HONEYWELL FORGE

TACKLING THE CYBERSECURITY JOURNEY ONE STAGE AT A TIME

Motor Oil confronts the complexities of strict regulations in the oil and gas industry, securing multiple sites and maintaining a seamless production with Honeywell's Cybersecurity Consulting Services

Case Study

Operational technology (OT) cybersecurity was not always a part of conversations around production environments. The main concern was always the efficiency of the production output. The risks of OT cybersecurity was unknown for many years. However, that all changed for the Chief Information Security Officer, Christos Syngelakis at Motor Oil, as the need for knowing what is connected, where it's connected and how it's connected became imperative.

Honeywell's distributed control system (DCS) provided Motor Oil with optimal control of the complex and large applications the company has distributed throughout its enterprise.

And even more recently, the need for people to have access to data for many purposes internally grew. This resulted in an incredible need for Motor Oil to secure its DCS network. To Syngelakis, the engineers that build such a sophisticated computerized control system would be the most ideal partners to embark on the OT cybersecurity journey with.

ASSESS, REMEDIATE AND RESPOND

Knowing what risks nested within Motor Oil's systems, whether from Honeywell or not, was compulsory before moving forward with an OT cybersecurity provider.

Honeywell's decades of OT cybersecurity experience and solutions that will maintain the seamless production of crude oil refining and petroleum was just as compulsory to Ioannis Minoyiannis, Head of Automation at Motor Oil, in choosing Honeywell as Motor Oil's OT cybersecurity provider.

Honeywell engineers and Motor Oil engineers collaborated to build out the most efficient OT cybersecurity plan with two priorities at the forefront: maintaining network security and being able to provide a safe and healthy workplace. Another point Honeywell engineers had to consider while building out the plan was not only are there strict regulations for the oil and gas industry, but there is also a legal obligation to inform local authorities if there is a cybersecurity incident.

Honeywell engineers started with stage one, an assessment, where the Honeywell team identified what must be done to better secure the network: Honeywell systems and other vendor solutions included. From there, design and implementation into the infrastructure began.

"We started to come together as one, built trust, and created a safer business and industrial environment."
- Christos Syngelakis, *Group Chief Information Security Officer, Motor Oil*

A major challenge Motor Oil realized during the assessment phase with Honeywell engineers was that employees were using 'siloed' engineering systems for production over the years and these systems were connected to work without prior knowledge of what has been connected where, why and how. Having a clear understanding of what assets are connected, connecting the assets you want there and where/how the assets are connected are crucial in monitoring and remediating the cybersecurity risks that might arise.

Thus, the next step for Honeywell engineers and Motor Oil engineers after the assessment phase was to start in manager risk for the segregated silos and to determine where risk exists in specific roles. Motor Oil needed to integrate cloud-based AI capabilities to support their business and maintain a safe environment. As day-to-day problems can pop up, trying to lessen risk from the IT connected environment, the organization knew they needed technology that is trusted for IT installation and proven to be effective in industrial environments. Also, being able to safely use the USB ports in the DCS system was something Motor Oil Engineers needed but could not manage before.

"Honeywell was the organization that had cybersecurity experts who were able to reach our target. With our OT DCS engineers, their mentality, and existing collaboration with Honeywell engineers, we had a solid foundation to build on."
– Ioannis Minoyiannis, *Head of Automation, Motor Oil*

A SAFER AND MORE SECURE ENVIRONMENT

Before the cybersecurity solution was in place, Motor Oil was forced to wait for updates that would cause delays in progression. Being able to receive updates sooner and remotely has helped the organization maintain efficiency. With manager-based support within the application, the implementation of a secure mutual authentication environment and USB-based updates by secure way media approval, control mechanism systems were created that allowed Motor Oil to elevate even more.

Honeywell helped Motor Oil unify its assets through a distinct approach so that the refinery operations organization can easily view what cyber risk means and utilize the many years of knowledge across Honeywell engineers to identify cyber related issues at both a high level and micro level.

As cybersecurity is a necessity for oil and gas, the integrity of the OT network is very crucial for the safety and operation of Motor Oil refinery. Through managed security services, segmentation of the network, and installation of Honeywell cybersecurity products, Motor Oil was in a very different situation than they were previously – they could actually feel more safe.

THE FUTURE IS WHAT WE MAKE IT

Honeywell Connected Enterprise
715 Peachtree Street NE
Atlanta, Georgia 30308
www.honeywellforge.ai

Case Study | Rev 1 | 06/2022

Honeywell