HONEYWELL FORGE

# PUMPING UP SECURITY

## Oil and Gas Company trusts Honeywell to Increase OT Cybersecurity Resilience and Reduce Cyber Risk

Case Study

## BREAKING THROUGH THE BEDROCK

Many industrial organizations lack the staff, budget and skills to manage cyber threats proactively and may have limited visibility into industrial control system (ICS) assets. With so many potential threats to these assets, prioritization is a challenge. However, it's recommended that plant operators understand the importance of continuous monitoring of operational technology (OT) assets. Oil and gas companies that want to prioritize the ongoing protection of ICS environments may be unable to identify threats because there is too much "background noise" from the number of security events and types of data.

A Honeywell oil and gas customer wanted to implement a two-pronged approach with a cybersecurity assessment and strategy implementation to improve the safety of its control system, meet compliance requirements and better secure the connections required for smooth operations and enhanced performance.

For industrial organizations like this oil and gas company, a successful cyber-attack may result in operational shutdowns, damaged equipment, financial loss, intellectual property theft, and substantial health and safety risks. As such, it is imperative that they monitor the right data sets to build an effective threat defense and improve their overall security posture.

The customer's specific cybersecurity requirements included:

- Industrial-grade secure remote access
- Improved security for content and data transfer
- Patch and antivirus management
- Comprehensive assessment and audit
- Managed threat detection
- 24/7/365 monitoring
- Threat alerts and reporting
- Incident investigation
- Log collection and analysis
- Increased remote monitoring support

## ASSESSING THE RISK

After the consultation between the customer and Honeywell, the customer decided to pursue a comprehensive solution that included:

- Security consulting services – assessments and audits
- Managed security services – patch and antivirus management
- Advanced monitoring and incident response (AMIR)

Honeywell started the two-pronged cybersecurity approach with an assessment and audit of the customer's existing OT environment to determine any gaps in their security coverage and plan a roadmap for an improved overall cybersecurity posture. The end-to-end AMIR solution operated as the brain of the OT cybersecurity program by collecting and analyzing event log data 24x7 from multiple sources, including firewalls, intrusion detection system/intrusion prevention system, routers, switches, Windows, Linux, the Honeywell process control system, and other lower-level ICS assets. AMIR proactively automated and orchestrated the detection of suspicious and anomalous behavior across the customer's ICS assets. If a cybersecurity event were detected, AMIR would notify Honeywell cybersecurity consultants a deeper forensic investigative analysis is necessary. Once the analysis is complete, the customer would have received a detailed security incident report on the event, which offers threat insights to help them oversee and better protect crucial OT assets.

## FROM THE GROUND UP

After receiving the final overall report, the oil and gas customer was able to accelerate and operationalize its OT/ICS incident detection and respond without the need to implement its own premise-based security technologies. The proactive monitoring that the customer gained from AMIR for suspicious behavior or indicators of compromise will increase the likelihood of detecting potential threats and significantly reduce the severity of the impact.

By utilizing the AMIR service, the oil and gas company can:

- Identify, mitigate and manage a wide range of cyber threats
- Monitor critical ICS assets continuously
- Proactively analyze, investigate and identify malicious activity
- Increase threat visibility and awareness
- Collect threat-related data from a range of assets
- Detect signs of compromise before an incident happens
- Better prevent future attacks and minimize overall risk
- Understand vulnerabilities and priorities
- Augment in-house expertise
- Lower the cost of security operations

Honeywell provided the oil and gas company with a 24/7 "eyes-on-glass" cybersecurity monitoring and incident response. The use of incident response automation is key to expediting typical responses and repetitive tasks, so minimal human intervention is required to detect and respond to security threats and incidents.

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