CASE STUDY

Securing an Offshore Oil-Drilling Rig in the North Sea

OVERVIEW

Sometimes the main challenge in landing a project to secure an industrial location is… physically landing at the location.

Offshore oil drilling is one of the most lucrative segments in the energy sector, and is expected to increase its market share as new reserves are discovered and new technologies for deep-water drilling emerge (CAGR of 8.3% during the period 2019-2023, according to market researcher Technavio).

The Offshore Oil Drilling industry still operates under the shadow of the 2010 BP Deep Horizon oil spill and the subsequent ecological disaster, and has been subject to scrutiny over security concerns, both physical and cyber.

Needless to say, offshore oil drilling rigs are still very much associated with the infamous 2010 BP Deep Horizon leak and the subsequent ecological disaster that have generated great awareness and scrutiny over the entire industry. This scrutiny and the demand for stricter security measures (physical and cyber) were part of the incentive to harden the cyber-security of the rig.

The offshore drilling cluster of under a dozen rigs described herein is located about 150 km off-shore, and is accessible only by weather-permitted helicopter flight.

Communication with the mainland is limited to low-throughput satellite and RF communications.

The rig is regularly staffed by a few dozen employees.

WINNING THE PROJECT

Radiflow was introduced to, and eventually won the project through its local partner, based on previous successful Radiflow deployments in the energy sector.

The main incentives to install IDSs were preventing breaches into the OT network; gaining visibility into the network and all assets, including access to each asset's status and properties; and achieving compliance with the presiding standards and regulations.

Prior to installing the Radiflow system, cyber-defense of the rig relied solely on a firewall.

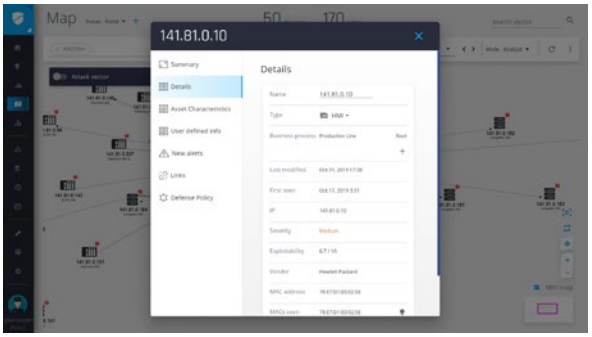
The iSID Industrial Threat Detection System installed at the oil rig goes beyond merely detecting breach attempts, with invaluable asset management features and insights for hardening the OT network.

SCOPE OF THE PROJECT

The first stage of the project called for installing Radiflow's iSID Intrusion Detection System at one of the rigs in the cluster, with the intention to do the same in the rest of the rigs (as the project grows with multiple instances of iSID, the client will be able to monitor and manage of the entire array of iSID systems through the Radiflow iCEN Central Management Solution.)

For this project, iSID was tasked with providing full visibility into the OT network, detection of attempted attacks and access violations, management of maintenance activities and monitoring of logic changes on controllers.

In addition, the Radiflow system provides operators with tools and insights for risk assessment and mitigation, for eliminating vulnerabilities and optimizing mitigation measures.



iSID enables drilling down to each assets properties, including logic version, alerts, defense policy and more.

Upon detecting anomalies, iSID would relay alerts to the company's SCADA system using Radiflow's OT protocols northbound interface. This enables the personnel at the operating room to be aware on any anomaly in their network or cyber and operation incidents through the SCADA system interface.

CHALLENGES

As mentioned, the main challenge of the project was physically accessing the site. This required Radiflow's local partner to diligently plan and stage the iSID system on terra firma prior to installation, and unsurprisingly, the installation took place smoothly. From then on, configurations were done remotely, in tight collaboration between the local partner, the Radiflow team, and the client.

CURRENT STATUS

At present, iSID is fully operational at the oil rig. It has already detected vulnerabilities and misconfigured PLCs in the rig's OT network and has issued recommendations for remediation.

The operator's information security staff has been trained on operating iSID (at the operator's premises).

Following a few upgrades and adjustments to the system, it is expected that the next phase of installing iSID at additional rigs will be green-lighted soon.

iSID network visualization map provides operators a clear understanding of the logical placement of assets in the OT network

ABOUT RADIFLOW

Radiflow develops trusted Industrial Cyber-Security Solutions for Critical Business Operations. Our portfolio of game-changing solutions for ISC/SCADA networks empowers users to maintain visibility and control of their OT networks. Our intelligent Threat Detection and Analysis Platform for industrial cyber-security minimizes potential business interruption and loss within your OT environment.

Radiflow's team consists of professionals from diverse backgrounds, from cyber-experts from elite military units and automation experts from global cyber-security vendors. Founded in 2009, Radiflow' solutions, are successfully deployed by major industrial enterprises and utilities protecting more than 3,000 critical facilities worldwide. More at www.radiflow.com.

US and Canada:
Tel: +1 (302) 547-6839
sales_NA@radiflow.com

EMEA:
Tel: +972 (77) 501-2702
sales@radiflow.com

UK:
Tel: +44 (0) 800 246-1963
sales_UK@radiflow.com

France:
Tel : +33 1 77 47 87 25
sales_FR@radiflow.com

DACH:
Tel: +49 (160) 109 75 65
sales_DACH@radiflow.com