HOLISTIC SECURE PLATFORM FOR INTELLIGENT THREAT AWARENESS AND BUSINESS-CONTINUITY IN TRUSTED ADAPTIVE HEALTHCARE ENVIRONMENTS

Ioannis Chouchoulis[1*], Ioannis Makropodis[1], Aristeidis Farao [1,2], Vaios Bolgouras [2], Apostolis Zarras [2], Christos Xenakis[1,2]

[1] InQbit Innovations SRL, Romania
[2] University of Piraeus, Greece
**corresponding author*

Abstract

The EU healthcare sector is undergoing rapid digital transformation, improving care and efficiency but also expanding its cyberattack surface through EHRs, telemedicine, IoT devices, and cloud platforms. Ransomware, third-party risks, complex regulation, legacy systems, and AI-driven vulnerabilities make it necessary to develop a next-generation, scalable, and interoperable cybersecurity solution for healthcare. To address these challenges, we propose HOSPITABLE, a modular, interoperable, and scalable cybersecurity framework designed to strengthen the resilience of healthcare environments through the integrated use of artificial intelligence, automation, and compliance-aware security services. The proposed framework combines an AI-powered Security Operations Center with SIEM and SOAR capabilities to support real-time threat detection, automated incident response, and forensic logging. These core functions are complemented by a Privacy and Compliance Center for regulatory readiness, a zero-trust identity and access management layer, a Training and Awareness Center offering adaptive and gamified exercises for different staff roles, and risk and cost assessment tools that support cybersecurity planning and investment decisions. The architecture has been designed to operate across heterogeneous hospital infrastructures, including large hospital networks and smaller regional facilities, while preserving interoperability and deployment flexibility. This paper presents the architecture, methodology, and components of HOSPITABLE, with the aim of delivering an interoperable and holistic cybersecurity solution that addresses technical safeguards, staff preparedness, and compliance with the evolving EU regulatory landscape.

Keywords: healthcare cybersecurity, compliance, AI-powered SOC, SIEM/SOAR, ransomware resilience, zero-trust IAM, compliance, privacy, gamified training, risk & cost tools, awareness

1. Introduction

The healthcare sector is a cornerstone of the European Union's economy and social resilience. In 2023, the healthcare expenditure in the EU reached €1.72 trillion, equivalent to 10.0% of GDP [1], while general government expenditure on health represented 7.3% of GDP and hospital services alone accounted for 3.2% of GDP [2]. Beyond expenditure, the EU health and social work sector employed 13.1 million people and generated €579.5 billion in value added in 2021 [3], underlining its major economic and societal importance. Within this ecosystem, hospitals are particularly critical, as they play a central role in service delivery, patient safety, and continuity of care.

Cyberattacks and ransomware have become major threats to hospitals and healthcare providers, affecting not only sensitive data but also patient safety and continuity of care. Hospitals are particularly critical in this context, as the EU explicitly recognizes them as essential services, while the European Commission has highlighted that cyber incidents in

hospitals may delay medical procedures, create gridlocks in emergency departments, and disrupt vital services, with direct consequences for patient safety.

At the same time, the digital transformation of European health systems delivers substantial efficiency gains but also broadens the attack surface and heightens exposure to sophisticated cyber threats. Consequently, healthcare has emerged as one of the most exposed critical sectors in Europe, with 309 significant cybersecurity incidents reported in 2023 alone [4]. In line with this, ENISA identifies ransomware and data breaches as two of the most prominent threats affecting the healthcare domain [5]. The World Health Organization has further stressed that cyber incidents in healthcare can directly endanger safe service delivery [6]. Recent European incidents [7] [8] [9] [10] affecting European healthcare organizations further demonstrate the severity, operational impact, and persistence of cyber threats in the sector.

Furthermore, healthcare institutions remain unevenly prepared. Although frameworks such as GDPR, NIS2, and EHDS define an increasingly strong regulatory direction, many providers still lack formal response structures and sufficient cyber maturity [11]. The threat landscape has also been shaped by geopolitical instability in the wider European context, increasing the exposure of hospitals and healthcare services to disruptive cyber activity [12] [13] [14].

In response to these challenges, this paper presents HOSPITABLE as a modular, interoperable, and scalable cybersecurity framework for healthcare environments. The vision of HOSPITABLE is to strengthen the digital resilience of European hospitals and healthcare providers by embedding cybersecurity into everyday clinical and operational processes. To this end, the framework integrates a healthcare-oriented Security Operations Center for monitoring, detection, and response; a Privacy and Compliance Center for data protection and regulatory support; a Training and Awareness Center for staff preparedness; a Risk Management and Cost Assessment Center for risk-informed planning and investment decisions; and an Interaction Center for AI-assisted guidance and cross-stakeholder coordination. Collectively, these components are designed to support secure, compliant, and resilient healthcare service delivery across heterogeneous hospital infrastructures.

2. HOSPITABLE framework

HOSPITABLE is designed as a modular cybersecurity framework for healthcare environments, where digital resilience is directly linked to patient safety, continuity of care, and the protection of sensitive health data. Its architecture combines real-time security monitoring, automated response, privacy and compliance support, adaptive awareness mechanisms, and risk-informed decision assistance within a unified architectural framework. Rather than addressing these dimensions through isolated tools, HOSPITABLE integrates them into a coherent framework that can support heterogeneous hospital infrastructures while preserving operational continuity.

2.1 Architecture and Methodology

The HOSPITABLE architecture is structured around five interacting functional domains, including the Security Operations Center, the Privacy and Compliance Center, the Training and Awareness Center, the Risk Management and Cost Assessment Center, and the Interaction Center. Methodologically, these domains are connected through bidirectional information flows that link technical monitoring, regulatory control, organizational preparedness, and decision support into a common operational model.

At the core of the framework, the Security Operations Center correlates telemetry, threat intelligence, and anomaly signals, while exchanging information with the Privacy and Compliance Center to align detection and response processes with privacy-preserving rules, access policies, and regulatory requirements. In parallel, security events inform the Training and Awareness Center by identifying recurring human-related weaknesses, thereby enabling role-specific adaptation of awareness and training activities. Security telemetry is also propagated to the Risk Management and Cost Assessment Center, where incidents and vulnerabilities are translated into technical, operational, and financial risk indicators. These outputs are subsequently consolidated by the Interaction Center, which provides contextualized

recommendations to technical, clinical, and managerial stakeholders.

The methodology of HOSPITABLE follows a progressive integration logic in which information produced by each functional domain is reused by the others to support continuous adaptation. Compliance findings influence training priorities and risk evaluation, behavioural indicators derived from awareness activities contribute to the assessment of organizational exposure, and risk and cost models support strategic prioritization and deployment planning. A cross-cutting cyber threat intelligence layer further enriches detection, playbook refinement, awareness scenarios, and advisory outputs, enabling the framework to remain responsive to evolving threat conditions. This integration-oriented methodology allows HOSPITABLE to operate as a unified yet modular framework that can be incrementally adopted according to institutional needs, available resources, and cybersecurity maturity. An overview of the HOSPITABLE architecture and the interactions among its core functional domains, as well as the mapping of key supporting assets, is presented in **Figure 1**.

2.2 Core Platform Modules

In this section we present the modules that complement the HOSPITABLE.

2.2.1 AI-assisted Security Operations Center

The AI-assisted Security Operations Center constitutes the operational core of HOSPITABLE, providing continuous monitoring, threat detection, and coordinated incident response across heterogeneous healthcare infrastructures [15]. It is designed for environments in which legacy IT systems, medical IoT devices, laboratory platforms, and critical clinical applications coexist and produce heterogeneous security telemetry [16]. To address this complexity, the SOC integrates SIEM, SOAR, vulnerability management, cyber threat intelligence, and identity and access management within a unified architecture supported by machine learning, explainable AI, and immutable logging [17]. In addition, its design supports secure interoperability with healthcare-specific data formats and workflows, while preserving accountability and human oversight in critical response decisions.

Within this domain, ClinicShield SIEM supports telemetry ingestion and contextual threat analysis across hospital information systems, medical IoT devices, servers, and cloud services, while the RapidResponse Orchestrator automates containment and response through healthcare-oriented playbooks adapted to incidents such as ransomware, denial-of-service attacks, and unauthorised access attempts. MediScan360 Vulnerability Manager enhances asset visibility and supports risk-based prioritisation of weaknesses across IT and OT domains, whereas TrustCare IAM [18] secures identities and access through mechanisms such as multi-factor authentication, single sign-on, and context-aware trust validation. In parallel, HealthThreat Radar enriches detection with adversarial knowledge and supports proactive analysis, while ReguLedger Vault reinforces accountability through immutable logging. Together, these assets establish a healthcare-oriented SOC capable of combining technical visibility, automated response, and accountable incident handling, while remaining modular enough to support incremental adoption across hospitals with different levels of cybersecurity maturity.

2.2.2 Privacy & Compliance Center

The Privacy and Compliance Center addresses the need to protect sensitive health data while ensuring alignment with complex regulatory and ethical requirements [19]. In healthcare environments, where data protection, lawful processing, and accountability are essential, this module embeds privacy-by-design and compliance-by-design principles directly into digital operations. Its role extends beyond static policy enforcement, operating instead as a proactive layer that supports secure data use, transparency, and continuous regulatory readiness [20].

Operationally, this domain is supported by PrivGuard AI, which enables privacy-preserving handling of sensitive datasets through mechanisms such as anonymisation,

pseudonymisation, and adaptive data protection controls. In parallel, CompliMed Gateway continuously maps operational practices against applicable regulatory requirements, identifies gaps, and supports the generation of auditable reports. ReguLedger Vault further strengthens legal defensibility and traceability by supporting immutable consent and activity records. A distinctive feature of this module is the use of explainable AI to justify automated privacy and compliance decisions, thereby improving transparency and supporting trust among security teams, compliance officers, and institutional stakeholders.

2.2.3 Training & Awareness Center

The Training and Awareness Center addresses the human dimension of healthcare cybersecurity, recognizing that hospitals remain highly vulnerable to phishing, weak credential practices, and other human-related security weaknesses [21] [22]. Since clinical and administrative personnel operate under significant time pressure, awareness mechanisms must be adaptive, role-specific, and practically relevant rather than generic or static. This module is therefore designed to align cybersecurity learning with the operational realities of hospital work.

Its operation is supported by MediLearn Arena, which provides adaptive learning pathways tailored to different staff roles through personalised and continuously updated content. To improve engagement and reduce training fatigue, the module incorporates gamified and immersive learning experiences that simulate realistic hospital cyber incidents. In parallel, PhishGuard Trainer supports realistic phishing simulations and behavioural reinforcement based on the evolving threat profile of the environment. These mechanisms allow organisations to monitor participation, assess resilience improvements, and connect awareness outcomes to the wideρ security ecosystem [23]. Through this approach, the Training and Awareness Center contributes not only to knowledge transfer but also to the development of a sustained and measurable security culture.

2.2.4 Risk Management & Cost Assessment Center

The Risk Management and Cost Assessment Center translates technical security signals into operationally relevant and economically meaningful indicators [24]. In hospital environments, cybersecurity decisions are often constrained by limited budgets, competing priorities, and the difficulty of demonstrating the value of preventive investments. This module addresses that gap by linking cyber risk exposure with financial assessment and decision support [25].

At its core, this domain is implemented through MediRisk Navigator, which visualises risk across the healthcare environment through dashboards and scoring mechanisms that combine technical severity with contextual factors such as patient criticality, continuity-of-service implications, and regulatory impact. In parallel, CostGuard Evaluator estimates the potential financial consequences of incidents and compares them with the cost of preventive measures, producing return-on-security-investment and total-cost-of-ownership views. Together, these assets support more informed investment prioritisation and help healthcare organisations justify cybersecurity measures not only on technical grounds, but also in terms of operational resilience and financial sustainability [26].

2.2.5 Interaction Center

The Interaction Center serves as the integration and decision-support layer of the HOSPITABLE architecture. Its purpose is to transform outputs from the other modules into accessible and actionable guidance for different stakeholder groups, including technical personnel, clinical actors, and executive decision-makers. In complex healthcare environments, a central challenge lies not only in generating security insight but also in communicating it appropriately across organizational levels.

This module is realised through MediAssist Advisor and InsightBoard 360. MediAssist

Advisor functions as an AI-driven advisory assistant that synthesises information from monitoring, compliance, risk, and awareness components in order to provide contextualised and explainable guidance. InsightBoard 360 complements this function by consolidating outputs from the other modules into stakeholder-oriented recommendations and prioritised decision-support views. Together, these assets enable the Interaction Center to provide technical playbooks for IT staff, strategic summaries for management, and practical recommendations for operational users [27]. Through this role, it bridges the gap between technical cybersecurity functions and organizational decision-making [28], ensuring that the platform's intelligence is translated into concrete and usable action across the healthcare environment.

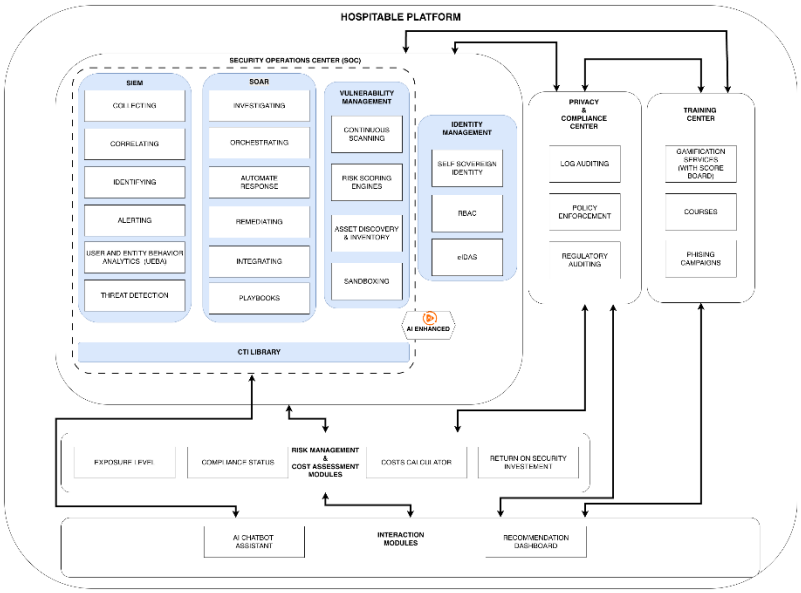

Figure 1. Overall architecture of the HOSPITABLE framework

3. Conclusions

HOSPITABLE offers a modular and interoperable framework for strengthening the cybersecurity of hospitals and healthcare providers against the growing spectrum of digital threats. By integrating functional domains such as the AI-assisted Security Operations Center, the Privacy and Compliance Center, the Training and Awareness Center, the Risk Management and Cost Assessment Center, and the Interaction Center, HOSPITABLE provides a holistic approach to healthcare cybersecurity that addresses technical protection, regulatory readiness, staff preparedness, and decision support. The adoption of an integration-oriented methodology ensures that security monitoring, compliance, awareness, and risk-informed planning are embedded across healthcare operations, enhancing resilience, trust, and continuity of care. Ultimately, HOSPITABLE aims to establish itself as a reference framework for resilient healthcare cybersecurity, promoting the development of secure, compliant, and trustworthy digital healthcare environments across Europe.

Acknowledgements

This research has been funded by the ANTIDOTE project funded under Grant Agreement No. 101183162 supported by Horizon Europe, by the NITRO and CyberAId with Grant Agreement No. 101145872 and 101249596 correspondingly, funded under the Digital Europe Programme.

References

[1] Eurostat, "Healthcare expenditure statistics - overview," European Commission, 2025. [Online]. Available: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Healthcare_expenditure_statistics_-_overview. [Accessed 6 April 2026].

[2] Eurostat, "Government expenditure on health," Statistics Explained , 2025. [Online]. Available: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Government_expenditure_on_health. [Accessed 6 April 2026].

[3] Eurostat, "News articles," Eurostat News, 22 March 2024. [Online]. Available: https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20240322-3. [Accessed 6 April 2026].

[4] European Commission, "Cybersecurity of hospitals and healthcare providers," Digital economy and society , 12 March 2026. [Online]. Available: https://commission.europa.eu/topics/digital-economy-and-society/cybersecurity-healthcare_en. [Accessed 9 April 2026].

[5] Prioritising eHealth cybersecurity against emerging challenges, "Prioritising eHealth cybersecurity against emerging challenges," 6 November 2024. [Online]. Available: https://www.enisa.europa.eu/news/prioritising-ehealth-cybersecurity-against-emerging-challenges. [Accessed 9 April 2026].

[6] World Health Organization, "WHO Director-General briefs the UN Security Council on ransomware attacks on healthcare," Departmental update, 26 November 2024. [Online]. Available: https://www.who.int/news/item/26-11-2024-who-director-general-briefs-the-un-security-council-on-ransomware-attacks-on-healthcare. [Accessed 9 April 2026].

[7] Stefan Krempl, "Ransomware: cyberattacks on large German hospitals on the decline," heise, 10 April 2024. [Online]. Available: https://www.heise.de/en/news/Ransomware-cyberattacks-on-large-German-hospitals-on-the-decline-9679711.html. [Accessed 9 April 2026].

[8] Wilkipedia, "Health Service Executive ransomware attack," [Online]. Available: https://en.wikipedia.org/wiki/Health_Service_Executive_ransomware_attack. [Accessed 9 April 2026].

[9] C. News, "Cybercriminals release more Hospital Clínic data on patients and staff," 17 April 2023. [Online]. Available: https://www.catalannews.com/society-science/item/cybercriminals-release-more-hospital-clinic-data-on-patients-and-staff. [Accessed 9 April 2026].

[10] S. J. H. Group, "Saint James Hospital Group: Cyber Security Incident," 11 July 2025. [Online]. Available: https://stjameshospital.com/cyber-security-update/. [Accessed 9 April 2026].

[11] Enisa, "ENISA THREAT LANDSCAPE: HEALTH SECTOR," European Union Agency for Cybersecurity (ENISA), 2023.

[12] Euronews, "European hospitals targeted by 'pro-Russian' hackers," 01 February 2023. [Online]. [Accessed 9 April 2026].

[13] J. Lyon, "Russian hacktivists DDoS hospitals, with pathetic results," The Register, 28 February 2023. [Online]. Available: https://www.theregister.com/2023/02/28/anonymous_sudan_ddos_hospitals/#:~:text=A%20series%20of%20distributed,centers%27%20operations%20or%20digital%20infrastructure. [Accessed 9 April 2026].

[14] NHS , "Synnovis cyber incident," NHS England, 10 November 2025. [Online]. Available: https://www.england.nhs.uk/synnovis-cyber-incident/. [Accessed 9 April 2026].

[15] L. A. a. I. M. Bushra A. Alahmadi, "99% False Positives: A Qualitative Study of SOC Analysts' Perspectives on Security Alarms," in *31st USENIX Security Symposium*, Boston, MA, USA, 2022.

[16] C. G. M. v. E. a. S. P. Lorenz Kustosch, "This paper is included in the Proceedings of the Security Updates for Connected Medical Devices," in *34th USENIX Security Symposium*, Seattle, WA, USA, 2025.

[17] M. M. C. P. D. V. Ronald E. Thompson, "There are rabbit holes I want to go down that I'm not allowed to go down": An Investigation of Security Expert Threat Modeling Practices for Medical Devices," in *33rd USENIX Security Symposium*, Philadelphia, PA, USA, 2024.

[18] G. P. M.-A. K. M. A. C. B. B. E. M. I. K. I. P. C. X. e. a. A. Farao, "Leveraging self-sovereign identity for e-health applications," in *International Symposium on Distributed Computing and Artificial Intelligence*, 2024.

[19] K. A. A. S. M. K. H. W. a. T. R. M. Raza Nowrozy, "Privacy Preservation of Electronic Health Records in the Modern Era: A Systematic Survey.," *ACM Comput. Surv. 56, 8, Article 204,* pp. 1-37 , August 2024.

[20] A. A. a. B. W. S. Qiyang Sun, "Explainable Artificial Intelligence for Medical Applications: A Review," *ACM Trans. Comput. Healthcare 6, 2, Article 17,* pp. 1-31, A[ro; 2025.

[21] L. C. a. E. S. Dawn Branley-Bell, "Promoting Cybersecurity Culture Change in Healthcare," in *Proceedings of the 14th PErvasive Technologies Related to Assistive Environments Conference (PETRA '21)*, New York, NY, USA, 2021.

[22] M. G. E. W. a. M. A. S. Markus Schöps, "Simulated Stress: A Case Study of the Effects of a Simulated Phishing Campaign on Employees' Perception, Stress and Self-Efficacy," in *Proceedings of the 33rd USENIX Security Symposium.*, Philadelphia, PA, USA, 2024.

[23] G. H. e. al., "Understanding the Efficacy of Phishing Training in Practice," in *2025 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, 2025.

[24] F. J. a. A. B. Sondes Ksibi, " Cyber-Risk Management within IoMT: a Context-aware Agent-based Framework for a Reliable e-Health System.," in *The 23rd International Conference on Information Integration and Web Intelligence (iiWAS2021)*, New York, NY, USA, 2021.

[25] S. P. C. X. a. E. P. Mohamed Ahmed, "MITRE ATT&CK-driven Cyber Risk Assessment," in *n Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES '22).*, New York, NY, USA, 2022.

[26] C. H. P. M. Ferda Özdemir Sönmez, "Decision support for healthcare cyber security," *Computers & Security, Volume 122,* 2022.

[27] H. S. L. S. a. V. Z. Neele Roch, "Navigating Autonomy: Unveiling Security Experts' Perspectives on Augmented Intelligence in Cybersecurity," in *Proceedings of the Twentieth Symposium on Usable Privacy and Security.*, Philadelphia, PA, USA, 2024.

[28] M. B. C. S. N. a. C. P. Fatemeh Jalalvand, "Alert Prioritisation in Security Operations Centres: A Systematic Survey on Criteria and Methods," *ACM Comput. Surv. 57, 2,,* pp. 1-36, February 2025.