HONEYWELL FORGE

OPTIMIZE YOUR CYBERSECURITY WITH MANAGED SECURITY SERVICES

STAR Refinery Optimizes Cybersecurity Capabilities Using Honeywell's Solution

Case Study

Today, oil and gas operations must go beyond the status quo when protecting their OT environment. It is critical to further strengthen and fortify cybersecurity protection measures.

BACKGROUND

Established in 1992, SOCAR is the state oil company of the Azerbaijan Republic, a country rich in oil and natural gas reserves. As an energy company offering integrated solutions, SOCAR is engaged in petroleum exploration; producing, processing, and transporting oil, natural gas and natural gas condensates, marketing crude petroleum and petrochemical products in domestic and international markets; and supplying natural gas to customers throughout Azerbaijan.

SOCAR Turkey Enerji A.S. (SOCAR Turkey) is a subsidiary of SOCAR. The company initiated its business operations in Turkey upon acquisition of majority shares of Petkim from the Privatization Administration in 2008.

The SOCAR Turkey Aegean Refinery (STAR Refinery) is located in Aliaga, Izmir Province, Turkey. It has an annual processing capacity of ten million tonnes (Mt) of crude oil, which is equivalent to 214,000 barrels per day (bpd). The refinery is jointly owned by SOCAR (60%) and the Ministry of Economy of Azerbaijan (40%).

Construction of the STAR Refinery began in October 2011 and operations started in October 2018.

CHALLENGE

Headlines about cyber breaches in the energy sector have gained the world's attention in recent years. While technology and security demands continue to increase for petroleum companies, skilled resources and time to apply critical security technology is often decreasing.

Although advances in process automation systems for oil refineries enable higher efficiencies and increased output, they can also bring greater cybersecurity risks. This can result in concerns about personnel safety, damage to expensive infrastructure, loss of production, and negative impacts on company reputation.

By understanding what contributes to the risk of a cyber incident, petroleum facilities can work to minimize them and achieve a higher level of performance and predictability of process systems and networks.

Throughout the oil and gas industry, the industrial control system (ICS) and process control network (PCN) play a critical role in plant operations. While their benefits in terms of efficiency and productivity have been extraordinary, these assets—once isolated in how they controlled and managed industrial processes and machinery—are now subject to the same vulnerabilities traditionally reserved for business systems.

At the STAR Refinery, specific cybersecurity support requirements included:

- Performance monitoring from several different network levels
- Flexibility for future extensions so that additional sites can be connected with minimal effort
- SC creation for L4 assets
- Centralized Microsoft and anti-virus updates

Protecting plant operations requires not only robust firewalls, but additional security measures and defenses. Detailed reporting is equally important to provide the information needed to manage and respond to malicious attacks.

HONEYWELL SOLUTION

A managed services solution for cybersecurity can help oil refineries and other industrial facilities bridge the gap between information technology (IT) and operational technology (OT) assets and better protect their control system environment. This approach is ideal for plant operators that prefer to augment or outsource their in-house capability with improved visibility into potential threats, extended multi-vendor support, and 24x7 coverage through an integrated security operations center (SOC).

Like other large refining operations, STAR Refinery was seeking an enhanced cybersecurity posture by bringing its ICS and PCN in-line with global industry standards. Refinery management consulted with Honeywell's cybersecurity experts on the counter-measures needed to elevate the refinery to the next level of cyber assurance and requested Honeywell's support to drive towards this objective.

In particular, the STAR Refinery was looking for on-premise solution supported by cloud-based managed security services to provide secure remote access and visibility of OT assets.

Honeywell offers an end-to-end solution intended to protect mission-critical OT assets. Recognized experts in industrial cybersecurity deliver these comprehensive services. They help to minimize the risk of severe operational, financial and reputational damage—enabling customers to overcome the limitations of traditional cybersecurity in an industrial setting.

With Honeywell Forge Managed Security Services (MSS), industrial organizations are empowered with intelligent, seamless protection across the expanding attack surface of their ICS and PCN. This solution delivers deep cybersecurity know-how to address the visibility, availability and reliability necessary for OT performance, whether in networked, application, cloud, or mobile environments.

Honeywell Forge Managed Security Services incorporates a host of core services intended to increase cyber resilience, expedite risk mitigation, improve recovery time, and improve safety records. They include:

- Honeywell's Secure Connection featuring encrypted communication to protect data
- Automated patching and anti-malware services to ensure all computers are updated with the latest security protections
- Continuous monitoring and alerting services to monitor the performance and health of the PCN
- Intelligent reporting services to transform system statistics into actionable trends

With Honeywell's MSS solution, STAR Refinery's OT assets are better managed and constantly kept up to date. An authenticated and encrypted virtual private network (VPN) enables Honeywell's dedicated support engineers and subject matter specialists to remotely troubleshoot security and maintenance issues.

CUSTOMER BENEFITS

Honeywell is committed to providing the next level of enterprise-wide cybersecurity to industrial organizations worldwide. Its MSS offering helps customers achieve global threat visibility and effective threat management; consistent, repeatable and measurable processes; a greater understanding of vulnerabilities and threat actors; improved customer skills transfer and quality staff retention; and predictable security cost models.

The most significant benefit of Honeywell's MSS solution is access to experienced cybersecurity professionals, across a wide range of disciplines, using advanced security technology, at a much lower cost than an on-premise security operations capability.

At the STAR Refinery, Honeywell's cybersecurity services:

- Reduced the risk of security breaches
- Helped to manage the security posture of process control infrastructure
- Provided 24/7 monitoring and alerting of the PCN, including controllers, servers and workstations
- Delivered intelligence reporting services to transform system statistics to actionable trends

With Honeywell's assistance, the STAR Refinery gained better control over its OT environment in terms of visibility, connectivity, reporting, and monitoring. The MSS solution provided secure remote access and enterprise visibility of OT-related work without the need for employees on site. This approach saved time for both customer engineers and contractors, who are now able to complete their required assignments faster than usual. GTAC remote access and support further reduced the need for onsite personnel. Engineers working from home has become the default practice, with site work reserved for emergencies and on-demand activities only. Reporting tasks and AV management have also become much easier.

SUMMARY

Honeywell's Industrial Cybersecurity Solutions help the process industry and critical infrastructure sectors defend the availability, reliability and safety of their plant operations.

Honeywell's suite of MSS solutions has helped the STAR Refinery secure the various aspects of its ICS/OT environment. This has ultimately contributed to improved uptime, stability, reliability, and safety for the complex refinery operation.

ABOUT HONEYWELL FORGE'S MANAGED INDUSTRIAL CYBERSECURITY SERVICES

Around the world, industrial firms and critical infrastructure operators' partner with Honeywell Forge to address the unique requirements of cybersecurity in process control environments. Honeywell Forge's broad expertise encompasses automation assets and their integrated communication networks – a distinct advantage in control system security.

Our services include:

SECURE REMOTE ACCESS AND SUPPORT

ACTIVITY AND TREND REPORTING

SECURITY AND PERFORMANCE MONITORING

ADVANCED MONITORING AND INCIDENT RESPONSE

PATCH AND ANTIVIRUS AUTOMATION AND MANAGEMENT

For more information

Learn more about how Honeywell Forge Managed Security Services can improve performance, visit www.becybersecure.com or contact your Honeywell Account Manager, Distributor or System Integrator.

Honeywell Connected Enterprise
715 Peachtree Street NE
Atlanta, GA 30308, USA

Honeywell Process Solutions
1250 West Sam Houston Parkway
S. Houston, TX 77042, USA

Honeywell House, Arlington Business Park
Bracknell, Berkshire, England RG12 1EB UK

Shanghai City Centre, 100 Zunyi Road
Shanghai, China 200051

www.honeywellprocess.com

MSS CS ENG | Rev 1 | 01/2021

THE FUTURE IS WHAT WE MAKE IT

Honeywell