A Data-Driven Assessment of the Web Cyberattack Surface: The case study of the Livorno Maritime-Logistic Ecosystem

Gianluca Dini
Dept. of Information Engineering
University of Pisa,
Pisa, Italy
gianluca.dini@unipi.it

Sergio V. Zambelli
Dept. of Information Engineering
University of Pisa,
Pisa, Italy
s.zambelli@studenti.unipi.it

Martina Neri
Centre for Logistics Systems
University of Pisa,
Livorno, Italy
martina.neri@pologistica.unipi.it

Federico Niccolini
Dept. of Political Sciences
University of Pisa,
Pisa, Italy
federico.niccolini@unipi.it

***Abstract*—The maritime-logistics sector is a fundamental component of smart cities and is increasingly exposed to cyber threats because of progressive digitalization. This paper presents a reproducible, low-intrusion method for measuring the publicly observable web attack surface of organizations in a port community. The workflow identifies official domains, captures traffic generated by ordinary browsing, applies OWASP ZAP passive rules, exports alert severity, confidence, and occurrence counts, and aggregates them into site- and group-level *comparative exposure indexes*. A case study of 109 websites in the Port of Livorno ecosystem reveals marked heterogeneity: eleven alert types account for approximately 90% of detections, three sites exceed an illustrative exposure threshold of 4, and group averages range from 0.26 for shippers to 1.48 for terminal operators. The index is an alert-prioritization proxy rather than a measure of cyber risk because it excludes exploitability, likelihood, asset criticality, business impact, internal infrastructure, and cascading effects. The method supports ecosystem-level triage and repeatable monitoring but requires independent validation before risk claims can be made.**

***Index Terms*—cybersecurity, maritime-logistics, web attack surface, OWASP ZAP, exposure assessment**

I. Introduction

The maritime-logistics sector is a fundamental component of smart cities and is increasingly exposed to cyber threats because of progressive digitalization. While this growing digitalization brings undeniable advantages, it also makes maritime-logistics infrastructure an attractive target for malicious actors [1]–[5].

In the context of smart cities, cyberattacks raise concerns about systemic risk, as they can propagate across interconnected actors and infrastructures, amplifying their impact beyond individual organizations [6]. In response, the regulatory frameworks have been strengthened. For example, at the European level, directives such as NIS2 emphasize cybersecurity requirements for essential and important entities, including transport and logistics infrastructures [7]. These frameworks can be framed within a cyber-resilience approach [8]–[10]. Nevertheless, translating high-level regulatory requirements into actionable, context-aware practices remains challenging.

A key issue in this context is the scarcity of tools that allow port authorities or smart city managers to obtain a quantitative and system-level understanding of *cyber exposure*. Although individual organizations may conduct internal security assessments, there is limited visibility at the ecosystem level, where vulnerabilities often arise from inter-dependencies among actors, services, and digital platforms [11]. This limitation hinders the ability to incorporate cybersecurity as a measurable and manageable dimension of resilience [12].

This paper addresses this gap by focusing on the case study of the maritime-logistic ecosystem associated with the Port of Livorno, Italy, a major commercial and passenger port with strategic regional and international importance, ranking among the most significant ports in the Northern Tyrrhenian Sea. Specifically, the paper focuses on the network of companies interacting through the Tuscan Port Community System of the Northern Tyrrhenian Sea Port System Authority. The main motivations and contributions of this work are threefold.

First, we propose a methodological tool that enables port authorities to: (i) gain a quantitative perception of the cyberattack surface of organizations operating within their ecosystem; and (ii) develop operational guidelines to improve organizational awareness and cybersecurity preparedness.

Second, we present a prototype based on non-intrusive passive scanning. The tool leverages OWASP Zed Attack Proxy (ZAP) to passively scan publicly accessible web resources of selected organizations, extracting structured evidence of potential security weaknesses without interacting with or disrupting target systems.

Third, we empirically assess the ecosystem's cybersecurity

posture by defining indexes that enable both comparative analysis across heterogeneous organizations and prioritization of interventions. The index supports data-driven cyber exposure monitoring and can be integrated into smart city dashboards for infrastructure oversight and decision support.

The aim is not to introduce a new vulnerability-analysis or cyber-risk assessment method. The proposed method and tool provide a sector authority with a comparative view of publicly observable alerts across the organizations under its jurisdiction. They help identify recurring technical issues for ecosystem-wide guidance and organizations that may warrant closer attention. Detailed vulnerability analysis, cyber-risk assessment, and remediation remain the responsibility of each organization.

Overall, this work advances the smart city research agenda by bridging high-level regulatory frameworks and data-driven operational methods for cybersecurity management in critical infrastructure. It proposes a scalable and replicable methodology to characterize the cybersecurity posture of maritime-logistics ecosystems, supporting analytical evaluation, operational decision-making, and the integration of cyber resilience into port and smart city governance.

II. Related Work

Cybersecurity in the maritime and logistics sector has attracted increasing attention in recent years because of the growing digitalization process and the emergence of cyber-physical threats.

A first line of literature examines cyber risk and documented incidents in the maritime domain. Katzikas *et al.* review the state of maritime cybersecurity [13], while Atmoko *et al.* analyse vulnerabilities affecting vessels, port systems, logistics networks, and cargo management platforms [14]. Complementarily, Senarak discusses fifteen port cyberattack case studies from 2011 to 2023 [2], and Neri *et al.* assess eight attacks against maritime organizations to examine the resilience practices adopted in response to cyber threats [3].

ENISA and other organizations have issued reports on maritime threat landscapes, best practices, and sector-specific risk management approaches [15], [16]. Although valuable at the strategic level, these contributions generally do not provide operational methodologies for quantitatively assessing the exposure of specific port ecosystems.

Harry *et al.* propose an OSINT-based methodology to quantify and aggregate the size, diversity, and severity of cyberattack surfaces across geographically distributed organizations, validating it through a large-scale study of U.S. county government infrastructures [17]. Their work is close to ours in adopting a data-driven and passive assessment paradigm based on externally observable evidence, including publicly accessible web resources, to derive quantitative indicators for comparing heterogeneous entities.

However, the two approaches differ in scope, data sources, and risk modelling. While Harry *et al.* integrate multiple OSINT sources, such as Censys, Shodan, and NVD, to reconstruct infrastructure-level attack surfaces across thousands of organizations, our work focuses on a defined port-community ecosystem and leverages OWASP ZAP passive scanning to create alert-based indexes for operational comparison and decision support. Furthermore, while Harry *et al.* explicitly combine vulnerability severity and exploitation likelihood to approximate cyber risk, our methodology emphasizes indicators derived from passive scanner alerts to support ecosystem-level assessment.

Automated black-box web vulnerability scanners are established tools for scalable assessment of externally observable weaknesses. Prior studies show that, although effective for detecting common vulnerabilities, their coverage remains partial, particularly for complex, logic-based flaws and dynamic web content [18], [19]. Comparative evaluations, including those involving OWASP ZAP, further reveal substantial variability in detection accuracy across tools and vulnerability classes [20]. At the same time, sector-specific applications of ZAP and large-scale analyses of HTTP security headers and web configurations confirm the value of passive, low-intrusion measurement for assessing externally visible cybersecurity posture [21]–[23].

In summary, the literature recognizes the strategic relevance of cybersecurity in maritime contexts and offers valuable contributions on threats, frameworks, and assessment techniques. However, integrated data-driven methodologies enabling port authorities to quantitatively assess ecosystem-wide attack surfaces and derive actionable insights remain limited. This gap motivates our approach, which combines passive scanning with organization- and sector-level exposure indexes.

III. Methodology

This section describes the adopted methodology for assessing the cyberattack surface of the maritime-logistic ecosystem associated with the Port of Livorno. The methodology is designed to be non-intrusive, reproducible, and scalable, enabling a port authority to monitor and compare the cybersecurity posture of its reference community. We adopt a case study approach that is suitable for investigating complex, real-world phenomena within their contextual boundaries [24].

The methodology comprises three main phases: i) identification of the target ecosystem, ii) passive scanning, and iii) definition and computation of comparative cyber-exposure indexes.

A. Target Ecosystem Identification

The first step defines the organizations composing the reference ecosystem. In this work, we focus on companies interacting through the *Tuscany Port Community System* (TPCS) of the Northern Tyrrhenian Sea Port Authority (https://tpcs.tpcs.eu/login-en.aspx). TPCS is a collaborative web platform that connects public authorities and private operators, supporting the integration and automation of logistics, documentation, import/export, and port operations.

For each organization participating in the TPCS, we collected publicly available information, including its official web domain, which constitutes a main externally exposed interface

and a potential access point for attackers. This phase produced a dataset of 109 target websites, each associated with an organization operating within the port ecosystem. For privacy reasons, in the rest of this paper we will refer to organizations by means of integer pseudonyms in the range $[1, 109]$.

B. Passive Scan with OWASP ZAP

The second phase consists of performing a passive scan of the identified corporate websites. To this end, we employed the OWASP Zed Attack Proxy (ZAP), a widely adopted open-source tool for web application security testing (https://www.zaproxy.org/).

Unlike active scanning techniques, passive scanning analyzes observed HTTP/WebSocket traffic without injecting payloads or altering server state, actions that may disrupt services. This distinction is central for ethically scanning real organization websites, since passive methods reduce operational risk while still detecting issues such as missing headers, insecure cookies, information disclosure, mixed content, or vulnerable client-side components.

For each target website, ZAP collects HTTP/HTTPS responses during standard browsing. ZAP then analyses the collected traffic and generates a set of *alerts*. An alert indicates that some evidence matches a known security-relevant pattern but does not prove exploitability through attack attempts. While a vulnerability is a validated weakness of a system, an alert is a warning requiring further investigation rather than evidence of a confirmed vulnerability. Alerts are thus inputs to vulnerability assessment.

Each alert is described by a *severity level*, indicating potential impact, a *confidence level*, indicating detection reliability, and the *number of instances*, capturing its observed frequency. ZAP classifies severity as informational, low, medium, or high, and confidence as low, medium, or high.

The output of this phase is a structured JSON report containing the alerts detected for each analyzed website, which forms the empirical basis for the quantitative analysis.

Passive scanning with ZAP provides an empirical approximation of the observable attack surface of web applications, understood as a subset of the broader attack surface defined by NIST [25]. Although not exhaustive, this approach enables a consistent, scalable, and comparative assessment of externally observable security indicators.

From an ethical and legal perspective, the assessment was conducted without prior authorization because it was limited to passive observation of publicly accessible web resources and involved no authentication attempts, active probing, exploitation, or modification of target systems. Given its passive and non-intrusive nature, the authors deemed formal ethical approval unnecessary. No individual notification, disclosure, or remediation process was undertaken. To reduce potential harm, organizations were pseudonymised, results were reported mainly in aggregate, and potentially identifying or exploitable technical details were omitted.

Finally, we remark that false positives and false negatives are intrinsic limitations of passive scanning because it identifies alerts based on observed traffic rather than confirming vulnerabilities through active testing. Alerts should therefore be treated as indicators requiring further investigation, not as verified vulnerabilities.

C. A comparative cyber exposure index

We define an index whose goal is not to estimate absolute cyber risk but to support comparisons between organizations. Let i denote an organization and j be an alert detected by ZAP during a scan of that organization. For such an alert, we denote by S_{ij} its severity level, by C_{ij} its confidence level, and by N_{ij} the number of occurrences observed during the scan. We define the *cyber exposure index* associated with alert j of organization i as $I_{i,j} = S_{ij} \times C_{ij}$.

The *organization-level cyber-exposure index* IS_i of the organization i is defined as

$$IS_i = \frac{\sum_j (I_{ij} \times \ln(1 + N_{ij}))}{E_i} \tag{1}$$

where $E_i \geq 1$ denotes the organization's *structural exposure*, namely the number of externally visible, distinct web assets that contribute to the organization's observable attack surface.

The proposed index IS_i is a proxy exposure and prioritization indicator that aggregates the severity and reliability of scanner findings into a single score. It is not a cyber-risk metric and should not be interpreted as such. Unlike CVSS [26], FAIR [27], or NIST-based risk assessment frameworks [28], IS_i does not model threat likelihood, exploitability, asset criticality, business impact, or organizational context. Instead, it relies solely on passive web-scanning evidence and is intended to support scalable exposure monitoring, relative comparison, and prioritization across organizations. Similarly, unlike MITRE ATT&CK [29], it does not characterize adversary behaviour or attack sequences.

Accordingly, a high index value does not establish that an organization is vulnerable or at high cyber risk. It only indicates that the organization should receive greater attention and independently verify the observed alerts.

In (1), the logarithm limits the influence of repeated alerts, while normalization by E_i reduces bias from differences in the number of web assets, enabling fairer comparisons among organizations.

Finally, the set of organizations can be partitioned into disjoint non-empty groups according to selected criteria. For example, organizations may be grouped according to economic scale (micro, small, medium, and large enterprises) or business activity (e.g., freight forwarders, transport operators, and terminal operators). Given a partition $\mathcal{P}$, we define the *group-level cyber-exposure index* for group $P \in \mathcal{P}$, and denote it by IG_P, as $IG_P = \frac{1}{N_P} \sum_{i \in P} IS_i$, where N_P is the number of organizations in the group P.

To compute the indexes, qualitative severity and confidence labels are mapped to numerical values. Severity levels are mapped as follows: informational $= 0$, low $= 1$, medium $= 3$, and high $= 5$. Confidence levels are mapped as follows: low $= 0.5$, medium $= 0.75$, high $= 1$. The selected heuristic

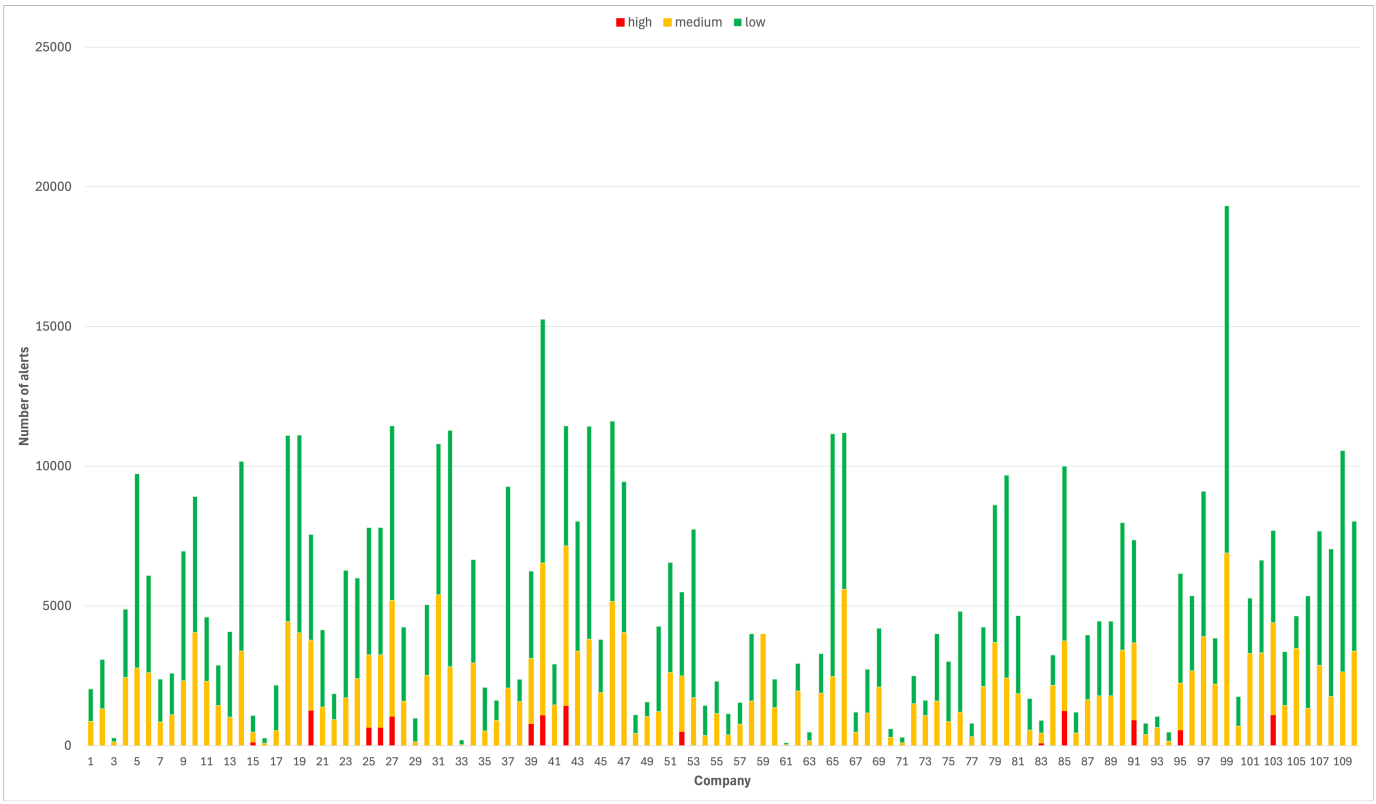


Fig. 1. Distribution of alerts over organizations.

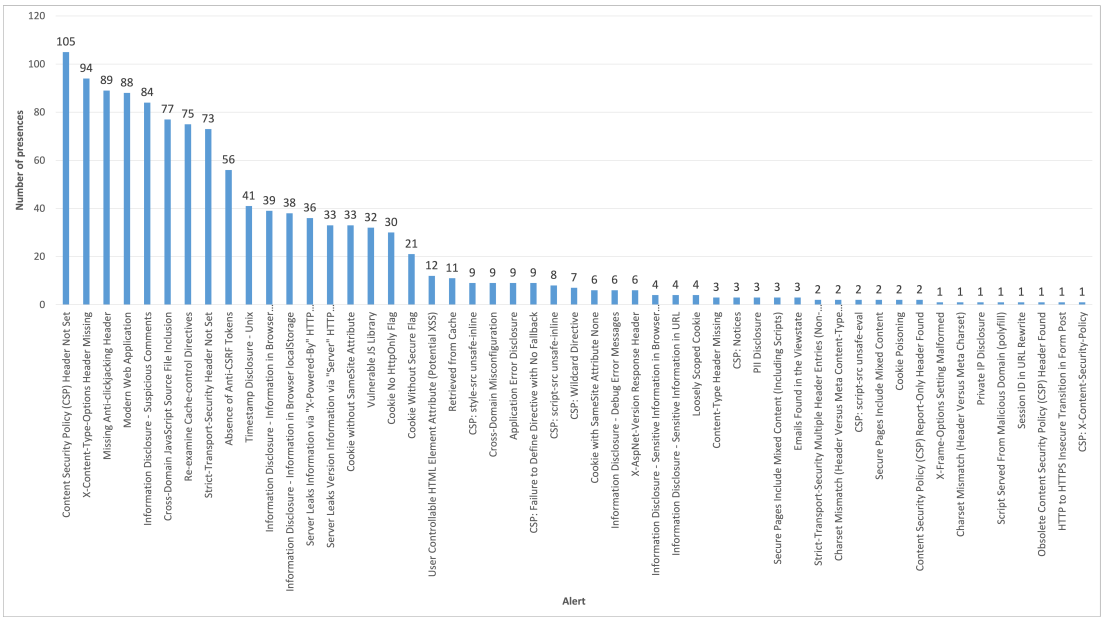


Fig. 2. Number of website scans in which each passive alert type was detected.

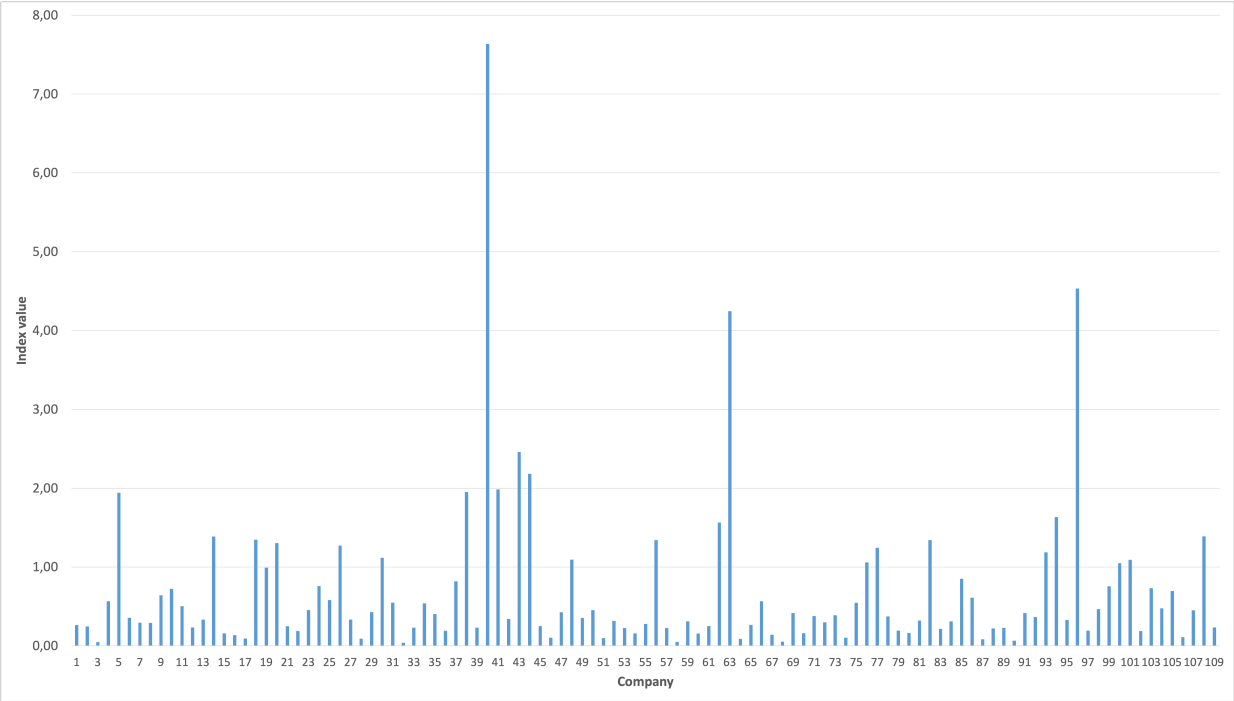


Fig. 3. Organization-level cyber-exposure index for each pseudonymized organization.

weights follow OWASP ZAP's severity and confidence rankings, giving higher scores to more severe and reliable alerts. They are not probabilities or estimates of financial loss, so the index supports prioritization rather than measuring cyber risk. Although other mappings are possible, the selected values provide a simple and transparent way to distinguish alerts by their operational relevance.

IV. Discussion

The application of the proposed methodology to the case study of the port of Livorno ecosystem revealed several relevant insights.

First, the overall landscape appears highly heterogeneous. Figure 1 shows the number and severity of alerts (y-axis) associated with each organization (x-axis). As shown in the figure, the analyzed organizations differ markedly in terms of both the number of detected alerts and their severity. This variability suggests that cybersecurity maturity is uneven across the maritime-logistic sector, likely reflecting differences in resources, awareness, and technological solutions adopted.

Second, the analysis helped identify the most frequent alerts in the ecosystem. Figure 2 shows each alert type (x-axis) and the number of scans in which the alert was detected (y-axis). For example, the `Content Security Policy (CSP) Header Not Set` alert appeared in 105 scans.

The figure highlights that a relatively small subset of alert types accounts for the majority of detections. For example, the first eleven alert types account for approximately 90% of the detections. This finding is particularly relevant from an operational perspective as it allows a port authority to prioritize mitigation guidelines targeting possible recurring weaknesses, thereby supporting a broad improvement in the overall security posture with relatively limited effort.

Third, a key contribution is the IS index, which serves as a practical indicator of what needs attention first. Figure 3 shows the IS value (y-axis) of each organization belonging to the ecosystem (x-axis) calculated as specified in (1). As illustrated in the figure, IS allows us to highlight sites that are potentially more exposed than others. For example, it turns out that organizations #40, #60, and #93 display descriptively higher index values than the other organizations. This is particularly relevant from an operational perspective, as it allows us to identify higher-priority sites within the ecosystem and provides a concrete basis for prioritizing interventions.

As a case study, we analyzed the public website of organization #40, which exhibits the highest IS value (7.63). The assessment identified several indicators suggesting possible weaknesses in software maintenance and cybersecurity governance, including outdated web technologies, legacy software components, and weaknesses in the configuration of publicly accessible services. More generally, the analysis revealed recurring issues related to software lifecycle management, web application hardening, and exposure of information that could facilitate subsequent attack phases.

To comply with responsible disclosure principles and minimize re-identification risks, detailed technical information is intentionally omitted. Nevertheless, the case illustrates how externally observable evidence obtained through passive analysis can help identify organizations that may require deeper security assessment and remediation efforts. More broadly,

it demonstrates that publicly available information alone can provide useful indicators for prioritizing cybersecurity interventions within a port ecosystem.

Finally, we also calculated group-level indexes using partitions based on economic size and business activity. Space limitations prevent a complete discussion. However, in summary, we observed that small enterprises have a higher index (0.80) than medium enterprises (0.75), whereas large enterprises have the lowest index value (0.52). This difference may reflect variations in resources, digital footprint, asset composition, or other factors not measured in this study. Micro enterprises, on the other hand, have a lower exposure index (0.62) than medium enterprises. However, this result should be interpreted with caution. Lower exposure of micro enterprises may not necessarily reflect better security practices, but rather a smaller digital footprint and, consequently, a smaller observable attack surface.

With regard to partitioning by business activity, the index varies from 0.26 for shippers to 1.48 for terminal operators, once again indicating substantial heterogeneity of the ecosystem in terms of cybersecurity posture.

V. Conclusions

This paper presented a low-intrusion workflow that uses OWASP ZAP passive alerts to compare web exposure across 109 organizations in the Port of Livorno ecosystem. The results identified recurring alerts and organizations requiring closer attention, supporting ecosystem-wide guidance and prioritization. The index measures alert exposure, not confirmed vulnerabilities or cyber risk. Future work will address validation, sensitivity analysis, and replication in other critical-infrastructure ecosystems.

Acknowledgement

The work was supported by the Centre for Logistics Systems of the University of Pisa in Livorno and by the EU NextGenerationEU program within the National Sustainable Mobility Center (CN00000023, Italian Ministry of University and Research Decree n. 1033—17/06/2022, Spoke 10).

We would like to thank the Northern Tyrrhenian Sea Port System Authority of Livorno, Italy, for helping us define the ecosystem of organizations analyzed.

References

[1] I. Yaqoob, K. Salah, R. Jayaraman, and Y. Al-Hammadi, "Cyber security issues and challenges in smart cities: A survey," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 55–89, 2021.

[2] C. Senarak, "Port cyberattacks from 2011 to 2023: a literature review and discussion of selected cases," *Maritime Economics & Logistics*, vol. 26, no. 1, pp. 105–130, 2024.

[3] M. Neri, M. Hofmann, and G. Dini, "Navigating cyber threats: an overview of cyber resilience in the maritime industry," in *2025 IEEE Int. Conf. Cyber Humanities (IEEE-CH)*, 2025, pp. 1–6.

[4] G. Potamos, S. Theodoulou, E. Stavrou, and S. Stavrou, "Building maritime cybersecurity capacity against ransomware attacks," in *Proc. Int. Conf. Cybersecurity, Situational Awareness and Social Media: Cyber Science 2022; 20–21 June; Wales*, 2023, pp. 87–101.

[5] O. Soner, G. Kayisoglu, P. Bolat, and K. Tam, "An investigation of ransomware incidents in the maritime industry: Exploring the key risk factors," *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, vol. 239, no. 4, pp. 659–678, 2025.

[6] C.-W. Ten, G. Manimaran, and C.-C. Liu, "Cybersecurity for critical infrastructures: Attack and defense modeling," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 40, no. 4, pp. 853–865, 2010.

[7] European Union, "Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the union (NIS2)," 2022.

[8] I. Linkov, D. A. Eisenberg, K. Plourde, T. P. Seager, J. Allen, and A. Kott, "Resilience metrics for cyber systems," *Environment Systems and Decisions*, vol. 33, no. 4, pp. 471–476, 2013.

[9] M. Neri, F. Niccolini, and F. Virili, "Organizational cyber resilience: toward an integrative conceptual framework," *Management Review Quarterly*, vol. 76, no. 1, pp. 789–840, 2026.

[10] D. Sepulveda Estay and P. Guerra, "The wave analogy of cyber-resilience as applied to shipping operations," in *Cybersecurity and Resilience in the Arctic*. SAGE Publications, London, UK, 2020, pp. 265–273.

[11] M. Gordan, D. A. Kountche, D. McCrum, S. Schauer, S. König, S. Delannoy, L. Connolly, M. Iacob, N. G. Durante, Y. Shekhawat *et al.*, "Protecting critical infrastructure against cascading effects: The precinct approach," *Resilient Cities and Structures*, vol. 3, no. 3, pp. 1–19, 2024.

[12] R. Roman, J. Lopez, and M. Mambo, "Cybersecurity and privacy in smart cities," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 51–57, 2018.

[13] S. K. Katsikas, G. Kavallieratos, and A. Amro, "Future trends in maritime cybersecurity," in *Computer and Information Security Handbook*. Elsevier, 2025, pp. 1663–1678.

[14] R. A. Atmoko, A. Z. Arfianto, M. K. Hasin, M. B. Rahmat, and L. A. Kurniawan, "Cybersecurity in digital maritime infrastructure," in *Maritime infrastructure for energy management and emission reduction using digital transformation*. Springer, 2025, pp. 127–183.

[15] A. Drougkas, A. Sarri, P. Kyranoudi, and A. Zisi, "Port cybersecurity: Good practices for cybersecurity in the maritime sector," European Union Agency for Cybersecurity (ENISA), Tech. Rep., 2019.

[16] A. Drougkas, A. Sarri, and P. Kyranoudi, "Cyber Risk Management for Ports: Guidelines for Cybersecurity in the Maritime Sector," European Union Agency for Cybersecurity (ENISA), Tech. Rep., 2020.

[17] C. Harry, I. Sivan-Sevilla, and M. McDermott, "Measuring the size and severity of the integrated cyber attack surface across US county governments," *Journal of Cybersecurity*, vol. 11, no. 1, p. tyae032, 2025.

[18] J. Bau, E. Bursztein, D. Gupta, and J. Mitchell, "State of the art: Automated black-box web application vulnerability testing," in *2010 IEEE Symp. Security and Privacy*, 2010, pp. 332–345.

[19] A. Doupé, M. Cova, and G. Vigna, "Why Johnny can't pentest: An analysis of black-box web vulnerability scanners," in *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer, 2010, pp. 111–131.

[20] B. Mburano and W. Si, "Evaluation of web vulnerability scanners based on OWASP benchmark," in *2018 26th International Conference on Systems Engineering (ICSEng)*. IEEE, 2018, pp. 1–6.

[21] Kasmawi, N. Hidayasari, and Mansur, "Vulnerability analysis using OWASP ZAP on higher education websites," in *AIP Conference Proceedings*, vol. 2665, no. 1. AIP Publishing LLC, 2023, p. 030015.

[22] A. Lavrenovs and F. J. R. Melón, "HTTP security headers analysis of top one million websites," in *Proc. 10th IEEE Int. Conf. Cyber Conflict (CyCon)*, 2018, pp. 345–370.

[23] U. Kishnani and S. Das, "Securing the web: Analysis of HTTP security headers in popular global websites," in *International Conference on Information Systems Security*. Springer, 2024, pp. 87–106.

[24] T. Hollweck, "Robert k. yin.(2014). case study research design and methods ." *Canadian journal of program evaluation*, vol. 30, no. 1, pp. 108–110, 2015.

[25] Joint Task Force, "Security and privacy controls for information systems and organizations," National Institute of Standards and Technology (NIST), Tech. Rep., 2020.

[26] P. Mell, K. Scarfone, and S. Romanosky, "Common vulnerability scoring system," *IEEE Security & Privacy*, vol. 4, no. 6, pp. 85–89, 2006.

[27] J. Freund and J. Jones, *Measuring and Managing Information Risk: A FAIR Approach*. Waltham, MA, USA: Butterworth-Heinemann, 2014.

[28] Joint Task Force Transformation Initiative, "Guide for conducting risk assessments," National Institute of Standards and Technology, NIST Special Publication 800-30 Revision 1, 2012.

[29] B. Al-Sada, A. Sadighian, and G. Oligeri, "MITRE ATT&CK: State of the art and way forward," *ACM Computing Surveys*, vol. 57, no. 1, pp. 1–37, 2024.