CASE STUDY: SECURING OPERATIONAL TECHNOLOGY AT AN OIL AND GAS OFFSHORE

Safeguarding Industry 4.0

Securing the future of tomorrow

Securing Operational Technology at an Oil and Gas Offshore

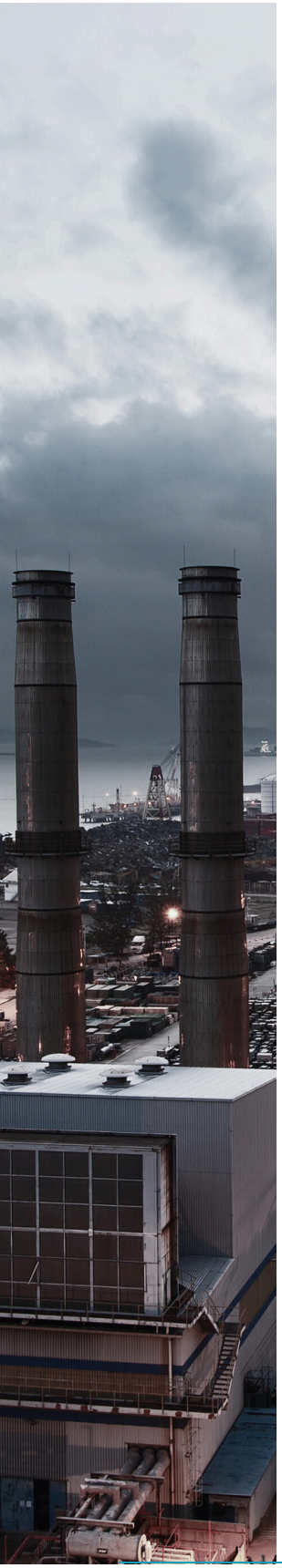
Overview

An offshore oil and gas responsible for drilling, extraction, and initial processing of oil and gas sought DTS's assistance to enhance the security of their Operational Technology (OT) systems. The operates several critical systems, including drilling control systems, blowout preventers (BOPs), gas detection systems, and pipeline monitoring systems. These systems rely on Supervisory Control and Data Acquisition (SCADA), Programmable Logic Controllers (PLCs), and Distributed Control Systems (DCS) for real-time monitoring and control of the operations.

Given the harsh environment and critical nature of offshore operations, the offshore platform faces increased risks from cyberattacks targeting its OT systems, which could result in catastrophic failures, environmental damage, and safety risks to personnel. Additionally, the platform must comply with industry standards such as NIST, IEC 62443, and NERC CIP to ensure the safety and security of its operations.

The client's objective was to develop a cybersecurity strategy that would ensure secure communication between OT systems, provide real-time threat detection, and protect critical assets from both internal and external cyber threats. DTS was tasked with providing a comprehensive cybersecurity architecture tailored to the offshore operational needs.

Challenges



Legacy Control Systems

The offshore platform relied on outdated PLCs and DCS that were vulnerable to cyberattacks due to their lack of modern cybersecurity measures. These systems controlled essential processes like drilling operations and blowout preventers, making them prime targets for cybercriminals.

Vulnerability in Blowout Preventers (BOPs) and Drilling Control Systems

The BOPs and drilling systems were directly connected to the offshore SCADA network. The lack of sufficient network segmentation made these critical systems highly susceptible to cyberattacks that could manipulate operational data, leading to catastrophic drilling failures or oil spills.

Remote Access Risks from Third-Party Vendors

The offshore reliance on third-party vendors for maintenance and support of its OT systems meant that external parties had remote access to sensitive control systems. This posed a significant risk if their access credentials were compromised or if vendors inadvertently introduced malware.

Limited Visibility into OT Environment

The lack of comprehensive monitoring tools and visibility into the status of the offshore OT systems made it difficult to detect and respond to potential threats in real time. This gap in visibility increased the risk of delayed detection of critical system anomalies or cyber intrusions.

Compliance with Industry Standards

The offshore was not fully compliant with key cybersecurity standards, such as NIST, IEC 62443, and NERC CIP. This non-compliance exposed the offshore to potential legal penalties, safety risks, and operational disruptions due to regulatory audits or cybersecurity breaches.

List of asset systems typically found in an oil and gas offshore platform:

- SCADA System (Supervisory Control and Data Acquisition)
- PLC Systems (Programmable Logic Controllers)
- Subsea Control Systems
- HVAC Systems (Heating, Ventilation, and Air Conditioning)
- CCTV and Physical Security Systems
- Data Historian Systems
- Hydraulic Systems
- Maintenance and Asset Management Systems
- Blowout Preventers (BOPs)
- Drilling Control Systems
- Drill Monitoring and Data Acquisition Systems
- Wellhead Control Systems
- Pipeline Monitoring and Control Systems
- Vibration Monitoring Systems
- Fire and Gas Detection Systems
- Environmental Monitoring Systems (Gas Leak, Temperature, and Pressure Sensors)
- Safety Shutdown Systems
- Power Distribution and Control Systems

List of asset systems typically found in an oil and gas offshore platform:

- Pipeline Monitoring and Control Systems
- Vibration Monitoring Systems
- Fire and Gas Detection Systems
- Environmental Monitoring Systems (Gas Leak, Temperature, and Pressure Sensors)
- Safety Shutdown Systems
- Power Distribution and Control Systems
- Energy Management Systems (EMS)
- Tank and Storage Management Systems
- Communication Networks (Satellite, Radio, Fiber Optic)
- Remote Monitoring and Telemetry Systems
- Chemical Injection and Dosing Systems

Approach / Methodology

1. Assessment and Gap Analysis

Conducted a comprehensive cybersecurity risk assessment of the offshore OT environment.
Identified legacy systems (PLCs, DCS, SCADA) and their vulnerabilities.
Mapped communication flows and third-party remote access paths.
Assessed the compliance posture against NIST, IEC 62443, and DoE standards.

2. Asset Identification and Criticality Mapping

Created an inventory of all critical systems: BOPs, drilling systems, pipeline monitoring, fire and gas detection, etc.
Prioritized systems based on risk impact, operational importance, and connectivity.
Evaluated exposure of each system to recent threat vectors (e.g., phishing, MITM attacks, DoS, malware).

3. Network Segmentation and Access Control

Implemented strict network segmentation between IT and OT networks.
Introduced demilitarized zones (DMZs) for secure vendor access and monitoring interfaces.
Enforced role-based access control (RBAC) and multi-factor authentication (MFA) for all remote connections.
Include Secure VPN and PAM solution for remote diagnosis.

4. Real-time Monitoring and Threat Detection

Deployed OT-aware threat detection tools for continuous monitoring.
Integrated Security Information and Event Management (SIEM) for anomaly detection and incident correlation.
Enabled logging and alerting for unauthorized access and suspicious activities.

5. Vulnerability Management and System Hardening

Applied patches and firmware updates to legacy systems where possible.
Disabled unused services and hardened configurations based on baseline security templates.
Deployed endpoint protection tools to mitigate malware and ransomware threats.

6. Incident Response and Recovery Planning

Developed and tested a dedicated OT incident response plan tailored to offshore operations.
Simulated attack scenarios involving safety shutdowns, drilling system compromise, and gas leak tampering.
Integrated backup and recovery mechanisms with isolated offline storage.

7. Compliance and Policy Alignment

Mapped implemented controls to meet compliance with IEC 62443 zones and conduits model.
Created OT cybersecurity policies and procedures aligned with DoE and IEC 62443 standards.
Conducted periodic audits and assessments to maintain regulatory readiness.

8. Training and Awareness

Conducted security awareness training for operators and engineers.
Provided tabletop exercises and drills involving cyber-physical attack scenarios.
Established a continuous learning program to keep staff informed of evolving threats.

Safeguarding Industry 4.0

CS4 – Cybersecurity for Industry 4.0, a specialized division within DTS Solution, excels in Operational Technology (OT) cybersecurity. With over 15 years of experience safeguarding OT environments across various sectors, CS4 empowers asset owners by enhancing cyber resilience and maturity within their operating environments.

Our Mission

We are dedicated to fortifying industrial operations with advanced cyber defense and comprehensive security programs. Our proactive approach to risk management and threat neutralization ensures that your Industry 4.0 infrastructure operates with resilience and reliability at its core.

Our Services

OT Cybersecurity Advisory & Consulting Services
We provide expert guidance to navigate the complexities of OT security, ensuring compliance and resilience in your critical systems.

OT Cyber Defense and Engineering
Our proactive cyber defense solutions are designed to detect, prevent, and respond to threats targeting your OT environment.

OT Managed Security Services
Through our HawkEye OT platform, we offer centralized monitoring, incident response, and threat hunting to protect your critical infrastructure from cyber threats.

Our Approach

At CS4, we prioritize a process-aware approach to cybersecurity, ensuring that your industrial environment is not only secure but also future-ready. We collaborate closely with asset owners, system integrators, and product suppliers to develop secure control systems and software, fortifying all aspects of your operations against evolving threats.

Partner with CS4 to secure your Industry 4.0 infrastructure and achieve unparalleled cyber resilience in your industrial operations.