Maritime Cybersecurity

Protecting the Critical Infrestructure
Of the Maritime Sector

Global Context

The Cyber Threat Landscape

900% increase in cyberattacks

Cyberattacks targeting the maritime sector have multiplied over the past three years.

Source: IBM Cost of a Data Breach Report 2024

Transport Sector: #2

ENISA ranks the transport sector as the second most targeted sector in Europe.

Source: ENISA Threat Landscape 2024

State-sponsored Actors

APT28, APT35 and Chinese threat groups are intensifying attacks against strategic European ports.

Source: NATO/CCDCOE 2025

287 Days

Average time to detect a breach in maritime OT systems.

Source: Lloyd's sector reports

Risk Assessment

Critical Onboard Vulnerabilities

Navigation Systems

GPS, ECDIS and AIS are vulnerable to spoofing and jamming. Dynamic Positioning (DP) systems are also targets.

Risk: CRÍTICAL

Communications

VHF, satellite communications, maritime email and GMDSS systems can be intercepted.

Risk: HIGH

Onboard Power and Propulsion Control

Power Mangement Systems (PMS) controlling propulsion and generators can be compromised.

Risk: CRÍTICAL

Cargo Management Systems

Cargo management systems control vessel stability, ballast operations, and port cargo handling.

Risk: HIGH

Critical Infrastructure

Risks in Port Infrastructure

Port Automation

AGV cranes, automated cargo-handling systems and autonomous vehicles rely on industrial networks.

⚠ Impact: €50M/day

Integrated Control Centers

Port Control Centers (PCC) integrate operations, security, customs and financial management.

⚠ Impact: Cross-sector

SCADA/ICS

Terminal Operating Systems (TOS) manage the global supply chain.

⚠ Impact: National Security

Documented Cases: Port of Barcelona (2023), Port of Los Angeles (2022), oil terminals in Germany and the Netherlands (2022). Total losses exceed $6B annually.

Legal Obligations

Regulatory Framework and Compliance

ISO 27001

International Security Standard

International standard for Information Security Management Systems (ISMS). It defines the requirements to establish, implement, maintain, and continually improve information security within an organization.

- Required for public sector contracts
- International reference framework
- Continuous improvement cycle

Globally recognized certification

IACS Requirements

E26 and E27 - 2024

As of July 1, 2024, new shipbuildings must comply with the IACS Unified Requirements:

- They focus on the cyber resilience of integrated onboard systems, from navigation to propulsion.
- They cover the design, construction, commissioning, and operational lifecycle of the vessel.
- They are based on five core functions: Identify, Protect, Detect, Respond, and Recover.

International Maritime Regulation

IMO Guidelines

Cybersecurity for Ships and Port Facilities

These guidelines provide internationally recognized best practices to enhance cybersecurity in maritime operations, covering ships and port facilities.

- Risk & Governance: Identify and manage vulnerabilities.
- Technical Measures: Protect networks and onboard systems.
- Incident Response: Detect, respond, and recover from cyber incidents.

International Maritime Regulation

Holistic Approach

Our End-to-End Solution

01 Risk Assesment

Comprehensive analysis of technical and organizational vulnerabilities in vessels and port infrastructure, with zero false positives.

02 AI-Driven Penetration Testing

Controlled attack simulations powered by proprietary artificial intelligence and the deployment of digital twins for critical environments.

03 Training

Specific training programs for crews and port personnel.

04 24/7 Monitoring

Specialized SOC with real-time threat detection.

05 Incident Response

Rapid-response team with protocols specific to maritime environments.

06 ISO 27001

Development and implementation of an ISMS adapted to the maritime environment.

100%
Regulatory Compliance

24/7
Monitoring

Real-time
Response

Unique Synergy

Strategic Alliance of Experts

Altum Ingeniería y Servicios

Naval Engineering

- Over 20 years of experience in naval engineering and maritime consulting.
- Experts in conducting risk analyses in maritime environments.
- Services for shipowners, shipyards, and port facilities.

Offices: Huelva & Madrid

Hermes Security

Cybersecurity + AI

- Innovative startup at BIC Euronova
- Custom AI that detects security vulnerabilities
- Predictive attack simulation using digital twins

Offices: Málaga & Huelva

Objetivo 17

Strategic Consulting

- Over 30 years of experience in key sectors
- Integration of ISO 27001 with compliance
- Global network of international partners

Office: Madrid

Proven Track Record

Our Clients

+50
Maritime Projects

+20
Years of Experience

100%
Satisfied Clients

- Navantia
- Puerto de Huelva
- Freire Shipyard
- SPC Spain
- Astilleros Armón
- Baleària
- Guardia Civil
- Silversun
- Acciona
- Moody's
- Gobierno de Islandia
- OVHcloud
- Alibaba Cloud
- BMW

Why Choose Us?

Unique Value Proposition

Industry-Leading Expertise

We uniquely combine deep naval engineering knowledge with predictive offensive cybersecurity excellence.

A key differentiator compared to generic consulting firms

In-House Artificial Intelligence

Our AI makes autonomous decisions and identifies security flaws by replicating the behavior of a human hacker.

Built from scratch by our team

Predictive Simulation

Exclusive technology to simulate attacks in virtual environments identical to the real ones, without impacting production systems.

Cutting-edge technology | Digital Twin

Comprehensive Compliance

We don't just comply with ISO 27001 and IACS—we integrate all requirements into a single, effective solution.

One partner for all regulations

The Smart Choice for Any Sector

Resource optimization, full transparency, and measurable results from day one.

Advanced Maritime Cybersecurity

Protecting Our Seas Together

Altum Ingeniería y Servicios

Daniel Santos

+34 959 283 295

daniel.santos@altum-marine.com

altum-marine.com

Hermes Security

Cristian Mateo

+34 621 373 780

cristian.mateo@hermesecurity.com

hermesecurity.com

Objetivo 17

Víctor Manuel Fuertes

+34 638 056 821

direccion@objetivo17.com

objetivo17.com

The security of our critical maritime infrastructure is everyone´s responsibility.

We are ready to support you.