CASE STUDY

Cyber Hardening for a Critical Subsea Production Unit

Executive Summary

The customer presented HMH with a unique challenge: securing a legacy control system originally delivered by another vendor. This project represented a strategic step beyond HMH's core systems, showcasing the flexibility and depth of our cybersecurity capabilities.

This control system plays a critical role in the daily operations of this specific rig, making its reliability and security non-negotiable. However, the state of the system posed a significant risk. It was built on outdated hardware, legacy software, and operating systems that had long surpassed their lifecycle. These components no longer complied with modern cybersecurity standards, leaving the system vulnerable to threats that could compromise both safety and production. Securing this system was therefore not just a technical requirement, it was essential for maintaining operational integrity and protecting the rig from potential disruptions or breaches.

Through multiple upgrades of complete drilling control systems, HMH has consistently demonstrated its strong expertise in OT systems and cybersecurity. Rather than designing a solution internally, the customer entrusted HMH to assess the existing installation and propose a comprehensive solution.

HMH Solution

Our team designed and delivered a robust cybersecurity upgrade comprised of:

- Multiple secure virtual servers
- Advanced Intrusion Prevention System (IPS)
- Antimalware technology with application whitelisting, lockdown functionality, and USB port locking

Overview

Objective

Enhance the cybersecurity posture of a legacy subsea production control system operating on outdated hardware and software.

Challenges

Obsolete components lacking modern security standards, high operational risk, and the need to secure third-party integrations without disrupting critical operations.

Solution

Delivered a comprehensive cybersecurity upgrade using virtual servers, IPS, antimalware with whitelisting, secure documentation, and coordinated offshore installation, resulting in a fully secured and modernized system.

Onshore Scope

Security Management Server

Delivery of a pre-configured virtual appliance (Linux-based), hosted in the client's virtual environment for centralized security orchestration.

Engineering Workstation (EWS)

Delivery of a pre-hardened virtual Windows Server, engineered for security operations.

IPS Configuration

Pre-configured to secure network traffic between operator firewalls and third-party devices.

Documentation

Complete network topology drawings, zone and conduit documentation, and customer specific mark-ups.

Licensing

Delivery and management of antivirus/antimalware and IPS licenses, including ongoing support and prepared for upgrades through HMH SecureOPS services.

Offshore Scope

Physical Installation

Site installation of IPS modules, in full coordination with customer facility teams and adherence to safety protocols.

Software Deployment

Installation of antivirus and whitelisting solutions on client assets.

Network Configuration

Secure integration of security appliances during scheduled maintenance windows. Full routing of current legacy network through IPS system.

Intelligent Learning Mode

After installation, all systems operated in a "learning mode" for at least 7 days to analyze real-world traffic patterns, ensuring a smooth transition to protected status and minimizing operational disruption.

Downtime

Limited downtime was required for the installation.

Result

The entire secure system was engineered, configured, delivered, and fully installed within three months, on time and in line with customer expectations.