FORESCOUT

Case Study

Oil & Gas Company Implements OT Network Monitoring to Reduce Cyber and Operational Risk

To help identify risk and mitigate to an acceptable level, the company deployed SilentDefense to understand what was on the OT network and to be able to quickly identify threats and vulnerabilities.

Customer Profile

This oil & gas company is an industry leader in the offshore drilling industry. It operates one of the largest, high quality rig fleets in the world and is among the most technologically advanced in the industry. They are committed to safety and operational excellence, with a focus on technology and innovation.

The Challenge

With quantifying and mitigating cyber and operational risk now becoming a top priority, oil & gas asset owners must craft long term risk reduction strategies. The team quickly recognized that the first step towards reducing risk was to identify and review potential vulnerabilities on critical systems offshore. In order to mitigate operational and safety risk, it was critical to fully understand the type of threats and their origin.

The first initiative centered around finding and training qualified people to map the network and establish a strategy to protect it. This operational technology (OT) cybersecurity team was tasked with identifying all the existing assets in the network and assessing what the risk levels were. However, this manual process was an enormous task, and the team needed an alternative approach. This original initiative risked taking a considerable amount of time, and threats could go unnoticed in such a vast operation connecting multiple oil rigs and offices around the world during that time.

The Project

To help automate and accelerate the process of mapping the network, the team decided that implementing an OT network monitoring tool was the alternative approach they needed. Although deploying this type of technology is widely used in the utility industry, it's still relatively uncommon in drilling, but the company was determined to make it happen. Centralized oversight was required for such an expansive and complicated network. The right solution would be able to keep track of all the devices connected to the network, identify any deviations in the normal baseline of network traffic, and archive the data for future reference.

The Solution

When SilentDefense was deployed during the proof of concept (PoC), the results provided an initial understanding of how deploying an OT network monitoring tool could help them reach the goal of deeper visibility to reduce cyber and operational risk. The PoC also exposed the challenges of deploying newer technology on legacy systems, which proved vital in providing an accurate budget for the project.

During this project, the company was not just architecting for one control system, multiple control systems throughout the global fleet required monitoring. Everything from the blow out preventer (BOP) to the dynamic propulsion systems (DPS) had to be monitored. Since it was not practical to have a sensor on every system, the hardware was strategically placed on choke points in the vessel's network.

The company ultimately chose Forescout SilentDefense over others because its proven and turnkey solution more accurately identified assets on the network, was the easiest to use, and didn't require new infrastructure to get it up and running. Forescout's approach also felt like more of a business partnership, rather than a traditional vendor relationship.

Main Results

- Visibility into process data and identification of previously unknown assets, which laid the foundation for implementing an in-depth gap assessment
- Quick identification of cyber risks like the presence of vulnerabilities on a specific device and operational risks like out of range process values
- Automated data gathering, including detailed reports on network traffic anomalies, for real-time analysis by the cybersecurity team

Other resources that might be interesting to you:

- Web Page: Cybersecurity for the Oil & Gas Industry
- Solution Brief: Securing Vulnerable ICS and OT Networks
- eBook: How to Effectively Implement ISA 99/IEC 62443

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com