

Europe Maritime Cybersecurity Market: Focus on End User, Solution, Service, Threat Type, and Country-Wise Analysis - Analysis and Forecast, 2023-2033

<https://marketpublishers.com/r/EDF1E901A1C2EN.html>

Date: December 2024

Pages: 73

Price: US\$ 3,250.00 (Single User License)

ID: EDF1E901A1C2EN

Abstracts

Hard copy option is available on any of the options above at an additional charge of \$500. Please email us at order@marketpublishers.com with your request.

This report will be delivered in 7-10 working days. Introduction to Europe Maritime Cybersecurity Market

The Europe maritime cybersecurity market is projected to reach \$3,492.9 million by 2033 from \$972.3 million in 2023, growing at a CAGR of 13.64% during the forecast period 2023-2033. Protecting digital assets and networks in the maritime industry from online threats is the main goal of maritime cybersecurity in Europe. As maritime operations depend more and more on digital technologies, cybersecurity has become crucial to ensuring efficiency, safety, and risk mitigation. These dangers range from widespread cyberattacks like viruses and scams to more complex attacks that target shore-based infrastructure and vessel systems. Serious repercussions, including interruptions in business operations, monetary losses, harm to the environment, and even death, can result from cybersecurity breaches. Shipping firms, port authorities, regulatory agencies, and trade associations are important participants in the European maritime cybersecurity market. Techniques like risk assessment, access control, incident response planning, and continuous employee training are necessary for effective cybersecurity management. Global rules, like those established by the International Maritime Organization (IMO) and the International Ship and Port Facility Security (ISPS) Code, provide frameworks for improving cybersecurity within the maritime sector. Collaboration between public and private sectors, along with technological innovation and information sharing, is crucial to address cyber threats effectively. As the maritime industry continues its digital transformation, robust

cybersecurity measures will be vital for ensuring resilience and sustainability across European maritime operations.

Market Introduction

The maritime sector's growing dependence on digital technologies for communication, navigation, and operations is driving a notable expansion in the European maritime cybersecurity market. Strong cybersecurity is crucial to protecting ships, ports, and associated infrastructure because of the increased susceptibility to cyberattacks that comes with this increased digitization. These dangers can cause operational disruptions, monetary losses, environmental harm, and threats to human safety. They range from viruses and phishing scams to more sophisticated attacks that target vital systems.

The increasing use of cloud computing, automation, and Internet of Things (IoT) devices in the maritime industry is propelling the market. In order to adhere to international standards like the ISPS Code and the regulations of the International Maritime Organization (IMO), major industry participants, including shipping companies, port authorities, and regulatory bodies, are concentrating on fortifying their cybersecurity frameworks. Furthermore, tackling changing cybersecurity challenges requires cooperation between the public and private sectors, improvements in threat detection, and continual staff training. The need for efficient cybersecurity solutions is anticipated to increase as Europe continues to embrace digital transformation in the maritime industry, guaranteeing safer and more robust operations.

Market Segmentation:

Segmentation 1: by Solution

Threat Detection and Response

Identity and Access Management

Network Security

Data Protection and Encryption

Others

Segmentation 2: by Service

Training and Consulting Services

Risk Assessment and Investigation

Support and Maintenance

Managed Services

Segmentation 3: by Threat Type

Malware Attacks

Phishing Attacks

Insider Threats

Others

Segmentation 4: by End User

Port Authorities

Shipping Companies and Transportation

Maritime Insurers

Others

Segmentation 5: by Country

U.K.

Germany

France

Rest-of-Europe

How can this report add value to an organization?

Product/Innovation Strategy: The product segment helps the reader understand the different types of services available for deployment and their potential in Europe region. Moreover, the study provides the reader with a detailed understanding of the Europe maritime cybersecurity market by products based on solution, service, and threat type.

Growth/Marketing Strategy: The Europe maritime cybersecurity market has seen major development by key players operating in the market, such as business expansion, partnership, collaboration, and joint venture. The favored strategy for the companies has been partnerships to strengthen their position in the Europe maritime cybersecurity market

Competitive Strategy: Key players in the Europe maritime cybersecurity market analyzed and profiled in the study involve maritime cybersecurity products and service offering companies. Moreover, a detailed competitive benchmarking of the players operating in the Europe maritime cybersecurity market has been done to help the reader understand how players stack against each other, presenting a clear market landscape. Additionally, comprehensive competitive strategies such as partnerships, agreements, and collaborations will aid the reader in understanding the untapped revenue pockets in the market.

Contents

Executive Summary
Scope and Definition

1 MARKETS

- 1.1 Trends: Current and Future Impact Assessment
 - 1.1.1 Artificial Intelligence and Machine Learning in Cybersecurity
 - 1.1.2 Increased Connectivity
 - 1.1.3 Zero Trust Architecture (ZTA)
- 1.2 Supply Chain Overview
- 1.3 Regulatory and Environmental Considerations
 - 1.3.1 Regulatory Implications
- 1.4 Ecosystem/Ongoing Programs
 - 1.4.1 Series of Assessments, including Threat Modeling and Open-Source Intelligence, Performed by NCC Group
- 1.5 Startup Funding Summary
- 1.6 Market Dynamics Overview
 - 1.6.1 Business Drivers
 - 1.6.1.1 Increasing Cyber Threats and Attacks
 - 1.6.1.2 Digitalization of Maritime Operations
 - 1.6.1.3 Global Supply Chain Reliance on Maritime Transport
 - 1.6.2 Business Challenges
 - 1.6.2.1 Lack of Trained Personnel
 - 1.6.2.2 Complex Regulatory Environment
 - 1.6.3 Business Opportunities
 - 1.6.3.1 Cybersecurity for Autonomous Vessels
 - 1.6.3.2 Integration of Internet of Things (IoT) and Operational Technology (OT) Security

2 REGIONS

- 2.1 Regional Summary
- 2.2 Drivers and Restraints
- 2.3 Europe
 - 2.3.1 Regional Overview
 - 2.3.2 Driving Factors for Market Growth
 - 2.3.3 Factors Challenging the Market

- 2.3.4 Application
- 2.3.5 Product
- 2.3.6 U.K.
- 2.3.7 Application
- 2.3.8 Product
- 2.3.9 Germany
- 2.3.10 Application
- 2.3.11 Product
- 2.3.12 France
- 2.3.13 Application
- 2.3.14 Product
- 2.3.15 Rest-of-Europe
- 2.3.16 Application
- 2.3.17 Product

3 MARKETS - COMPETITIVE BENCHMARKING & COMPANY PROFILES

- 3.1 Next Frontiers
- 3.2 Geographic Assessment
 - 3.2.1 SAAB AB
 - 3.2.1.1 Overview
 - 3.2.1.2 Top Products/Product Portfolio
 - 3.2.1.3 Top Competitors
 - 3.2.1.4 Target Customers
 - 3.2.1.5 Key Personnel
 - 3.2.1.6 Analyst View
 - 3.2.1.7 Market Share, 2022
 - 3.2.2 Thales
 - 3.2.2.1 Overview
 - 3.2.2.2 Top Products/Product Portfolio
 - 3.2.2.3 Top Competitors
 - 3.2.2.4 Target Customers
 - 3.2.2.5 Key Personnel
 - 3.2.2.6 Analyst View
 - 3.2.2.7 Market Share, 2022
 - 3.2.3 Leonardo S.p.A.
 - 3.2.3.1 Overview
 - 3.2.3.2 Top Products/Product Portfolio
 - 3.2.3.3 Top Competitors

- 3.2.3.4 Target Customers
- 3.2.3.5 Key Personnel
- 3.2.3.6 Analyst View
- 3.2.3.7 Market Share, 2022
- 3.2.4 Airbus SE
 - 3.2.4.1 Overview
 - 3.2.4.2 Top Products/Product Portfolio
 - 3.2.4.3 Top Competitors
 - 3.2.4.4 Target Customers
 - 3.2.4.5 Key Personnel
 - 3.2.4.6 Analyst View
 - 3.2.4.7 Market Share, 2022
- 3.2.5 BAE Systems
 - 3.2.5.1 Overview
 - 3.2.5.2 Top Products/Product Portfolio
 - 3.2.5.3 Top Competitors
 - 3.2.5.4 Target Customers
 - 3.2.5.5 Key Personnel
 - 3.2.5.6 Analyst View
 - 3.2.5.7 Market Share, 2022
- 3.2.6 Terma
 - 3.2.6.1 Overview
 - 3.2.6.2 Top Products/Product Portfolio
 - 3.2.6.3 Top Competitors
 - 3.2.6.4 Target Customers
 - 3.2.6.5 Key Personnel
 - 3.2.6.6 Analyst View
 - 3.2.6.7 Market Share, 2022
- 3.2.7 Westminster Group Plc
 - 3.2.7.1 Overview
 - 3.2.7.2 Top Products/Product Portfolio
 - 3.2.7.3 Top Competitors
 - 3.2.7.4 Target Customers
 - 3.2.7.5 Key Personnel
 - 3.2.7.6 Analyst View
 - 3.2.7.7 Market Share, 2022
- 3.2.8 Kongsberg Digital
 - 3.2.8.1 Overview
 - 3.2.8.2 Top Products/Product Portfolio

- 3.2.8.3 Top Competitors
- 3.2.8.4 Target Customers
- 3.2.8.5 Key Personnel
- 3.2.8.6 Analyst View
- 3.2.8.7 Market Share, 2022
- 3.2.9 Smiths Group plc
 - 3.2.9.1 Overview
 - 3.2.9.2 Top Products/Product Portfolio
 - 3.2.9.3 Top Competitors
 - 3.2.9.4 Target Customers
 - 3.2.9.5 Key Personnel
 - 3.2.9.6 Analyst View
 - 3.2.9.7 Market Share, 2022
- 3.2.10 Nettitude Ltd.
 - 3.2.10.1 Overview
 - 3.2.10.2 Top Products/Product Portfolio
 - 3.2.10.3 Top Competitors
 - 3.2.10.4 Target Customers
 - 3.2.10.5 Key Personnel
 - 3.2.10.6 Analyst View
 - 3.2.10.7 Market Share, 2022
- 3.2.11 HGH
 - 3.2.11.1 Overview
 - 3.2.11.2 Top Products/Product Portfolio
 - 3.2.11.3 Top Competitors
 - 3.2.11.4 Target Customers
 - 3.2.11.5 Key Personnel
 - 3.2.11.6 Analyst View
 - 3.2.11.7 Market Share, 2022
- 3.2.12 Other Key Players

4 RESEARCH METHODOLOGY

- 4.1 Data Sources
 - 4.1.1 Primary Data Sources
 - 4.1.2 Secondary Data Sources
 - 4.1.3 Data Triangulation
- 4.2 Market Estimation and Forecast

List Of Figures

LIST OF FIGURES

Figure 1: Maritime Cybersecurity Market (by Region), \$Million, 2022, 2023, and 2033

Figure 2: Europe Maritime Cybersecurity Market (by End User), \$Million, 2022, 2023, and 2033

Figure 3: Europe Maritime Cybersecurity Market (by Solution), \$Million, 2022, 2023, and 2033

Figure 4: Europe Maritime Cybersecurity Market (by Service), \$Million, 2022, 2023, and 2033

Figure 5: Europe Maritime Cybersecurity Market (by Threat Type), \$Million, 2022, 2023, and 2033

Figure 6: Maritime Cybersecurity Market, Recent Developments

Figure 7: Value Chain Analysis

Figure 8: Impact Analysis of Market Navigating Factors, 2023-2033

Figure 9: U.K. Maritime Cybersecurity Market, \$Million, 2022-2033

Figure 10: Germany Maritime Cybersecurity Market, \$Million, 2022-2033

Figure 11: France Maritime Cybersecurity Market, \$Million, 2022-2033

Figure 12: Rest-of-Europe Maritime Cybersecurity Market, \$Million, 2022-2033

Figure 13: Strategic Initiatives, 2020-2024

Figure 14: Share of Strategic Initiatives, 2020-2024

Figure 15: Data Triangulation

Figure 16: Top-Down and Bottom-Up Approach

Figure 17: Assumptions and Limitations

List Of Tables

LIST OF TABLES

Table 1: Market Snapshot

Table 2: Maritime Cybersecurity Market, Opportunities across Regions

Table 3: From a policy perspective, the U.K. and the U.S. are the leading geographies with a seemingly favorable environment.

Table 4: Maritime Cybersecurity (by Region), \$Million, 2022-2033

Table 5: Europe Maritime Cybersecurity Market (by End User), \$Million, 2022-2033

Table 6: Europe Maritime Cybersecurity Market (by Solution), \$Million, 2022-2033

Table 7: Europe Maritime Cybersecurity Market (by Service), \$Million, 2022-2033

Table 8: Europe Maritime Cybersecurity Market (by Threat Type), \$Million, 2022-2033

Table 9: U.K. Maritime Cybersecurity Market (by End User), \$Million, 2022-2033

Table 10: U.K. Maritime Cybersecurity Market (by Solution), \$Million, 2022-2033

Table 11: U.K. Maritime Cybersecurity Market (by Service), \$Million, 2022-2033

Table 12: U.K. Maritime Cybersecurity Market (by Threat Type), \$Million, 2022-2033

Table 13: Germany Maritime Cybersecurity Market (by End User), \$Million, 2022-2033

Table 14: Germany Maritime Cybersecurity Market (by Solution), \$Million, 2022-2033

Table 15: Germany Maritime Cybersecurity Market (by Service), \$Million, 2022-2033

Table 16: Germany Maritime Cybersecurity Market (by Threat Type), \$Million, 2022-2033

Table 17: France Maritime Cybersecurity Market (by End User), \$Million, 2022-2033

Table 18: France Maritime Cybersecurity Market (by Solution), \$Million, 2022-2033

Table 19: France Maritime Cybersecurity Market (by Service), \$Million, 2022-2033

Table 20: France Maritime Cybersecurity Market (by Threat Type), \$Million, 2022-2033

Table 21: Rest-of-Europe Maritime Cybersecurity Market (by End User), \$Million, 2022-2033

Table 22: Rest-of-Europe Maritime Cybersecurity Market (by Solution), \$Million, 2022-2033

Table 23: Rest-of-Europe Maritime Cybersecurity Market (by Service), \$Million, 2022-2033

Table 24: Rest-of-Europe Maritime Cybersecurity Market (by Threat Type), \$Million, 2022-2033

I would like to order

Product name: Europe Maritime Cybersecurity Market: Focus on End User, Solution, Service, Threat Type, and Country-Wise Analysis - Analysis and Forecast, 2023-2033

Product link: <https://marketpublishers.com/r/EDF1E901A1C2EN.html>

Price: US\$ 3,250.00 (Single User License / Electronic Delivery)

If you want to order Corporate License or Hard Copy, please, contact our Customer Service:

info@marketpublishers.com

Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page <https://marketpublishers.com/r/EDF1E901A1C2EN.html>