a best practice architecture.

CHALLENGES & SUCCESSES

Honeywell experts remained diligent to exceed the customer's expectations in spite of the shut down in India due to the pandemic and the unexpected need to assess and remediate assets.

We also had one secret weapon: one of our OT cybersecurity experts had real-life experience in the pharmaceutical industry. This made it possible for the team to better tailor the assessment (and recommendations) to this particular customer.

.

Honeywell Connected Enterprise
715 Peachtree Street NE
Atlanta, Georgia 30308
www.becybersecure.com

Case Study | Rev | 09/2021

THE FUTURE IS WHAT WE MAKE IT

Honeywell