HELPING IMPROVE SECURITY
FOR A GLOBAL PHARMACEUTICAL MANUFACTURER'S OT ENVIRONMENT

Case Study

Honeywell

THE CHALLENGE

For a pharmaceutical manufacturer to maintain their leading position in a competitive market, their main priorities were to improve their visibility into their network activities, automating their asset inventory, and gaining full visibility into external contractors, including remote maintenance traffic. They also needed to be compliant with the industry regulatory requirements for their advanced technologies.

THE OUTCOME

Increased near real-time visibility of all OT and IoT environments, enabling them to reduce operational downtime, while strengthening their network security, and maintaining an up-to-date inventory of all their production assets. Additionally, they now have a solution designed to continuously monitor all network activities, have near real-time threat detection capabilities, have visibility into remote access activities, and comply with the FDA's strict industry regulations.

This pharmaceutical company manufactures high-quality, proprietary, and off-patent pharmaceuticals in countries such as the US, Canada, and Israel. They also manufacture a wide range of prescription and over-the-counter medicines that are distributed globally in dozens of countries.

Sector
Process Manufacturing

Industry
Pharmaceuticals

Location
United States

Production
Over 180 drugs, sold in 25 countries

INCREASED CONNECTIVITY INTRODUCES NEW SECURITY CHALLENGES

Adopting new technologies within their OT and IoT environment has led to a significant increase in the number of devices and the traffic between them. Before implementing Cyber Insights, the pharma company needed to maintain their complex OT network using older, manually generated asset inventory methods, which proved to be challenging, as a series of unexplained incidents were difficult to investigate. Moreover, their security team was aware of the ever-growing OT attack landscape, in which other pharmaceutical manufacturers suffered hundreds of millions of dollars in damages due to attacks on their OT networks.

The fear of a potential attack and the difficulties in controlling OT network activities led their security team to proactively implement a solution that is designed to provide them with the visibility and security program improvements while taking into consideration the unique characteristics of their inter-connected OT environment.

"Honeywell's asset inventory and visibility tools helped us to stop using outdated spreadsheets and to completely digitalize our network management."

OT NETWORK ADMINISTRATOR

FINDING THE RIGHT SOLUTION

After evaluating several solutions, including both dedicated OT systems and IT security systems, the security team chose Cyber Insights. They felt that Cyber Insights is the ideal solution for their needs as it is designed to provide the security team with continuous monitoring of their OT environments, a deep understanding of OT protocols, and a user interface that they determined was ideal for use by their OT engineering team. Cyber Insights also offered functionality designed to provide their security team with the capability to monitor their compliance with industry regulations and standards and to provide them remote access visibility. Within hours after Cyber Insights was installed, the security team was provided insight into the identified risks and threats that might jeopardize their operational continuity. For example, the platform helped them map connectivity between their OT network and the Internet and detected new connections – in near real-time.

Cyber Insights also helped provide their OT security team with alerts regarding identified deviations from normal operational activities, including remote access connections by 3rd party vendors, and configuration changes on their critical-path controllers. Cyber Insights helped the security team improve its then current security program and the operational continuity of its cutting-edge pharmaceutical manufacturing facilities.

"Our dynamic and advanced production environment, together with regulator demands such as Track and Trace systems, required a significant improvement in our security capabilities. With Cyber Insights, we feel secure while we bring our production environment into the IoT era."

VP TECHNICAL SERVICES

ABOUT HONEYWELL OT CYBERSECURITY

Honeywell offers OT Cybersecurity solutions that are designed to help customers better protect industrial and building assets, operations and people from digital-age threats. With more than 25 years of OT cybersecurity experience and more than 100 years of control industry experience, Honeywell combines proven cybersecurity technology and OT know-how to help customers maximize productivity, improve reliability and increase safety. We provide innovative cybersecurity software, services and solutions that are designed to help customers better protect assets, operations and people within buildings and industrial facilities around the world. Our state-of-the-art Cybersecurity Centers of Excellence and Innovation allow customers to safely simulate, validate and accelerate their OT cybersecurity initiatives.

Honeywell Connected Enterprise
715 Peachtree Street NE
Atlanta, Georgia 30308
buildings.honeywell.com/us/en/solutions/services/cybersecurity

**THE
FUTURE
IS
WHAT
WE
MAKE IT**

Case Study | 02/2024
© 2024 Honeywell International Inc.

Honeywell