CYDOME

Case Study

OIL & GAS MARITIME CYBER RISKS
TANKERS SHIPPING COMPANY IMPLEMENTS CYDOME TO REDUCE MARITIME CYBER RISKS

The company deployed Cydome's solution to understand what was onboard its tanker and identify its cyber risks.

CUSTOMER PROFILE

This shipping company operates a fleet of tankers for the shipping of oil & gas and is committed to safety and operational excellence, with a focus on technology and innovation.

THE CHALLENGE

With the increase in cyber crime at the maritime industry and the maritime cybersecurity regulations (IMO 2021 guidelines and TMSA3) in effect as to cyber security implementation- assessing, measuring and mitigating cyber threats has become top priority. Shipping companies responsible for the transfer of oil & gas are required to embed cyber security solutions and craft policies and strategies to reduce the risks.

As a first step towards reducing risk - it was clear that an identification and review of all such potential vulnerabilities on the assets onboard the tanker is required. Next step designed to support mitigation of both operational and safety risk was to fully understand the type of threats and their origin.

THE SOLUTION

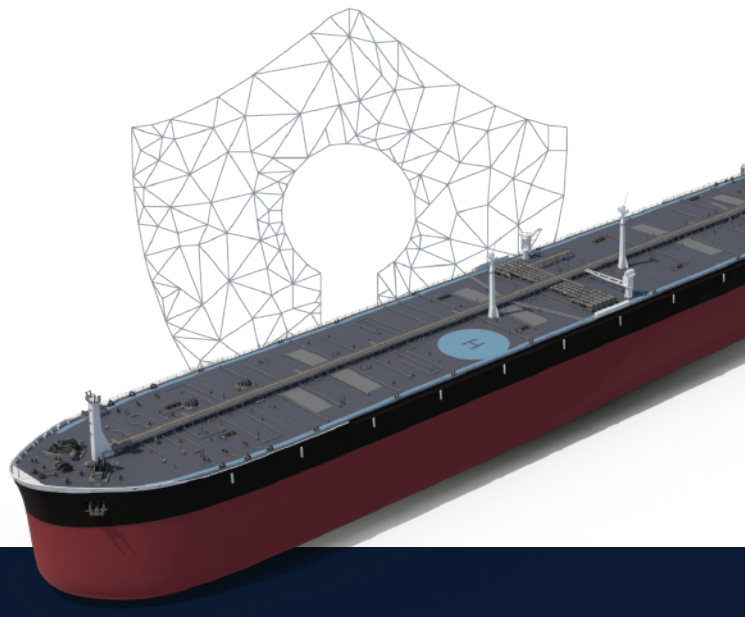
Upon deployment of Cydome's solution, the results provided a clear understanding of all existing assets in the network and an assessment of what are the risk levels. The results were already visible for demonstration within two weeks after deployment. Once the Solution completed the identification and mapping stage of all devices connected to the network it continued to identify any deviations in the normal baseline of network traffic, and archived the data for future reference.

The centralized fleet management solution provided a deeper visibility onboard the tanker - including full scope asset mapping, vulnerability scanning clearly identified with their severity level, real-time alerting of cyber threats with a recommendation for remediation, all to reduce cyber and operational risk.

THE PROJECT

The first stage of the project focused on automatic identification of all the existing assets in the network and assessing what the risk levels were. Conducting such full scope assessment in a manual process would have been an enormous task.
The second stage included the implementation of a real-time monitoring solution of the assets connected to the network with an automated, built-in cybersecurity check-up (vulnerability scan).

Shipping companies responsible for the transfer of oil & gas are required to embed cyber security solutions and craft policies and strategies to reduce the risks.
As a first step towards reducing risk - it was clear that an identification and review of all such potential vulnerabilities on the assets onboard the tanker is required. Next step designed to support mitigation of both operational and safety risk was to fully understand the type of threats and their origin.



MAIN RESULTS

- Visibility into current assets onboard the tanker and all such network identification including unknown assets, such as Unpatched & End-of-Life systems detected and Weak and default credentials detected on critical assets.
- Quick identification of cyber risks with its continuous vulnerability scanning, including unauthorized/3rd parties access detection and lack of segregation on the network, such as Multiple VLAN Network segregation breaches and OT Segregation breach.
- Real-time detection and monitoring of cyber threats with better cyber security reporting and embedded scoring to be demonstrated for the TMSA and IMO 2021 regulation.

The company ultimately chose Cydome's solution based on evident full scope analysis, a self deployed solution effectively reducing cyber risks. And got great feedback from the team using the Solution on its monitoring ease of use together with the supporting tools and reports ready to be used for maritime regulation demonstration.