

Fleet-Wide Maritime OT Cybersecurity for a Leading European Dredging Operator

Solution: OT Security Platform | Industry: Maritime | Location: Europe

AT A GLANCE

The mission

- Meet the IACS UR E26/E27 maritime cybersecurity requirements.
- Secure onboard OT systems against rising threats.
- Run safe, fleet-wide cyber operations.

The solution

- Radiflow platform deployed across the fleet.
- Onboard monitoring with centralised shore visibility.
- Overlapping networks resolved, built for low connectivity.
- Visual alerts and playbooks for crew response.

The impact

- Achieved full fleet OT visibility and compliance.
- Protection maintained with low or no connectivity.
- Faster, clearer crew response to OT alerts.

BACKGROUND

A leading European dredging operator needed fleet-wide OT cybersecurity aligned to IACS UR E26/E27, across vessels with overlapping networks and intermittent satellite connectivity.

01 THE CHALLENGE

What stood in the way.

Overlapping network subnets

Vendor restrictions prevent standardised IP addressing, so multiple systems run on identical subnet ranges.

Limited connectivity at sea

Vessels often operate on intermittent or low-bandwidth satellite connections.

Non-specialist crew

Onboard personnel needed simple, clear alerts that require no cybersecurity expertise.

Fleet-wide visibility

Centralised monitoring was needed across geographically dispersed vessels.

02 THE SOLUTION

How Radiflow solved it.



iSID The sensor

Passive monitoring on each vessel. Maps every device, learns normal behaviour and flags known threats (CVEs) and anomalies, acting as the onboard alerting system for the crew



vSAP The virtual collector

Tags traffic with unique identifiers via GRE tunnelling, so iSID can tell apart devices with identical IP addresses and build a full inventory despite clashing L2-L4 addressing.



iCEN The console

One consolidated view of every vessel for the shore-based SOC: alerts, assets and health, wherever the ship is.



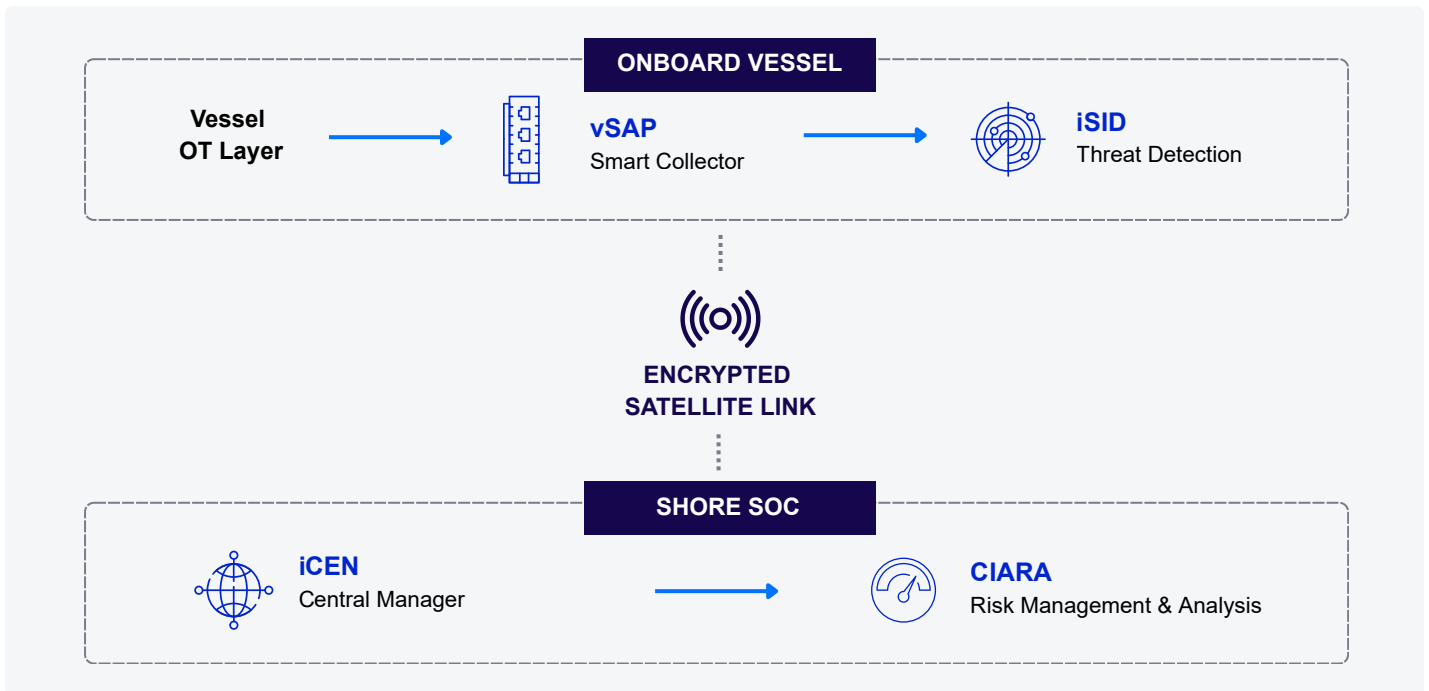
CIARA The risk engine

Risk assessment and attack simulation that maps likely attack paths using MITRE ATT&CK, and shows what to fix first.



03 THE ARCHITECTURE

How it fits together.



04 THE IMPACT

What changed.

The operator now has complete OT visibility across its fleet, and a platform built for the connectivity and operational realities of life at sea. iSID shows the team what is on each vessel's network; CIARA tells them what to fix first.

Autonomous onboard operation, combined with bandwidth-efficient synchronisation, keeps every vessel protected whether it is docked or working in remote waters.

WHY RADIFLOW

- The only OT platform purpose-built for maritime connectivity constraints
- Solves the overlapping IP challenge without network reconfiguration
- Operates fully offline with no cloud dependency
- IACS E26/E27 compliance built in, using the same engine as IEC 62443
- Crew playbooks enable effective response with no cybersecurity expertise required onboard

Radiflow

Radiflow develops OT security and risk management solutions that ensure operational resilience and compliance, and optimise cybersecurity expenditure while minimising risk. One platform, fully passive and fully on premise, deployable locally or centrally and integrated with leading technology partner platforms. Radiflow protects more than 20,000 sites worldwide.