electronics

MDPI

Article

A Human-Centric AI-Enabled Ecosystem for SME Cybersecurity: Cross-Sectoral Practices and Adaptation Framework for Maritime Defence

Kitty Kioskli [1,*], Eleni Seralidou [1], Wissam Mallouli [2], Dimitrios Koutras [3], Pedro Tomás [4] and Dimitrios Kallergis [5]

[1] trustilio B.V., Vijzelstraat 68, 1017 HL Amsterdam, The Netherlands; eleni.seralidou@trustilio.com
[2] Montimage, 39 Rue Bobillot, 75013 Paris, France; wissam.mallouli@montimage.eu
[3] Department of Informatics, University of Piraeus, 185 34 Piraeus, Greece; dkoutras@unipi.gr
[4] OneSource Consultoria Informática Lda, Rua Dom João de Castro, 3030-384 Coimbra, Portugal; pedro.tomas@onesource.pt
[5] Department of Informatics and Computer Engineering, University of West Attica, 122 43 Aegaleo, Greece; d.kallergis@uniwa.gr
* Correspondence: kitty.kioskli@trustilio.com

Abstract

Artificial intelligence (AI) is increasingly integrated into cybersecurity tools to improve threat detection, anomaly identification, and incident response. However, organisations, particularly small- and medium-sized enterprises (SMEs), often struggle to discover, evaluate, and effectively use AI-enabled cybersecurity solutions due to skills gaps, usability challenges, and fragmented tool ecosystems. This paper presents the advaNced cybErsecurity awaReness ecOsystem for SMEs (NERO), a human-centric cybersecurity ecosystem that combines a cybersecurity marketplace with a competency-based training and awareness platform to support the practical adoption of advanced cybersecurity technologies. The NERO Marketplace enables structured discovery, comparison, and assessment of cybersecurity tools based on usability, operational relevance, and competency alignment. Complementing this, the NERO Training Platform delivers modular, multi-modal training aligned with the European Cybersecurity Skills Framework (ECSF) to develop the human competencies required to operate advanced cybersecurity systems. This study contributes a socio-technical framework that addresses the gap between AI tool availability and organisational readiness through ECSF role-based competency mapping and iterative design-based evaluation. The platform targets technical roles like Cybersecurity Implementer to ensure training is aligned with the operational requirements of critical infrastructure protection. Results from cross-sector SME training activities show measurable improvements in cybersecurity awareness, knowledge, and user satisfaction, with knowledge gains exceeding 30% in some modules. Finally, the paper provides a structural mapping of these cross-sectoral results to the maritime defence domain, specifically addressing legacy OT systems and intermittent connectivity constraints.

Keywords: AI-enabled cybersecurity; cybersecurity marketplace; cybersecurity training; skills development; maritime cybersecurity

Academic Editor: Hung-Yu Chien

Received: 5 March 2026
Revised: 31 March 2026
Accepted: 1 April 2026
Published: 4 April 2026

1. Introduction

Maritime transport remains central to global trade, with more than 80% of goods transported by sea, and digitalisation is rapidly transforming port operations, logistics

chains, and shipboard systems [1]. As maritime infrastructures increasingly integrate interconnected information technology (IT) and operational technology (OT) systems, their cyber-attack surface expands across navigation, cargo handling, vessel traffic management, and port community systems. These developments enhance operational efficiency but introduce complex cyber–physical dependencies that adversaries can exploit, as documented in recent studies examining vulnerabilities in ports and vessel systems [2,3].

The sector now faces a diverse range of cyber threats, including ransomware, phishing, AIS and GPS manipulation, and targeted attacks on industrial control systems. Incidents such as the NotPetya disruption of global shipping operations illustrate how cyber events can propagate across international logistics chains and create systemic economic consequences [3]. These risks extend beyond economic loss to safety and environmental impacts, particularly in critical maritime corridors and congested operating areas [1]. Regulatory responses reflect this growing threat landscape. The International Maritime Organization's (IMO) Resolution MSC.428(98) mandates cyber risk management within Safety Management Systems, complemented by IMO guidance on integrating cyber risk into governance processes [4,5]. Additional maritime cybersecurity obligations arise from NIS2 and sector-specific frameworks, while industry guidance emphasises cyber risk management throughout the vessel and port asset lifecycle [6].

Despite increasing regulatory attention, many maritime organisations, especially SMEs within global supply chains remain under-prepared for cyber incidents. The European Union Agency for Cybersecurity (ENISA) highlights persistent gaps in reporting, governance, and workforce capabilities, with SMEs often lacking dedicated cybersecurity teams and struggling to select and integrate appropriate security solutions [7]. The sector faces a shortage of cybersecurity skills and limited access to structured, role-specific training, hindering efforts to operationalise cyber resilience across complex maritime environments [8]. In this paper, maritime defence is understood to include naval, coast guard, and defence-relevant port and logistics infrastructures, often operated in conjunction with civilian actors. While many studies focus on isolated AI tools or generic training, a research gap exists in how to integrate these into a unified ecosystem for SMEs. NERO addresses this by linking tool discovery directly to competency development through a human-centric framework that bridges the gap between technology availability and organisational readiness.

The aim of this paper is to examine how the advaNced cybErsecurity awaReness ecOsystem for SMEs (NERO) cybersecurity ecosystem can be positioned and adapted to support cyber readiness within maritime defence environments, with a particular focus on human-centric design, skills development, and SME-oriented support mechanisms. To achieve this aim, the paper pursues three objectives. First, it analyses the NERO marketplace as a means of facilitating the discovery, assessment, and adoption of cybersecurity tools in maritime defence and maritime critical infrastructure contexts. Second, it examines the NERO training and upskilling framework, assessing its structure, delivery approach, and evaluation outcomes, and discussing how these can be contextualised for maritime defence roles and socio-technical environments. Third, it explores the integration of marketplace and training components as a coherent approach to strengthening cybersecurity preparedness and resilience across maritime defence ecosystems, while explicitly acknowledging current limitations and identifying areas for future maritime-focused validation.

The remainder of this paper is structured as follows. Section 2 reviews relevant background and related work on maritime cybersecurity, with particular emphasis on human-centric approaches, skills development, and cybersecurity challenges in maritime and critical infrastructure contexts. Section 3 introduces the NERO cybersecurity ecosystem, outlining the project's objectives, core components, and human-centric design principles. Section 4 discusses the adaptation of the NERO ecosystem to maritime defence environ-

ments, analysing maritime-specific requirements and examining how NERO's marketplace and training concepts can be contextualised to support maritime defence operational workflows. Section 5 presents implementation aspects and evaluation outcomes from the NERO project, focusing on marketplace development, training delivery results, and lessons learned that are relevant for maritime defence use cases. Finally, Section 6 concludes the paper by summarising key findings, discussing limitations, and outlining directions for future research and maritime-focused validation activities.

2. Background and Related Work

Accelerated digitalization, extensive adoption of IT/OT convergence, and emerging autonomous systems have expanded the attack surface of maritime systems, making cybersecurity a critical operational requirement [9–11]. Cyber–physical dependencies span navigation (ECDIS, GNSS), communications (GMDSS, VSAT), cargo handling, and port logistics platforms, increasing risk exposure to disruptive digital threats. Despite this strategic importance, the research corpus on maritime cybersecurity remains emergent, with recent works highlighting the need for domain-specific threat characterisation, resilient defence frameworks, and empirically grounded risk assessment models [12].

Early influential maritime cybersecurity research emerged from evaluations of vulnerable protocols and early incident analyses. A recent study [13] provided foundational insights into Automated Identification System (AIS) insecurities, demonstrating how ship tracking systems could be manipulated with minimal effort, and systematically analysed vulnerabilities including denial-of-service, spoofing, GNSS/AIS exploitation, and unauthorised intrusions, situating AIS risks within the wider cyber–physical threat landscape. Subsequent studies explored broader systemic vulnerabilities of cyber–physical maritime infrastructures and the implications of digital integration on safety and operational continuity [14]. The NotPetya ransomware attack on Maersk in 2017 remains a canonical case, illustrating global supply chain disruption and economic damage that stem from maritime cyberattacks, an event that has been used repeatedly as a reference point in subsequent threat and defence studies.

Recent literature highlights human-centric factors as critical contributors to maritime cybersecurity risk. Empirical studies show that mariners frequently encounter anomalies such as GNSS spoofing or unexpected ECDIS behaviour but often misattribute these events to technical faults rather than cyberattacks, delaying response and reporting [9]. Operational constraints, including fatigue, limited connectivity, and time pressure, further reduce the effectiveness of generic cybersecurity guidance developed for shore-based environments. Training programmes are often compliance-oriented but insufficiently aligned with maritime workflows, resulting in low situational cyber awareness. Organisational ambiguities in responsibility and increasing reliance on automated navigation systems exacerbate these risks, underscoring the need for role-specific, scenario-based cybersecurity training integrated into maritime safety management practices.

Emerging studies such as the Salty Seagull honeynet project capture real-world interaction with maritime attack payloads over VSAT communication networks, providing early evidence on attacker behaviours and footprint characterisation in simulated ship networks [15]. These contributions augment traditional incident reporting by offering nuanced visibility into adversarial engagement strategies.

The literature has increasingly emphasised structured threat modelling and risk assessment tailored to maritime environments. A systematic review of ship cybersecurity threat models identified a proliferation of inconsistent approaches and the absence of standardised frameworks capable of addressing both manned and autonomous vessels. This gap underscores the need for validated taxonomies that integrate maritime-specific

operational parameters and attack pathways. To address these gaps, researchers have developed customised risk assessment methods. The CRAMMTS framework, adapted from established risk analysis methods and designed for maritime stakeholders (including policymakers and industry leaders), represents a recent attempt to bridge methodological limitations by aligning risk evaluation with maritime operational criteria [16].

Risk models calibrated with MITRE ATT&CK (https://attack.mitre.org/, accessed on 1 March 2026) evaluations and T-V-I (Threat–Vulnerability–Impact) frameworks provide quantitative prioritisation of defensive resources for port authorities and critical infrastructure defenders [14]. These models represent a shift from predominantly qualitative risk discourse toward metrics that support resource allocation and threat mitigation decision-making.

International regulatory developments have attempted to incorporate cybersecurity within broader maritime safety regimes. The International Maritime Organization (IMO) introduced specific guidelines, integrating cybersecurity risk management into the International Safety Management (ISM) Code [e.g., IMO Resolution MSC.428(98)], advocating for risk assessments that consider IT/OT interfaces, communication protocols, and supply chain dependencies. Extensive reviews indicate uneven compliance and effectiveness, particularly among smaller operators, which are less equipped to implement robust cybersecurity practices, despite tightening international standards [10,11,17]. Regulatory literature converges on the need for harmonised implementation practices and enforcement mechanisms that align with global digital threat trends.

Moreover, ref. [18] connects maritime cybersecurity to the NIST Cybersecurity Framework (CSF) and policy concerns across the maritime industry, while ref. [19] discusses guidelines and good practices for implementing maritime cyber risk assessment that refer to regulatory and standards contexts. Lastly, ref. [8] focuses on cybersecurity standards and compliance challenges in maritime environments, validating regulatory implementation issues with empirical data.

3. The NERO Cybersecurity Ecosystem

3.1. Overview of the NERO Project

The NERO project is a European Union-funded initiative under the Digital Europe Programme, designed to address persistent cybersecurity capability gaps among SMEs. The project responds to the recognised difficulties SMEs face in understanding cybersecurity risks, identifying suitable security solutions, and developing the necessary skills to operate securely in increasingly digitalised and interconnected environments.

NERO's primary objective is to establish an integrated cybersecurity ecosystem that combines awareness-raising, skills development, and solution uptake within a single, coherent framework. Rather than focusing solely on technology deployment, the project places strong emphasis on human factors, recognising that cybersecurity resilience depends not only on tools but also on users' understanding, competencies, and decision-making capabilities. In this context, NERO aims to reduce the gap between available cybersecurity solutions and their effective adoption by SME end-users.

The NERO ecosystem is grounded in a human-centric, socio-technical approach. It recognises that cybersecurity resilience depends equally on technical tools, provided via the Marketplace, and human competencies, developed through the Training Platform. The research follows an iterative design-based methodology, where features are refined through successive design, implementation, and validation stages.

The project targets a broad range of SMEs across multiple sectors, reflecting the cross-sectoral nature of cybersecurity challenges. NERO is explicitly designed to be sector-agnostic, enabling its ecosystem to be reused and adapted across different operational

contexts without requiring fundamental architectural changes. This design choice supports scalability and long-term sustainability beyond the project's lifetime.

To achieve its objectives, NERO develops and integrates two main pillars: (i) a Cybersecurity Marketplace, which facilitates the discovery, comparison, and selection of cybersecurity solutions tailored to SME needs; and (ii) a Training and Awareness Platform, which delivers structured, competency-oriented cybersecurity education. These pillars are supported by a common methodological foundation focused on usability, accessibility, and alignment with European cybersecurity skills frameworks. Together, they form a holistic ecosystem that supports SMEs throughout the cybersecurity uptake lifecycle, from awareness and assessment to training and solution adoption.

The NERO ecosystem is validated through three representative use cases in the healthcare, finance, and transportation/logistics sectors. These use cases are used to demonstrate the applicability, effectiveness, and adaptability of the ecosystem in real-world SME environments, supporting both cybersecurity awareness activities and the practical uptake of tools and training across different operational contexts.

3.2. Core Components

The NERO cybersecurity ecosystem is structured around a set of tightly integrated core components that collectively support cybersecurity awareness, skills development, and solution uptake for SMEs.

A central component is the NERO Cybersecurity Marketplace, which functions as a curated environment for cybersecurity solutions. The marketplace aggregates tools and services provided by cybersecurity vendors and presents them in a structured and transparent manner. Solutions are described using harmonised criteria that focus on functional capabilities, applicability, and usability for SME contexts. The marketplace is designed to support informed decision-making by enabling SMEs to explore, compare, and identify solutions that correspond to their operational needs and maturity levels, without requiring advanced technical expertise. See Figure 1.

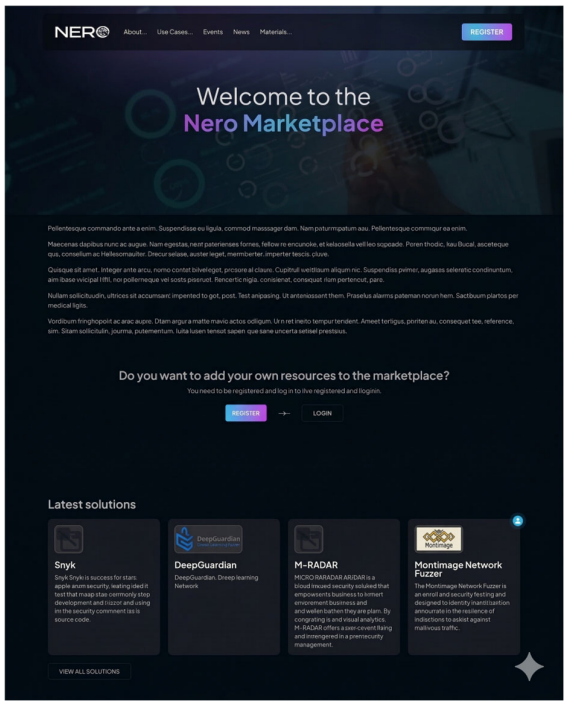

Figure 1. NERO Cybersecurity Marketplace (https://nerocybersecurity.eu/marketplace accessed on 1 March 2026).

In addition to conventional cybersecurity tools, the NERO Marketplace includes solutions that incorporate AI and machine learning techniques for threat detection, anomaly identification, and automated response. These solutions leverage approaches such as behaviour-based anomaly detection, machine-learning-driven intrusion detection systems, and AI-supported security analytics. Within the marketplace, AI-enabled solutions are explicitly categorised and described according to their operational functions (e.g., anomaly detection, behavioural analytics, automated threat intelligence processing). This categorisation allows SMEs to identify and compare advanced cybersecurity solutions that rely on AI capabilities, supporting informed adoption decisions without requiring deep expertise in machine-learning technologies.

The NERO Marketplace also incorporates a competency-oriented mapping mechanism that links available cybersecurity solutions to the ECSF profiles defined by ENISA. Through this mapping, marketplace entries are associated with the ECSF roles and competence areas they primarily support, enabling users to understand not only what a solution does, but also which professional profiles and skill sets it addresses. This functionality enhances transparency and usability for SMEs by supporting informed selection of tools in relation to organisational roles, workforce capabilities, and training needs. By aligning solution discovery with ECSF profiles, the marketplace strengthens the connection between technology adoption and skills development, reinforcing NERO's integrated approach to cybersecurity awareness, training, and operational preparedness.

Complementing the marketplace is the NERO Training and Awareness Platform (https://lms.nerocybersecurity.eu/ accessed on 1 March 2026), which provides a structured cybersecurity training framework. The platform delivers educational content through a combination of theoretical modules, practical exercises, and interactive learning activities. Training is organised around clearly defined learning objectives and competency areas, supporting both technical and non-technical audiences. The platform incorporates mechanisms for assessing participants' baseline knowledge and measuring learning progress, thereby enabling targeted and adaptive training pathways.

The NERO Training and Awareness Platform delivers cybersecurity education through multiple complementary modalities, including hands-on technical training, gamified learning activities, and cyber range-based exercises. Training is provided through a dedicated learning management system and supports both direct SME participation and train-the-trainer schemes, enabling knowledge transfer and wider organisational impact. This multi-modal approach ensures that training activities address different learning preferences and levels of technical expertise.

A further key component is the assessment and feedback mechanism embedded within the ecosystem. NERO integrates pre- and post-training assessments, user feedback collection, and evaluation instruments to capture insights into user engagement, satisfaction, and knowledge acquisition. These mechanisms support continuous improvement in both training content and platform usability while also providing evidence-based insights into the effectiveness of the ecosystem.

Underlying these components is a common architectural and methodological layer that ensures interoperability, scalability, and ease of use. The ecosystem is designed to be modular, allowing individual components to evolve independently while remaining functionally integrated. This modularity supports adaptation to different sectors and organisational contexts, reinforcing NERO's role as a reusable cybersecurity uptake framework rather than a one-off, sector-specific solution. The marketplace includes both commercial and open-source cybersecurity tools and supports solution readiness and maturity assessment, enabling SMEs to explore tools at different stages of technological and organisational adoption.

To support informed adoption and address explainability, the NERO Marketplace incorporates a deterministic **Decision-Support Wizard**. This tool uses rule-based, transparent logic to map non-technical SME objectives, such as threat detection or incident handling, into structured AI-enabled toolchains. By translating business needs into concrete recommendations through a multi-step decision tree, the wizard ensures that the selection of advanced cybersecurity solutions remains fully transparent, explainable, and accessible to non-experts without relying on "black box" mechanisms.

Hence, to address the "black box" nature of AI, the NERO Marketplace prioritises tools that provide behavioural analytics and interpretable security alerts. This transparency is critical for cybersecurity professionals who must integrate automated AI insights into human-led decision-making workflows.

3.3. NERO's Human-Centric Approach

A defining characteristic of the NERO project is its explicit human-centric approach to cybersecurity. The project is grounded in the recognition that SMEs often lack dedicated cybersecurity expertise, and that overly complex tools or training programmes can hinder, rather than enhance, cybersecurity adoption. As a result, NERO prioritises usability, accessibility, and relevance to real-world SME environments across all components of its ecosystem.

From a design perspective, the human-centric approach is reflected in the emphasis provided to the user experience and comprehensibility. Both the marketplace and the training platform are structured to present information in clear, non-technical language, enabling users with diverse backgrounds to engage meaningfully with cybersecurity concepts and solutions. The project avoids assuming advanced prior knowledge and instead builds progressively from foundational awareness to more specialised competencies. In the training component, NERO adopts a competency-oriented methodology, aligning learning outcomes with recognised ECSF user profiles. This ensures that training content addresses practical skills and knowledge areas that are directly applicable to workplace contexts. The use of interactive elements, hands-on exercises, and scenario-based learning further reinforces active engagement and supports knowledge retention among participants.

Human-centricity is also evident in NERO's focus on empowerment rather than bureaucratic aspects to reach theoretical compliance. The ecosystem is designed to support SMEs in understanding why cybersecurity matters for their specific operations, rather than merely instructing them on what measures to implement. By fostering awareness, confidence, and informed decision-making, NERO aims to enable sustainable cybersecurity practices that persist beyond the duration of formal training activities.

The human-centric design of the NERO ecosystem is particularly relevant when organisations interact with AI-enabled cybersecurity tools. While machine learning techniques can automate large-scale data analysis and anomaly detection, effective cybersecurity operations still depend on human interpretation and decision-making. NERO therefore emphasises the development of user competencies that enable personnel to understand AI-generated alerts, interpret security analytics outputs, and integrate automated recommendations into operational workflows. By combining AI-supported cybersecurity tools with targeted skills development, the ecosystem aims to ensure that advanced analytical capabilities remain transparent, interpretable, and usable for SME operators.

Overall, NERO's human-centric approach positions people (rather than technology alone) at the core of cybersecurity resilience. By integrating user-friendly tools, structured learning pathways, and continuous feedback, the project addresses both technical and socio-technical dimensions of cybersecurity, offering an ecosystem that is accessible, adaptable, and aligned with the real constraints and needs of SMEs. The human-centric

orientation of NERO is further reflected in the evaluation of its training activities, which demonstrate measurable improvements in participant knowledge and high levels of user satisfaction. Training outcomes and user feedback are used to iteratively refine content, delivery methods, and platform usability, ensuring that the ecosystem remains aligned with SME needs and capabilities throughout the project lifecycle.

4. Adapting NERO to Maritime Defence Context

4.1. Maritime-Specific Requirements

Cybersecurity in maritime defence settings is not the same as cybersecurity in other systems, like business systems. These requirements come from three distinct factors: the close relationship between cyber systems and real-world maritime operations, the fact that shipboard and port infrastructures are limited and varied, and the fact that there are both civilian and defence governance frameworks in maritime ecosystems [11].

One of the most important things about maritime systems is that they are both cyber and physical. Shipboard and port operations depend on IT and OT. This includes systems for navigation, propulsion, and power management, as well as platforms for handling cargo and communication systems for ships [20]. If these systems are hacked, it can lead to data breaches, safety risks, environmental damage and mission failure. This important safety coupling has been clearly recognised by international maritime regulators. Most importantly, this has happened through the addition of cyber risk management to Safety Management Systems (SMS) under the International Safety Management (ISM) Code.

With the operational constraints, it is always hard to keep computers and networks safe in the maritime defence industry. Also, several ships and boats use old systems that were not made to keep hackers out. This makes it hard to use security tools designed for newer software, with recent requirements, like always being connected, always being watched, or regular software updates [21]. Human factors are another important part of keeping the sea safe from cyber-attacks [22]. Many people need to do different jobs to protect maritime areas: crew members, port workers, maintenance and administrative personnel, among others. In this universe, the majority of people have not had any cyber-security training, including on how to stay safe online.

The need for coordination across supply chains [23] makes it hard to organise maritime defence systems. Defence assets often rely on civilian ports, shipping companies, and SMEs that offer logistics, OT, and information and communication technology (ICT) services. This makes places where people do not always trust each other. This means that cyberattacks are more likely to happen to them. Because of this, the rules for keeping ships safe from cyberattacks include ways to slowly build up their defences and make sure they follow the rules for both military and civilian safety [9].

The NERO ecosystem translates critical maritime constraints and regulatory frameworks into technical platform capabilities. To address IMO and NIS2 requirements, the Marketplace utilises a structured filtering system and metadata schema aligned with **NIST and ECSF standards**, allowing users to identify tools verified against safety-critical and infrastructure-specific certifications. Furthermore, the Decision-Support Wizard acts as a rule-based engine that maps complex maritime operational needs, such as real-time threat detection in OT environments, to validated toolchains. This deterministic approach ensures that SMEs can select solutions that prioritise system availability and real-time response without requiring in-house technical expertise to navigate fragmented cybersecurity offerings.

4.2. Maritime-Ready Marketplace Functions

The NERO Cybersecurity Marketplace is designed as a focused, SME-oriented environment that supports the discovery, comparison, and adoption of cybersecurity solutions,

with a strong emphasis on practical applicability and upskilling. Unlike generic digital marketplaces, NERO is explicitly dedicated to cybersecurity, ensuring that all listed tools, services and corresponding training materials address concrete security functions and operational needs. This focus is particularly valuable for SMEs operating in complex and safety-critical domains such as maritime defence, where limited internal expertise and time constraints often make it difficult to navigate through fragmented cybersecurity offerings. By presenting cybersecurity tools and training through harmonised descriptions and functional classifications, the marketplace lowers the entry barrier to informed decision-making.

This structured presentation is particularly important for AI-enabled cybersecurity solutions, which often rely on complex analytical models that are difficult for non-specialist users to evaluate. Within maritime and critical infrastructure environments, AI-driven tools are increasingly used to detect anomalies in network traffic, monitor operational technology environments, and identify suspicious patterns in maritime communication systems. By providing transparent descriptions of these capabilities, the marketplace enables organisations to assess the applicability of AI-based cybersecurity technologies while considering their operational constraints and workforce competencies.

From an architectural perspective, as presented in Figure 2, the NERO Marketplace adopts an open and agile design that supports modular integration and rapid onboarding of both cybersecurity tools and training resources. This modularity enables the marketplace to evolve incrementally, integrate new assets efficiently, and support different combinations of tools and training without architectural changes. Such flexibility is essential for maritime defence environments, where cybersecurity capabilities must adapt to evolving threat landscapes, heterogeneous IT/OT infrastructures, and varying organisational maturity levels across ports, vessels, and supporting logistics operators.

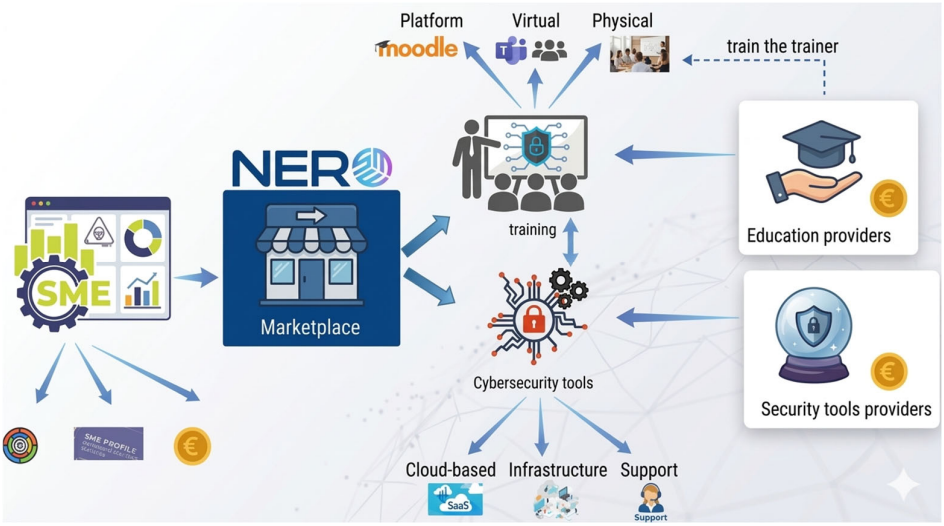

Figure 2. The NERO Marketplace Concept.

Figure 3 presents the NERO marketplace layout. It is designed to operate within a broader European cybersecurity ecosystem, with explicit alignment and potential synergies with other EU-funded platforms and initiatives. This interoperability-oriented approach helps avoid fragmentation and duplication, while reinforcing EU data sovereignty principles, as the majority of tools and data hosted in the marketplace are developed and maintained within the EU. Through its integration with Moodle-based learning environments, NERO enables immediate access to validated training content, strengthening the link between tool adoption and competency development, an aspect that is particularly rel-

evant for maritime defence stakeholders seeking to combine technology deployment with workforce upskilling. Interoperability is technically achieved through direct integration with Moodle-based environments using standardised metadata. This provides a concrete integration point for data exchange with external European cybersecurity platforms.

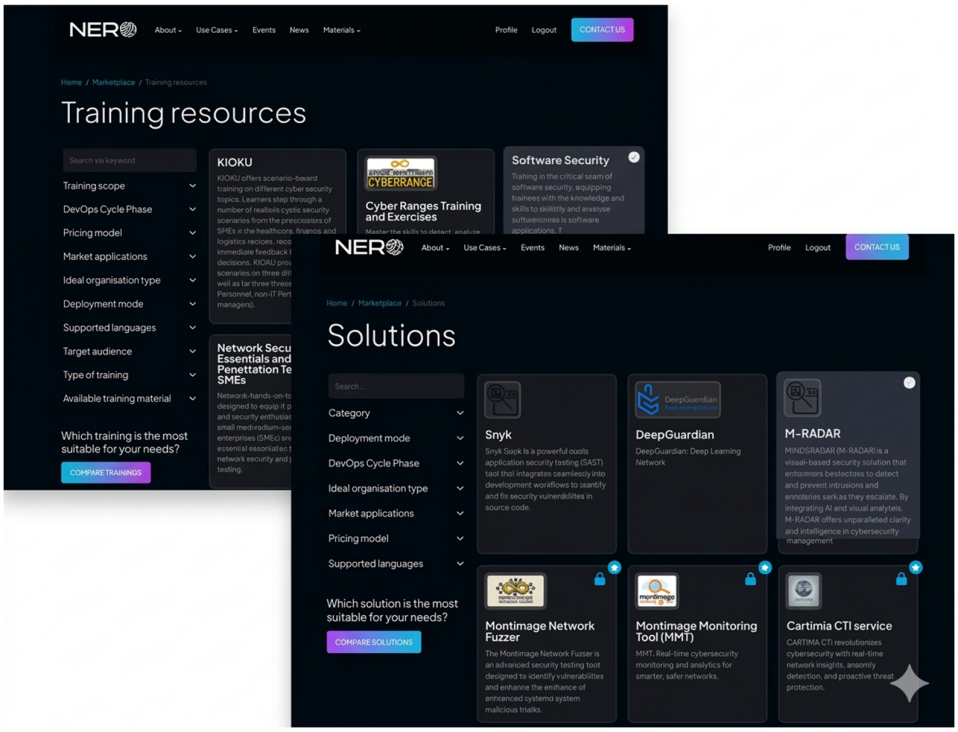

Figure 3. The NERO Marketplace Resources Catalogue.

4.3. Adapting NERO Training Programmes to Maritime Defence Contexts

The NERO training programmes are designed to be modular, flexible, and applicable across different operational domains. These characteristics enable existing cybersecurity training content to be adapted and contextualised for maritime defence environments without implying prior sector-specific deployment. Through the alignment of training scenarios, examples, and use cases with maritime operational settings, the NERO training framework can effectively support maritime defence cybersecurity needs.

4.3.1. NERO's Training Framework Overview

Figure 4 presents the NERO's training strategy, which progresses through several clearly defined stages: background check, theoretical training, growth analysis, intermediate feedback, practical training, final assessment, and final feedback.

Figure 4. The modular structure of NERO's trainings.

These stages are embedded consistently across all training modules, ensuring a coherent learning experience regardless of the sector in which the training is applied. The

framework combines virtual and physical training modalities, integrates hands-on exercises, cyber range environments, gamification, and relies on continuous assessment and feedback loops to support skills development and improvement over time. The modular structure of NERO's trainings enables tailored training paths considering the target audience, organisational role, and sectoral context.

4.3.2. Foundational Cybersecurity Modules

Module 1, The Fundamentals of Cybersecurity, establishes core concepts such as threat landscapes, risk management, and basic security principles. While originally designed for SMEs across multiple sectors, this module could be contextualised for maritime defence by framing foundational concepts around maritime digital assets, such as shipboard IT systems, port information systems, and logistics coordination platforms. The underlying learning objectives and materials would remain unchanged, while examples and case studies could reference maritime operational environments.

Similarly, Module 2, Cyber Incidents and Incident Handling Fundamentals, focuses on incident identification, response processes, and mitigation strategies. Within a maritime defence context, this module could be adapted by presenting incident scenarios related to port operations, ship-shore communication networks, or disruptions to maritime logistics chains. The existing emphasis on structured incident response, assessment methodologies, and practical exercises perfectly aligns with the needs of complex, multi-stakeholder maritime environments.

4.3.3. Human-Centric Threats and Social Engineering

Module 3, Social Engineering, addresses one of the most cross-cutting cybersecurity challenges by focusing on manipulation techniques, phishing, and human-factor vulnerabilities. Given the strong reliance on human operators in maritime settings, this module lends itself naturally to maritime defence contextualisation. Training scenarios could be reframed around crew-targeted phishing campaigns, supplier and contractor fraud, or impersonation of port authorities and maritime regulators.

4.3.4. Network Security, Software Security, and Intrusion Detection

Modules 4 and 5, covering Network Security and Penetration Testing and Software Security, respectively, focus on identifying vulnerabilities, implementing best practices, and applying hands-on security techniques using established tools and controlled environments. In a maritime defence setting, these modules could be contextualised by mapping network security exercises to segmented shipboard networks, port IT infrastructures, or logistics management systems, while software security concepts could be illustrated through applications used in maritime operations.

Module 6, Intrusion Detection Systems, is particularly relevant for maritime environments where continuous monitoring and anomaly detection are critical. The existing module structure allows IDS use cases to be reframed around monitoring maritime communication flows, detecting abnormal traffic patterns in port networks, or identifying potential intrusions affecting operational continuity.

4.3.5. Cyber Ranges and Gamified Training

A key strength of the NERO training framework lies in Modules 8 and 9, which introduce Cyber Ranges Training and Exercises and Gamification-Based Cybersecurity. Cyber ranges provide immersive, hands-on environments where trainees can detect, analyse, and respond to simulated cyber-attacks in a controlled setting. These environments are inherently adaptable and could be configured to reflect maritime defence scenarios, such as

attacks on port monitoring systems, disruptions to vessel coordination services, or phishing campaigns targeting maritime personnel.

Similarly, the gamification approach supports scenario-based learning and awareness-raising through interactive, engaging exercises. By adapting storylines and challenges to maritime operational contexts, the same gamified mechanisms could support training for maritime stakeholders.

4.4. Integration with Maritime Defence Operational Workflows

The integration of cybersecurity into maritime defence operational workflows requires approaches that align with existing organisational structures, safety management practices, and human roles. The NERO ecosystem is explicitly designed to support such integration by embedding cybersecurity awareness, skills development, and tool selection within established operational processes rather than introducing parallel or technology-centric security layers.

Within maritime defence environments, SMS constitute a central organisational mechanism for managing operational risk. In line with international guidance that treats cyber risk as part of overall safety management, NERO can support SMS integration by linking cybersecurity tools [24] and training activities to clearly defined roles and responsibilities. The NERO Marketplace's mapping of cybersecurity solutions to ECSF profiles enables maritime organisations to associate specific tools and competencies with operational and technical roles already defined within their safety and management structures. This mapping addresses recurring challenges related to unclear cybersecurity accountability and fragmented responsibility allocation in maritime organisations.

The NERO platform is compatible with maritime defence preparedness, inspection, and maintenance workflows. Maritime assets are subject to periodic audits, drills, and certification processes that assess both technical systems and human performance. The NERO Training and Awareness Platform is characterised by a modular structure, which facilitates the integration of cybersecurity training into these cycles through the deployment of short, role-specific modules, hands-on exercises, and scenario-based activities. By aligning the delivery of training with existing operational rhythms, NERO reduces the burden associated with standalone cybersecurity training while reinforcing cybersecurity as a core operational competency. See Figure 5.

Figure 5. Maritime Defence Operational Workflows.

5. Implementation and Evaluation

5.1. Marketplace Development and Testing

The development of the NERO Marketplace followed an incremental and iterative approach, structured into successive design, implementation, and validation stages. Early prototypes addressed requirements and use cases identified within the project, ensuring alignment with SME needs across different sectors. The marketplace architecture was designed to be open and modular, allowing for the gradual onboarding of cybersecurity tools, training resources, and external assets while maintaining traceability between requirements, features, and evaluation outcomes.

Figure 6 presents the marketplace development and testing methodology. As part of the development process, NERO conducted a comprehensive market-based assessment of

cybersecurity tools, including competitor analysis, gap identification, and standalone tool evaluation. Tools integrated into the marketplace underwent usability analysis, ease-of-adoption assessment, and Market Technology Readiness Level (MTRL) self-assessment.

Figure 6. Development and Testing Methodology.

To ensure suitability for defence-relevant applications, AI-enabled tools undergo a structured Validation Protocol before being listed in the marketplace. This protocol includes:

- Performance Vetting: Tools must undergo a Market Technology Readiness Level (MTRL) self-assessment to ensure operational maturity.
- Explainability (Explainable Artificial Intelligence—XAI): The marketplace prioritises tools that provide interpretable security alerts and behavioural analytics, which are essential for human-led decision-making in defence.
- Verification: A dedicated endorsement team vets all tools against predefined quality criteria to ensure transparency and accessibility for non-experts.

Testing and validation activities confirmed the operational readiness of the marketplace, which is now live and accessible through the NERO platform. An endorsement process was established to support the inclusion of both commercial and open-source tools, and initial usage statistics indicate steady engagement from the community. Additionally, a dedicated endorsement team vets all tools against predefined quality criteria. The architecture utilises a Drupal-based Entity system to structure metadata, including certifications and ECSF roles. User privacy and data security are further protected through Drupal-based encryption, role-based access control, and secure session management. The platform's security architecture is designed to mitigate high-stakes risks inherent to defence contexts:

- Supply Chain Attacks: The risk of malicious tool listings is mitigated through a mandatory vetting and endorsement process for all vendors.
- Adversarial AI Risks: By mapping tools to ECSF profiles, the platform ensures human operators remain 'in-the-loop' to verify AI insights, preventing over-reliance on automated data.
- Data Integrity: Protection against exploitation is provided via Drupal-based encryption, role-based access control (RBAC), and resilience against SQL injection.

These mechanisms, along with resilience against vulnerabilities like SQL injection, ensure a trusted environment for sensitive maritime defence contexts. Feedback collected through pilot activities and ongoing security validation is used to refine marketplace features and guide future extensions, including the assessment of integrated toolchains. These results demonstrate that the NERO Marketplace is not a static catalogue but an evolving ecosystem, capable of supporting sustainable cybersecurity uptake and providing a solid foundation for maritime defence-oriented adaptations.

5.2. Training Implementation Outcomes and Lessons Learned

The NERO training activities conducted during Training Round I (February–April 2025) provide a robust evidence base on the effectiveness and practical conditions of delivering cybersecurity training to small and medium-sized organisations across multiple sectors. The trainees primarily originated from SMEs operating in healthcare, transport and logistics, finance, ICT, and other sectors. Therefore, the findings reflect cross-sector

SME training outcomes, offering insights that can inform potential adaptation to other operational domains, including maritime defence.

Four distinct training courses were delivered during Training Round 1: Cyber Ranges Training and Exercises, DeepGuardian Framework Hands-On, Software Security, and Gamified Scenario-Based Cybersecurity Training. Training effectiveness was evaluated through pre- and post-training questionnaires, covering participant profiling, cybersecurity knowledge and hygiene, training-specific content, and satisfaction levels. The first questionnaire was composed of a set of profiling questions, followed by general cybersecurity knowledge and best practices, while the second focused on generic cybersecurity hygiene, knowledge and best practices, and a set of dedicated questions related to the training core and satisfaction rate.

Overall participant satisfaction across the four courses was consistently high, approaching or exceeding the target threshold of 80%. Satisfaction rates ranged from 77% for the DeepGuardian Hands-On Training to 88% for the Software Security module, with Cyber Ranges and Gamified Trainings achieving 83% and 86%, respectively. Most trainees characterised the training content as clear, relevant, and useful for their professional or academic activities. The effectiveness of the training was measured against a target Key Performance Indicator (KPI) of 15% knowledge improvement. The results from the DeepGuardian training showed an average improvement of over 30%, doubling the initial target and providing a quantitative baseline for the platform's educational impact.

In terms of knowledge and improvement of awareness, measurable gains were observed in most training sessions. The DeepGuardian Hands-on Training demonstrated a particularly strong increase, with an average improvement of over 30% between pre- and post-training assessments, significantly exceeding the 15% NERO target KPI. The Gamified scenario-based training also achieved a knowledge increase above the target, while the Software Security training showed more modest gains.

Training completion rates emerged as the main challenge. While the DeepGuardian training achieved a 100% completion rate, three out of four trainings fell below the 80% target, with completion rates ranging between approximately 54% and 70%. Analysis indicated that these apparent dropouts were primarily due to non-completion of post-training questionnaires rather than early disengagement from the training itself, as supported by attendance records from both physical and virtual sessions. This distinction is important, as it suggests strong engagement during delivery but limitations in post-training questionnaire adherence. Attendance records from physical and virtual sessions confirm that active participation consistently exceeded 85% across all modules. This indicates that the 15–30% gap in reported completion rates (54–70%) represents a failure to submit the final administrative questionnaire rather than actual participant dropouts or role-specific disengagement. Figure 7 presents an overview of the answers collected for the different metrics used to evaluate the overall user satisfaction rate.

Hands-on exercises, cyber range simulations, and scenario-based approaches were consistently identified as strengths, contributing to higher engagement and practical understanding. At the same time, time constraints were frequently mentioned: sessions of 1.5–2 h were generally considered effective but tight, particularly for hands-on components. Additional feedback highlighted the value of modular expansion, clearer interconnection between training resources, and incentives such as certificates or micro-credentials to support completion.

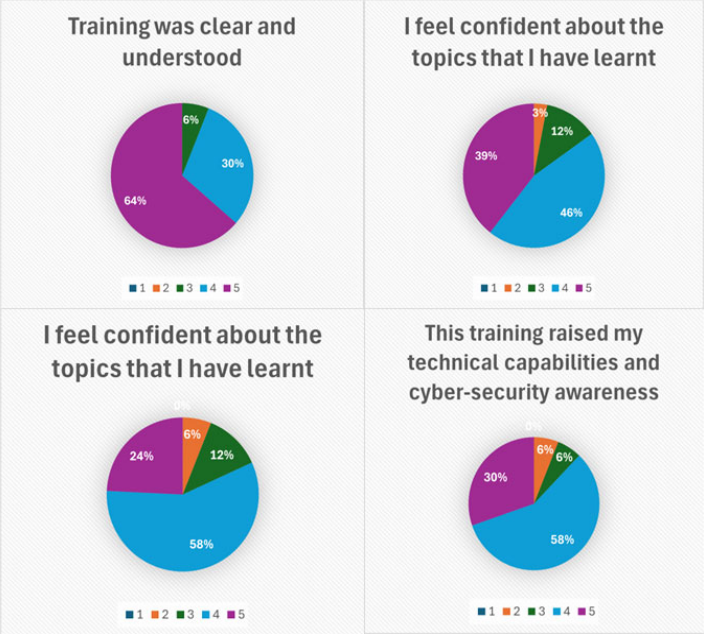

Figure 7. Aggregated Overview of Average Satisfaction Rate Metrics Collected During Training Round I.

Implications for Maritime Defence Contexts

Although the results collected so far do not stem from maritime-specific training delivery, they offer several relevant insights into the potential adaptation of NERO training programmes to maritime defence environments.

First, the consistently high satisfaction levels across diverse SME sectors suggest that the NERO training approach is broadly applicable and well received by participants with different operational backgrounds. This is particularly relevant for maritime defence, where personnel profiles range from highly technical IT specialists to operational staff, crew members, and port authority personnel.

Second, the observed challenges related to completion rates and time constraints are especially pertinent to maritime defence contexts. Maritime operators, ship crews, and port staff often operate under strict schedules, shift work, and limited availability. The findings suggest that micro-training and flexible delivery (i.e., synchronous and asynchronous, virtual and physical) would be particularly suitable for maritime environments.

Third, the strong positive feedback on hands-on exercises, cyber ranges, and scenario-based training is highly relevant for maritime defence. Maritime systems are characterised by complex cyber–physical interactions involving operational technology, communication systems, and safety-critical processes. The demonstrated effectiveness of cyber ranges and practical simulations implies that similar approaches could be valuable when contextualised for shipboard systems, port infrastructure, or maritime logistics networks, supporting experiential learning without exposing real systems to risk.

In environments where cybersecurity training competes with operational priorities, demonstrable value, recognition of participation, and practical relevance are likely to be decisive for successful adherence.

The Training Round I (trainees n = 234) included a representative distribution of professional roles, specifically IT administrators, non-technical staff, and management. This cross-section reflects the primary skill categories found within maritime port authorities and logistics SMEs, supporting the transferability of results to the maritime defence sector.

5.3. Applicability to Maritime Use Cases

The NERO cybersecurity ecosystem shows potential for maritime cybersecurity defence by looking at how it has been tested in the transportation and logistics area. From an operational and organisational perspective, this sector shares strong similarities with port-centric and maritime defence supply chains, where interactions between multiple stakeholders, digital platforms, and critical infrastructures are present. NERO's second use case (UC2), which focuses on strengthening supply-chain resilience, provides a suitable and realistic reference point for examining how NERO's capabilities can be transferred to maritime cybersecurity contexts. While direct validation in port environments or vessel systems is planned for future work, the Transport and Logistics use case (UC2) serves as a functional proxy to demonstrate the ecosystem's ability to manage multi-stakeholder supply chain risks. Furthermore, UC2 serves as a functional proxy for maritime defence because the transport and logistics SMEs involved face identical operational constraints. These include intermittent connectivity requiring robust data handling and legacy OT systems (like warehouse controllers) that share vulnerabilities with shipboard propulsion or cargo systems. By achieving knowledge gains of over 30% in these environments, the ecosystem demonstrates readiness for the maritime defence supply chain.

UC2 deals with cybersecurity issues in the world of maritime logistics. These include ensuring communication between different groups, keeping track of fleets, and making sure ports work together. Such factors may contribute to cyber attacks on digital services in ports and logistics to happen, which may result in operational disruption, including those related to physical space management. For instance, in the past, a hacked email system at a port led to a mix-up with ferry tickets, showing how cyber problems can affect safety, trust, and logistics among all the people involved.

This use case can prove how the NERO framework tackles important maritime cybersecurity problems. It achieve this by bringing together practical technical tools with training and validation activities. AI and machine learning techniques are increasingly employed in maritime cybersecurity tools to identify anomalous behaviour in network traffic, detect deviations in operational technology communications, and analyse large volumes of sensor and log data generated by port and logistics systems. Within the NERO ecosystem, such AI-enabled tools can be accessed and evaluated through the marketplace, allowing maritime organisations to explore advanced detection capabilities while complementing them with appropriate training and operational procedures.

The validation of UC2 also demonstrates that NERO's approach is well suited to maritime defence supply chains, which typically involve a diverse set of stakeholders, including SMEs, port authorities, and service providers with different levels of cybersecurity maturity. By bringing together multiple cybersecurity tools within a shared marketplace and linking their use to clearly defined human roles, NERO supports the establishment of a common baseline of cybersecurity capabilities without requiring uniform or tightly integrated technological infrastructures. This approach is particularly valuable in maritime defence environments, where civilian and military actors often operate side by side and depend on shared digital and physical resources.

6. Conclusions

This paper analysed how the NERO cybersecurity ecosystem, integrating a human-centric marketplace with a competency-oriented training and awareness platform, can be leveraged to strengthen cyber readiness in maritime defence settings. By combining supported discovery and selection of cybersecurity solutions with structured upskilling pathways aligned to recognised skills profiles, NERO offers a practical mechanism to reduce adoption barriers and improve operational cybersecurity capacity across heterogeneous

maritime stakeholders, including SMEs embedded in defence-relevant supply chains. The modular design of both the marketplace and the training framework enables sector-specific contextualisation while retaining a consistent methodological core, supporting the development of role-aware training journeys and tool uptake strategies that match the operational constraints of maritime environments. In particular, the integration of AI-enabled cybersecurity tools within the marketplace highlights the growing role of machine learning-based detection and analytics in modern cyber defence, while the training platform ensures that users develop the competencies required to interpret and operationalise AI-generated insights.

As a takeaway, the NERO training framework is explicitly constructed to support reuse and contextualisation across different domains. As such, NERO provides a solid and adaptable foundation upon which maritime defence-oriented cybersecurity training could be developed, building on existing content, tools, and pedagogical approaches without requiring fundamental redesign.

The principal limitation of this work is that the empirical evidence reported for training effectiveness originates from cross-sector pilots rather than from deployments in maritime defence organisations or maritime critical infrastructure operators. While NERO uses a vetting process to mitigate risks, a formal platform threat model and longitudinal studies on competence retention remain future priorities. These results imply that maritime cybersecurity must shift from generic awareness to role-specific technical training integrated directly into OT safety workflows. Consequently, while the analysis motivates transferability, the results cannot be interpreted as direct evidence of effectiveness in shipboard, port, or defence-operational contexts, where constraints such as intermittent connectivity, legacy OT dependencies, safety-critical operations, and multi-actor governance can significantly shape both training delivery and tool adoption. In addition, the evaluation metrics emphasise short-term outcomes (e.g., satisfaction and pre/post knowledge gains) and do not yet capture longer-term behavioural change, sustained competence retention, or measurable impacts on incident frequency, response quality, or resilience outcomes across maritime systems. Finally, the paper focuses on adaptation potential rather than full technical integration with maritime operational workflows and sector-specific assurance requirements, which would require targeted validation in representative environments.

Future work should prioritise domain-grounded validation of NERO through maritime-focused pilots that reflect realistic operational conditions across vessels, ports, and maritime defence supply chains. This includes developing and evaluating maritime-specific cyber range exercises (e.g., ship-shore communications, port community systems, navigation and positioning disruptions, and OT-centric scenarios), enriching the marketplace taxonomy with maritime-relevant solution categories and assurance attributes, and aligning training outcomes with sectoral roles and responsibilities under safety and security management processes. Longitudinal evaluation designs should be adopted to assess retention, behavioural change, and operational impact, complemented by measurement of resilience indicators relevant to critical maritime infrastructures (e.g., detection-to-response time, recovery performance, and continuity of safety-critical functions). Finally, integrating micro-credentialing and modular training delivery tailored to shift-based maritime work patterns may improve training completion and uptake, while structured collaboration with port authorities, defence stakeholders, and SME providers can support scalable dissemination and sustained ecosystem growth. A primary limitation of this evaluation is its focus on immediate knowledge gains and user satisfaction. While NERO employs a vetting process for tools, a formal platform threat model and longitudinal studies to measure long-term skill retention remain areas for future work.

Author Contributions: Conceptualization, K.K.; methodology, D.K. (Dimitrios Kallergis), D.K. (Dimitrios Koutras) and W.M.; software, W.M., P.T. and E.S.; validation, W.M., P.T. and D.K. (Dimitrios Koutras); formal analysis, D.K. (Dimitrios Koutras), W.M. and P.T.; investigation, D.K. (Dimitrios Kallergis) and D.K. (Dimitrios Koutras); resources, E.S., W.M. and P.T.; data curation, W.M. and P.T.; writing—original draft preparation, K.K., E.S., D.K. (Dimitrios Koutras), W.M., P.T. and D.K. (Dimitrios Kallergis); writing—review and editing, K.K. and E.S.; visualisation, E.S. and W.M.; supervision, K.K.; project administration, K.K. and E.S.; funding acquisition, K.K. All authors have read and agreed to the published version of the manuscript.

Funding: The authors would like to acknowledge the financial support provided for the following project: the 'Advanced Cybersecurity Awareness Ecosystem for SMEs' (NERO) project, which has received funding from the European Union's DEP programme under grant agreement No. 101127411. The views expressed in this paper represent only the views of the authors and not those of the European Commission or the partners in the above-mentioned project.

Data Availability Statement: Data are contained within the article. The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: Authors Kitty Kioskli and Eleni Seralidou were employed by the company trustilio B.V. Author Wissam Mallouli was employed by the company Montimage. Author Pedro Tomás was employed by the company OneSource Consultoria Informática Lda. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. United Nations Conference on Trade and Development. Review of Maritime Transport 2024: Navigating Maritime Chokepoints (UNCTAD/RMT/2024). 2024. Available online: https://unctad.org/publication/review-maritime-transport-2024 (accessed on 7 December 2025).
2. Ben Farah, M.A.; Ukwandu, E.; Hindy, H.; Brosset, D.; Bures, M.; Andonovic, I.; Bellekens, X. Cyber security in the maritime industry: A systematic survey of recent advances and future trends. *Information* **2022**, *13*, 22. [CrossRef]
3. Liu, G.; Amri, O.; Liang, Y.; Zhang, Z.; Merino Laso, P.; Bertelle, C.; Berred, A.; Lefebvre, D. Survey and future trends for cybersecurity in maritime and port sectors: A discrete event systems perspective. *Mathematics* **2025**, *13*, 3650. [CrossRef]
4. International Maritime Organization. Resolution MSC.428(98): Maritime Cyber Risk Management in Safety Management Systems. 2017. Available online: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf (accessed on 7 December 2025).
5. International Maritime Organization. Maritime Cyber Risk. Available online: https://www.imo.org/en/ourwork/security/pages/cyber-security.aspx (accessed on 7 December 2025).
6. DNV. Maritime Cyber Security Regulations. Available online: https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/regulations/ (accessed on 7 December 2025).
7. European Union Agency for Cybersecurity. ENISA Transport Threat Landscape. 2023. Available online: https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape (accessed on 7 December 2025).
8. Chupkemi, D.C.; Mersinas, K. Challenges in Maritime Cybersecurity Training and Compliance. *J. Mar. Sci. Eng.* **2024**, *12*, 1844. [CrossRef]
9. Raymaker, A.; Kumar, A.; Wong, M.Y.; Pickren, R.; Chhotaray, A.; Li, F.; Zonouz, S.; Beyah, R. A sea of cyber threats: Maritime cybersecurity from the perspective of mariners. In *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security*; Association for Computing Machinery: New York, NY, USA, 2025; pp. 588–602. [CrossRef]
10. Clavijo Mesa, M.V.; Patino-Rodriguez, C.E.; Guevara Carazas, F.J. Cybersecurity at sea: A literature review of cyber-attack impacts and defences in maritime supply chains. *Information* **2024**, *15*, 710. [CrossRef]
11. Martínez, F.; Sánchez, L.E.; Santos-Olmo, A.; Rosado, D.G.; Fernández-Medina, E. Maritime cybersecurity: Protecting digital seas. *Int. J. Inf. Secur.* **2024**, *23*, 1429–1457. [CrossRef]
12. Dominguez-Péry, C.; Vuddaraju, L.N.R.; Corbett-Etchevers, I.; Tassabehji, R. Reducing maritime accidents in ships by tackling human error: A bibliometric review and research agenda. *J. Shipp. Trade* **2021**, *6*, 20. [CrossRef]
13. Miller, T.; Durlik, I.; Kostecka, E.; Sokołowska, S.; Kozlovska, P.; Zwolak, R. Artificial intelligence in maritime cybersecurity: A systematic review of AI-driven threat detection and risk mitigation strategies. *Electronics* **2025**, *14*, 1844. [CrossRef]

14. Badea, M.; Bucovețchi, O.; Gheorghe, A.V.; Hnatiuc, M.; Raicu, G. Maritime industry cybersecurity threats in 2025: Advanced persistent threats (APTs), hacktivism and vulnerabilities. *Logistics* **2025**, *9*, 178. [CrossRef]
15. Makrakis, G.M.; Pijpker, J.; Hassing, R.; Loves, R.; McCombie, S. Salty Seagull: A VSAT honeynet to follow the bread crumb of attacks in ship networks. *arXiv* **2025**, arXiv:2508.11325. [CrossRef]
16. Tatar, B.; Karabacak, B.; Keskin, O.F.; Foti, D.P. Charting new waters with CRAMMTS: A survey-driven cybersecurity risk analysis method for maritime stakeholders. *Comput. Secur.* **2024**, *145*, 104015. [CrossRef]
17. Schinas, O.; Metzger, D. Cyber-seaworthiness: A critical review of the literature. *Mar. Policy* **2023**, *151*, 105592. [CrossRef]
18. Dimakopoulou, A.; Rantos, K. Comprehensive analysis of the maritime cybersecurity landscape based on the NIST CSF v2.0. *J. Mar. Sci. Eng.* **2024**, *12*, 919. [CrossRef]
19. Ćelić, J.; Vukšić, M.; Baždarić, R.; Cuculić, A. The challenges of cyber resilience in the maritime sector: Addressing the weak awareness of the dangers caused by cyber threats. *J. Mar. Sci. Eng.* **2025**, *13*, 762. [CrossRef]
20. Progoulakis, I.; Rohmeyer, P.; Nikitakos, N. Cyber physical systems security for maritime assets. *J. Mar. Sci. Eng.* **2021**, *9*, 1384. [CrossRef]
21. Kechagias, E.P.; Chatzistelios, G.; Papadopoulos, G.A.; Apostolou, P. Digital transformation of the maritime industry: A cybersecurity systemic approach. *Int. J. Crit. Infrastruct. Prot.* **2022**, *37*, 100526. [CrossRef]
22. Dominguez-Péry, C.; Merino Laso, P. A literature review and a bibliometric analysis of cybersecurity in ships maritime navigation. *ARIS2—J.* **2024**, *4*, 111–131. [CrossRef]
23. Koutras, D.; Malamas, V.; Kotzanikolaou, P.; Dasaklis, T. A risk assessment methodology for supply chain tracking services. In *Proceedings of the 2023 International Conference on Cyber Management and Engineering (CyMaEn)*; IEEE: New York, NY, USA, 2023; pp. 555–559. [CrossRef]
24. Koutras, D.; Grigoriadis, C.; Papadopoullos, M.; Kotzanikolaou, P.; Douligeris, C. Automating environmental vulnerability analysis for network services. In *Proceedings of the 2022 IEEE Symposium on Computers and Communications (ISCC)*; IEEE: New York, NY, USA, 2022; pp. 1–7. [CrossRef]