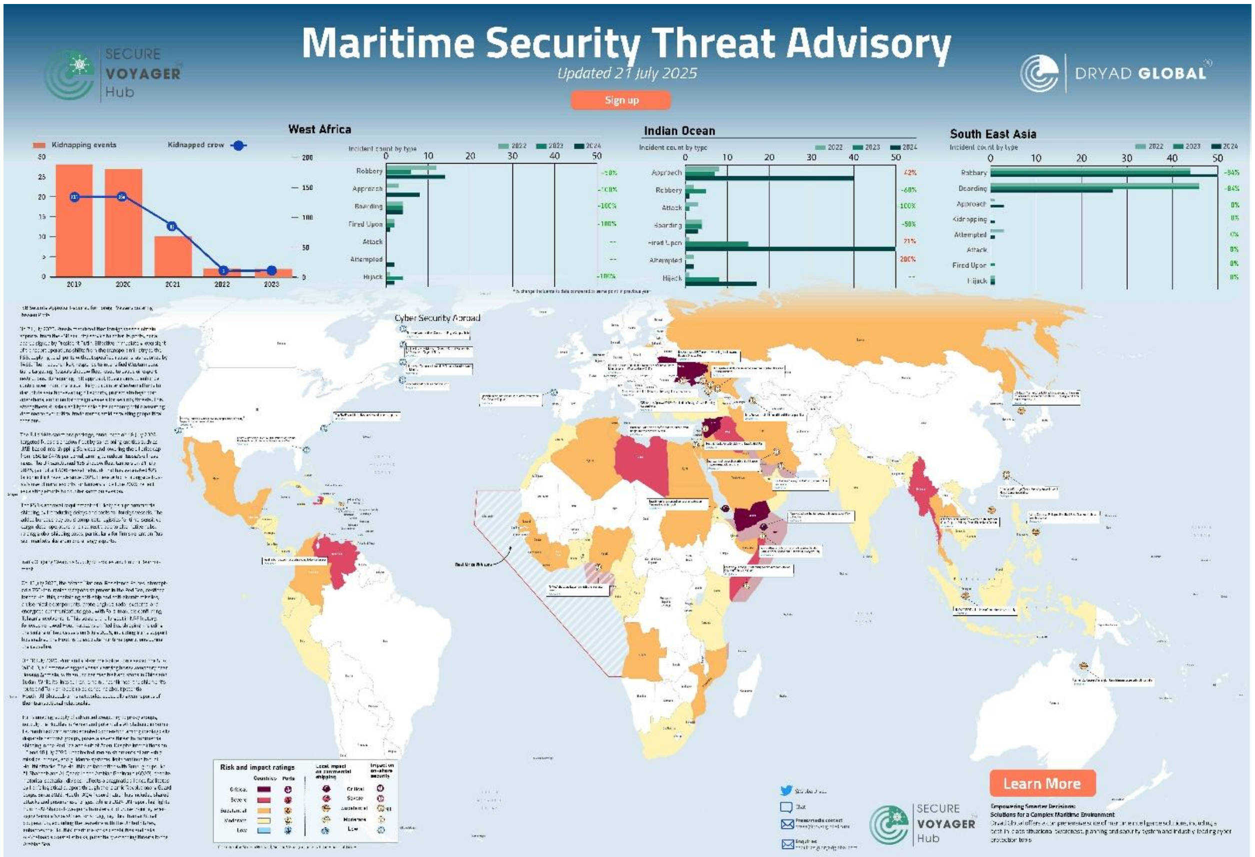
Maritime Cybersecurity, Risk, and the Threat Landscape

Global Operational Technology (OT) Vulnerabilities:

OT systems, which govern essential shipboard functions such as navigation, propulsion, and cargo handling, remain a major focus for attackers. Many of these systems rely on outdated software and lack modern cybersecurity measures, making them highly susceptible to breaches. Additionally, the growing interconnectivity of IT and OT systems introduces cascading risks, where a single breach can disrupt both operational and digital environments. Direct attacks on OT systems could result in vessel immobilization, navigational failures, or safety incidents, making the security of these systems a top priority.



Asking the larger business questions:

What are the biggest cybersecurity threats facing the maritime industry in 2026?

How can AI and large language models be used in maritime cyberattacks?

What are supply chain cyberattacks, and how do they affect maritime operations?

Why are operational technology (OT) systems vulnerable in the maritime sector?

What are the cybersecurity risks associated with autonomous vessels?

How do state-sponsored cyberattacks target maritime infrastructure?

What is hybrid warfare, and how does it impact global maritime security?

What steps can maritime operators take to enhance cybersecurity now and beyond 2026?

Why do smaller maritime operators struggle with cybersecurity compliance?

How can maritime companies protect against AI-driven cyberattacks?

Understanding the answers and their impact:

US ProTech has access to Dryad research data and the two are currently collaborating to bring new, unknown, and emerging security data to answer the aforementioned questions for the Maritime industry. In addition to providing essential Cybersecurity related risk data and proposing solutions for consideration to industry professionals, the Team seeks to assist organizations who have the mandated to navigate these industry related compliance requirements with meaningful products, and services, both fee-based, and those which are completely complementary. Two immediate resources include “CDM” (Continuous Diagnostics & Mitigation” and a “SIEM” (Security Information Event Management) solution.

Considerations:

1. US ProTech, and its flagship CDM-SIEM Cybersecurity platform “Anamo” offers the last-line of OT/IT defense.
2. From its position of command at the internal core of any targeted system (Linux or Window Operation Systems) Anamo sees all Transactions where others remain blind.
3. Anamo, harnesses patented Comparative HashID Analytics technology, a Host-Based CDM-SIEM Cybersecurity platform delivering actionable intelligence collected upon fact-base forensic information unavailable to all Network-based, Cloud-based, or other external monitoring applications.

“Managing customer Cybersecurity risk-posture via continuous granular inspections of systems, Users, UUIDs, Ports, Permissions, CVE’s and Transactions from individual or grouped systems, especially where converged OT and IT systems are concerned in near real-time was impossible before Anamo” (said J. Goetsch, CEO of Anamo).

Limited NFR Licensing is available to qualified Maritime operators, see: www.Anamo.io