NERO: Advanced Cybersecurity Awareness Ecosystem for SMEs

Charalambos Klitis*
eBOS Technologies Ltd
Nicosia, Cyprus
charalambosk@ebos.com.cy

Ioannis Makris
METAMIND INNOVATIONS IKE
Kozani, Greece
makris@metamind.gr

Pavlos Bouzinis
METAMIND INNOVATIONS IKE
Kozani, Greece
pbouzinis@metamind.gr

Dimitrios Christos Asimopoulos
METAMIND INNOVATIONS IKE
Kozani, Greece
mdasimopoulos@metamind.gr

Wissam Mallouli
MONTIMAGE EURL
Paris, France
wissam.mallouli@gmail.com

Kitty Kioskli
TRUSTILIO BV
Amsterdam, Netherlands
kitty.kioskli@trustilio.com

Eleni Seralidou
TRUSTILIO BV
Amsterdam, Netherlands
eleni.seralidou@trustilio.com

Christos Douligeris
UNIVERSITY OF PIRAEUS RESEARCH CENTER
Piraeus, Greece
cdoulig@unipi.gr

Loizos Christofi
eBOS Technologies Ltd
Nicosia, Cyprus
loizos.christofi@ebos.com.cy

ABSTRACT

NERO represents a sophisticated Cybersecurity Ecosystem comprising five interconnected frameworks designed to deliver a Cybersecurity Awareness initiative, as advocated by ENISA as the optimal method for cultivating a security-centric mindset among employees to mitigate the impact of cyber threats. It integrates activities, resources, and training to nurture a culture of cybersecurity. NERO primarily equips SMEs with a repository of Cyber Immunity Toolkits, a Cyber Resilience Program, and Gamified Cyber Awareness Training, all accessible through a user-friendly Marketplace. The efficacy and performance of this concept will be affirmed through three distinct use case demonstrations across various sectors: Improving Patient Data Security in Healthcare with Cybersecurity Tools, Enhancing Supply Chain Resilience in the Transportation and Logistics Industry through Cybersecurity Awareness, and Elevating Financial Security via Enhanced Cybersecurity Awareness and Tools.

CCS CONCEPTS

• **Security and privacy → Intrusion/anomaly detection and malware mitigation**; *Network security*; Human and societal aspects of security and privacy.

KEYWORDS

Cypersecurity, Cybersecurity-aware culture, SMEs, Healthcare, Transportation and Logistics, Finance

ACM Reference Format:
Charalambos Klitis, Ioannis Makris, Pavlos Bouzinis, Dimitrios Christos Asimopoulos, Wissam Mallouli, Kitty Kioskli, Eleni Seralidou, Christos Douligeris, and Loizos Christofi. 2024. NERO: Advanced Cybersecurity Awareness Ecosystem for SMEs. In *Proceedings of The 19th International Conference on Availability, Reliability and Security (ARES 2024).* ACM, New York, NY, USA, 8 pages. https://doi.org/XXXXXXX.XXXXXXX

ARES 2024, July 30 – August 2, 2024 , Vienna, AUST
2024. ACM ISBN 978-1-4503-XXXX-X/18/06
https://doi.org/XXXXXXX.XXXXXXX

1 INTRODUCTION

The geopolitical landscape has fostered a surge in cyberwarfare, hacktivism, and damaging cyberattacks. Ransomware, often initiated through phishing, and Distributed Denial of Service (DDoS) attacks are among the top risks identified in the 2017 study. Geopolitical events, notably the Russian invasion of Ukraine, have significantly influenced the global cyber environment, leading to a rise in threats and the emergence of new vectors like zero-day exploits and AI-enabled disinformation. Malicious attacks targeting various sectors, including ransomware, malware, social engineering, data breaches, and supply chain compromise, continue to pose significant risks[3–5].

Cybersecurity awareness is paramount in combating cybercrime and safeguarding organizations. Despite the proliferation of security measures, many organizations still fall victim to cyberattacks. The COVID-19 pandemic has exacerbated vulnerabilities in industries like finance, manufacturing, healthcare, and education, highlighting the urgent need for enhanced cybersecurity measures[1, 2].

Small and medium-sized enterprises (SMEs) are particularly vulnerable to cybercrime due to limited resources and expertise. The Eurobarometer survey conducted in 2021 revealed that 28% of European SMEs experienced cybercrime, with concerns ranging from online bank account hacking to phishing attacks. SMEs face challenges such as low awareness of cybersecurity threats, budget constraints, and a lack of specialized personnel[7, 8].

To address these challenges, SMEs need to prioritize cybersecurity and adopt intelligent technologies to detect and prevent cyber threats. The European Commission recognizes SMEs as crucial drivers of the economy, emphasizing the need for tailored cybersecurity solutions and support. ENISA provides guidance and action plans to help SMEs strengthen their cybersecurity posture and adapt to evolving threats[2].

As cyber systems become more complex, cyber resilience becomes increasingly vital. Industry 4.0 technologies, such as AI, cloud computing, and IoT, require robust cybersecurity measures to defend against sophisticated cyberattacks. Cyber immune systems,

inspired by the human adaptive immune system, play a crucial role in detecting and mitigating unknown cyber threats[6].

In summary, cybersecurity and cyber defense are essential components in today's increasingly digital world, requiring proactive measures to ensure cyber resilience and protect critical infrastructure and information assets.

2 NERO ECOSYSTEM

Figure 1 illustrates the high-level architecture of the NERO project, defining an ecosystem characterized by five distinct frameworks: ARCANA, VICTORIOUS, AUDACIOUS, CYBIT, and ASTRAS. Each framework assumes a unique role within the architecture, contributing to the overall functionality and effectiveness of the ecosystem.

In this section, our objective is to provide an overview of NERO's ecosystem and decode the pivotal roles of the various frameworks slated for development in the project. Additionally, we will commence a preliminary exploration of the communication dynamics between the frameworks, laying the foundation for a more comprehensive discussion in subsequent works.

This initial exploration serves as a precursor to dive deeper into the intricate interplay among the frameworks, illuminating how they collaboratively work to advance NERO towards its objectives. Through meticulous examination and analysis, our aim is to untangle the complex web of NERO's ecosystem, fostering a deeper understanding and guiding strategic decision-making in the project's trajectory.

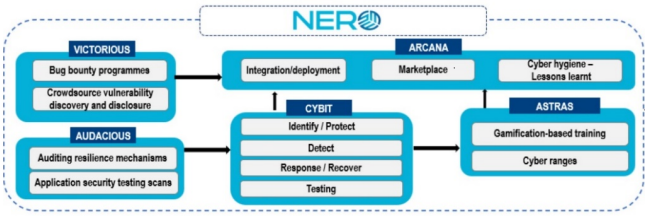

Figure 1: NERO high-level Ecosystem.

2.1 Market Oriented Cybersecurity Awareness training (ARCANA)

The ARCANA framework functions as the central interface within the ecosystem, housing NERO's marketplace, which serves as a centralized repository for all cybersecurity tools and training materials. The integration and deployment of cybersecurity tools within this marketplace are crucial for instilling cyber hygiene practices among SMEs. NERO is dedicated to seamlessly integrating its cybersecurity tools into the NERO marketplace platform, complemented by comprehensive training sessions for SMEs on their utilization and advantages.

Moreover, SMEs will receive extensive technical support following the deployment of these tools. Tool effectiveness will be monitored and analyzed on an ongoing basis to identify areas for enhancement. Well-coordinated awareness campaigns and workshops aimed at educating SMEs on cyber hygiene practices will facilitate promoting the availability of cybersecurity tools within the marketplace.

Furthermore, collaborative efforts with cybersecurity experts will amplify the dissemination of best practices in this field. Such collaborative endeavors are vital for nurturing a resilient cybersecurity ecosystem and ensuring SMEs possess the knowledge and tools required to effectively safeguard their digital assets.

2.2 Vulnerability Discovery to Secure ICT Solutions (VICTORIOUS)

The VICTORIOUS framework is designated to host Bug Bounty Programs and Crowdsource Vulnerability Discovery and Disclosure (CSVDD) initiatives, both strategies aimed at enhancing software security by incentivizing the identification and reporting of vulnerabilities. Their principal goal is to identify and rectify potential security flaws before malicious entities can exploit them. Through NERO's Bug Bounty Programs, security researchers will receive rewards for uncovering and reporting vulnerabilities, assisting companies in promptly and cost-effectively addressing security concerns.

CSVDD guidelines establish a structured framework for responsibly identifying, reporting, and managing security vulnerabilities. These guidelines enable organizations to consistently and effectively receive and respond to security reports from the public. By leveraging bug bounty programs and CSVDD, NERO aims to achieve numerous benefits, including a reduction in the risk of security breaches, heightened security for users and customers, and the proactive identification and resolution of security issues.

NERO is equipped to tackle the challenges associated with these initiatives, such as the risk of false positives or malicious reports and the allocation of resources for reviewing and managing security concerns. This will be accomplished by adhering to a well-defined process for receiving and handling security reports, complete with clear guidelines for reporting, disclosure, and acknowledgement of security researchers. Implementing NERO's Bug Bounty Programs and CSVDD offers an effective approach to strengthening software security, ensuring maximal benefits while mitigating potential risks.

2.3 Audit-Based Certification for Cybersecurity Preparedness (AUDACIOUS)

The AUDACIOUS framework is tasked with auditing resilience mechanisms and conducting application security testing scans, both critical components for safeguarding an organization's digital assets. Within NERO, these activities will be meticulously performed to evaluate and reinforce security controls, identifying any vulnerabilities or shortcomings. Auditing resilience mechanisms aims to validate the efficacy of systems and processes in detecting, responding to, and recovering from potential security threats. Conversely, application security testing scans focus on revealing vulnerabilities inherent in software application code, addressing concerns such as cross-site scripting and SQL injection.

NERO will systematically carry out these assessments, promptly addressing any identified vulnerabilities to mitigate the risk of security breaches. A clearly defined process will govern the reporting and management of vulnerabilities, supported by regular employee training sessions that underscore the importance of application security. This comprehensive approach ensures that NERO remains

proactive in enhancing its security posture, thereby protecting its digital infrastructure against potential threats.

2.4 Cyber Immunity Toolkit Repository (CYBIT)

The CYBIT framework assumes a critical role in testing, detecting, identifying, protecting, responding, and recovering using a wide array of tools provided by NERO's partners. Cybersecurity entails the essential task of safeguarding information systems, networks, and data from unauthorized access, theft, and harm. Within this domain, the processes of identifying, protecting, detecting, responding, recovering, and testing cybersecurity tools serve as fundamental pillars of a robust cybersecurity program.

NERO initiates its cybersecurity defense strategy by meticulously identifying potential vulnerabilities which may arise from factors such as outdated software, weak passwords, or insecure networks. Subsequently, protective measures, such as firewalls and encryption, are implemented to counter unauthorized access attempts. NERO leverages detection tools, including intrusion detection systems, to vigilantly monitor network activity and promptly identify potential threats.

In the unfortunate event of a security breach, NERO adopts a proactive approach, swiftly responding to minimize damage and prevent further losses. Furthermore, comprehensive testing and validation of cybersecurity tools and processes are conducted to ensure their effectiveness. This encompasses rigorous penetration testing, vulnerability scans, and various security assessments to identify and rectify any weaknesses in the cybersecurity posture.

The overarching objective of the CYBIT framework is to enhance resilience against cyber threats and strengthen the protection of critical assets. Through these comprehensive measures, NERO remains steadfast in its commitment to safeguarding its digital infrastructure against evolving cyber threats.

2.5 Innovative Cyberesecurity Awareness Training Mechanisms (ASTRAS)

Last but certainly not least, the ASTRAS framework will serve as the designated platform for housing all essential tools for the training program within the NERO project. These tools will be meticulously categorized into two distinct groups: gamification-based training and cyber ranges. Each method will be strategically employed to offer tailored training experiences, accommodating users' varying levels of expertise and experience.

Cybersecurity gamification-based training and cyber ranges represent cutting-edge methodologies crafted to enhance the capabilities and knowledge of both individuals and organizations in combating cyber threats. Within NERO, gamification-based training utilizes immersive game-like scenarios and simulations to impart foundational knowledge in cyber defense while refining users' decision-making skills in identifying and responding to cyber-attacks.

On the other hand, NERO's cyber ranges provide a dynamic simulated environment tailored for testing and refining defensive strategies against simulated cyber-attacks. This enables organizations to evaluate and strengthen their response mechanisms effectively. Both approaches, whether through gamification or cyber ranges, excel in engaging users and making cybersecurity education interactive and enjoyable.

Through the ASTRAS framework, NERO is poised to elevate skills and awareness levels through gamification-based training and cyber ranges, thereby enhancing organizations' overall resilience against cyber threats. By leveraging these innovative training methodologies, NERO aims to empower individuals and organizations with the necessary skills and knowledge to navigate the intricate landscape of cybersecurity effectively.

2.6 Framework Interconnections

Effective communication between frameworks within the NERO ecosystem is essential for ensuring robust cybersecurity management. The CYBIT framework, responsible for testing and detection, closely collaborates with ASTRAS, which specializes in updating training materials and staying informed about current cybersecurity threats. This mutually beneficial relationship facilitates seamless coordination between proactive testing insights and targeted training initiatives. CYBIT's real-time assessments provide valuable insights into emerging vulnerabilities and potential attack vectors, empowering organizations with a proactive risk management approach. By sharing this crucial information with ASTRAS, organizations can access timely and relevant training resources tailored to effectively address the latest cybersecurity challenges. Furthermore, this collaboration fosters a culture of continuous learning and improvement, encouraging proactive engagement with cybersecurity best practices across the organization. As CYBIT and ASTRAS work together, they not only enhance organizations' resilience against cyber threats but also equip them to navigate the evolving digital landscape with confidence. Through ongoing communication and collaboration, CYBIT and ASTRAS significantly contribute to the adaptability and effectiveness of the NERO ecosystem in safeguarding vital assets and data against cyber threats.

Communication between CYBIT and ARCANA within the NERO ecosystem is crucial to ensure comprehensive cybersecurity management. CYBIT, responsible for testing and detection, generates vital insights into emerging vulnerabilities and potential cyber threats. By conveying these findings to ARCANA, which acts as the central hub for the ecosystem and hosts the marketplace for cybersecurity tools and resources, organizations gain immediate access to actionable information. This enables ARCANA to distribute relevant updates, alerts, and recommendations to users, ensuring they are equipped to effectively address identified vulnerabilities. Furthermore, ARCANA can offer CYBIT valuable user feedback, including their experiences with deployed tools or areas requiring additional support. This feedback loop facilitates continuous improvement and refinement of cybersecurity strategies and toolsets, ultimately enhancing the overall resilience of organizations against cyber threats. Through ongoing communication and collaboration, CYBIT and ARCANA significantly contribute to the effectiveness and adaptability of the NERO ecosystem in safeguarding critical assets and data from potential security breaches.

Effective communication between AUDACIOUS and CYBIT within the NERO ecosystem is vital for ensuring a strong cybersecurity posture. AUDACIOUS, focusing on auditing and resilience mechanisms, conducts thorough assessments to pinpoint vulnerabilities

and weaknesses in an organization's digital infrastructure. By sharing these audit findings with CYBIT, which specializes in testing and detection, organizations can obtain a comprehensive understanding of their cybersecurity landscape. CYBIT then utilizes this information to conduct targeted testing and detection activities, validating and refining the audit insights. Furthermore, CYBIT may offer real-time feedback to AUDACIOUS regarding detected vulnerabilities, enabling AUDACIOUS to promptly prioritize and address critical issues. This collaboration promotes a synergistic approach to cybersecurity, where audit insights inform testing strategies and testing outcomes enhance audit effectiveness. Ultimately, the communication between AUDACIOUS and CYBIT facilitates proactive risk management, empowering organizations to effectively mitigate potential threats and bolster their overall resilience against cyberattacks. Through continuous collaboration and information exchange, AUDACIOUS and CYBIT significantly contribute to the effectiveness and adaptability of the NERO ecosystem in safeguarding against evolving cybersecurity threats.

Effective communication between ASTRAS and ARCANA within the NERO ecosystem is crucial for enhancing cybersecurity training and awareness initiatives. ASTRAS, acting as the repository for training tools and resources, consistently updates its materials to address evolving cybersecurity threats and challenges. By conveying these updates to ARCANA, which serves as the central hub and marketplace for cybersecurity solutions, ASTRAS ensures that organizations have access to the latest training materials and resources. ARCANA, in turn, distributes these resources to users, making them readily available for procurement and use. Additionally, ARCANA may offer feedback to ASTRAS based on user interactions and needs, enabling ASTRAS to customize its training programs to better meet the requirements of organizations within the ecosystem. This collaborative communication fosters a culture of continuous learning and improvement, empowering organizations to stay informed about cybersecurity best practices and enhance their resilience against emerging threats. Through ongoing collaboration, ASTRAS and ARCANA play a pivotal role in strengthening the cybersecurity posture of organizations within the NERO ecosystem, ultimately safeguarding critical assets and data from potential security risks.

Communication between VICTORIOUS and ARCANA within the NERO ecosystem is essential for orchestrating the Bug Bounty Program efficiently. VICTORIOUS, tasked with overseeing the Bug Bounty Program, plays a pivotal role in detecting, evaluating, and addressing cybersecurity vulnerabilities identified by security researchers. By transmitting bug reports, assessments, and remediation actions to ARCANA, which acts as the central hub and marketplace for cybersecurity solutions, VICTORIOUS ensures that organizations within the ecosystem are promptly alerted to potential security threats and vulnerabilities. ARCANA, in turn, disseminates this information to users, offering them insights into emerging vulnerabilities and facilitating the acquisition of necessary tools and resources for remediation. Additionally, ARCANA may furnish feedback to VICTORIOUS based on user experiences and Bug Bounty Program requirements, enabling VICTORIOUS to refine and optimize its bug bounty program continuously. This collaborative communication streamlines vulnerability management efforts enhances the overall resilience of organizations within the NERO ecosystem and helps safeguard critical assets and data from potential security risks. Through ongoing collaboration, VICTORIOUS and ARCANA make significant contributions to the cybersecurity posture of organizations, ensuring proactive protection against emerging threats.

2.7 NERO Tools

Initially, NERO's marketplace will feature 15 tools, each tailored to address a specific function related to the five frameworks comprising NERO's Ecosystem. These tools are developed either by a consortium partner or an external entity, and their utilization will be integral to the initial design of NERO, with their value defined in the project's Use Cases. While these 15 tools form the initial offering, NERO's marketplace remains open for integration with any provided tool, expanding its repository to offer relevant solutions through the platform. The current portfolio of the NERO project includes:

2.7.1 ONE Holistis Security and Privacy Framework (HSPF) . The Hybrid Secure Federated Framework (HSPF) offers a practical solution for developing a robust threat detection model while prioritizing data privacy and security. It employs Federated Learning alongside privacy-preserving techniques such as Multi-Party Computation, Secure Aggregation, Differential Privacy, and Homomorphic Encryption. The Federated Anomaly Detection model, trainable by any node within 5G networks, utilizes network flow analysis and Unsupervised Learning to identify potential threats in received communications. This model promptly flags and blocks threats for immediate or future mitigation. The Federated Implementation involves a Central Server acting as an Aggregator, ensuring the privacy of participants by solely aggregating Training Weights from clients. The Aggregator computes gradients and returns resulting weight values to clients for further training. The process involves categorizing network flows, identifying attacks, and implementing predefined actions through a policy enforcer, with visualization available via a dashboard.

2.7.2 MINDS Honeypot as a Service (M-HaaS). MINDS Honeypot as a Service (M-HaaS) combines Artificial Intelligence (AI) and Software-Defined Networking (SDN) to manage and deploy industrial honeypots for capturing and analyzing malicious network activities. The platform utilizes Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs), offering robust data storage, normalization, and visualization capabilities. M-HaaS comprises two solutions: Game Theory Intelligence (GTI) and NeuralPot. GTI employs mathematical and logical modeling to bolster cybersecurity defenses in industrial networks. By analyzing factors such as the number of connected devices and network capacity, GTI determines the optimal number of honeypots to deploy, maximizing the potential for trapping malicious actors while conserving computing resources. This strategic deployment creates a deceptive landscape, enhancing network security without compromising operational efficiency.

2.7.3 MINDS RADR (M-RADAR). M-RADAR is an anomaly detection system that combines human interaction and visual-based monitoring to detect various security attacks. It utilizes both signature-based methods and AI algorithms, providing visualization graphs

for a clear overview of the network's status. The system employs a wide range of data visualization techniques, including traditional and advanced methods, to aid network administrators in detecting anomalies. Additionally, M-RADAR utilizes supervised and unsupervised machine learning algorithms to generate security events and inform network operators about security attacks. These algorithms are regularly updated with new attack types, ensuring continuous protection for the network.

2.7.4 Montimage Monitoring Tool (MMT). MMT, the Montimage Monitoring Tool, is a comprehensive software suite designed to meet the multifaceted monitoring needs of modern IT environments. It enables organizations to analyze application, system, and network traces both offline and in real-time.

2.7.5 MDS Kioku AI. The Kioku AI tool, part of the NERO platform, enhances scenario-based cybersecurity training for SMEs using advanced machine learning and natural language processing techniques. Its architecture includes interconnected subcomponents like the Scenario Generation Engine, Adaptation and Learning Module, Feedback Loop, Integration Layer, and Analytics and Reporting, all designed to dynamically generate and adapt training scenarios tailored to SMEs' needs and infrastructure.

2.7.6 SNYK. Snyk is a developer-focused security platform that promotes the implementation of security by design principles in software and application security. It provides a holistic toolset for identifying and resolving vulnerabilities in code, open-source dependencies, containers, and infrastructure as code, empowering developers to enhance the security of their applications from the outset.

2.7.7 Trustillio Practical Human Centric Risk Management (HRM) methodology. The Human Risk Management (HRM) methodology integrates the human factors considerations into ISO 27001, enabling SMEs to effectively manage security risks. It proactively addresses human threats, leveraging best practices to strengthen overall security and empower employees as key defenders. HRM evaluates cybersecurity risks by assessing vulnerabilities, impact, and threat frequency, recognizing humans as a potential weak link often overlooked by existing standards. Unlike traditional approaches, HRM emphasizes social mitigation measures alongside technical controls to reduce human vulnerabilities and the occurrence of human threats. By examining the human element, HRM identifies and addresses human threats and vulnerabilities, proposing targeted technical and social controls tailored to employees' needs.

2.7.8 PLUR Seer Box. Seer Box is an advanced solution ensuring web application and service security by reconstructing application logic from user-generated traffic, unlike traditional firewalls relying on known signatures. This innovation fosters collaboration between development, operations, and security teams, simplifying web application security. Powered by Pluribus One's analysis engine, Seer Box not only detects ongoing attacks but also identifies potential future threats by monitoring anomalous behaviors. It provides developers with feedback on vulnerabilities found in the application. Seamlessly integrating with existing IT infrastructure, Seer Box reads data from servers, traffic balancers, and application delivery controllers, continuously updating its knowledge of web services and applications to offer real-time insights into the attack surface.

2.7.9 MONT Attack Detec React (ADR). The Attack Detect React (ADR) Cyber Range is an advanced virtual platform aimed at enhancing cybersecurity readiness and awareness. It offers experiential learning opportunities to individuals and organizations, enabling them to gain hands-on experience in identifying cyber threats, detecting malicious activities, and implementing effective countermeasures. Through simulated attack scenarios and live monitoring, participants acquire valuable insights into the strategies used by cyber adversaries. The primary goals of the ADR Cyber Range include raising awareness, comprehending attack methods, familiarizing with detection techniques, and learning about mitigation strategies.

2.7.10 TRUST-IT, COMMpla Cyber Range Capacity Building in Cybersecurity (CyberWiser). The web portal serves as a central access point for trainers and trainees to access Cross-Learning Facilities, which host dedicated workspaces for specific users or teams. It ensures seamless integration of these facilities and other CYBERWISER.eu components through a Single Sign-On mechanism based on the OpenID Connect module. Users can access the Cross-Learning Facilities via workspaces organized according to their profiles and skills. Each workspace utilizes a Learning Content Management System (LCMS) to deliver customized training courses to users or teams. The LCMS also enables theoretical validation of acquired competencies, providing certifications for completed training courses.

2.7.11 TRUST-IT, COMMpla CyberSecurity Privacy Marketplace. The Marketplace serves as a comprehensive platform offering curated content from completed EU-funded research projects and products/services from providers across Europe. It utilizes the Drupal 7 content management system (CMS) to effectively organize and manage this content. Accessible through web browsers, the Marketplace features a user-friendly frontend interface enabling users to browse, search, and interact with its content and functionalities. Users can securely create accounts and log in, managing their profiles and preferences upon registration. Additionally, users have the option to create their own "Provider minisite" within the Marketplace, allowing providers to showcase their offerings related to cybersecurity and privacy through customizable templates or forms.

2.7.12 MONT Anti-phising Cyber Range. The Anti-Phishing Cyber Range Mobile Application is an innovative educational tool that empowers users to combat phishing attacks effectively. Through experiential learning, users gain hands-on experience in identifying, analyzing, and mitigating phishing threats directly from their mobile devices. The app simulates real-world email scenarios, providing practical insights into cybercriminal tactics. Key features include email simulation, phishing classification, explanations of phishing, and phishing attack classification. Additionally, the app offers access to educational resources, interactive tutorials, and informative content to deepen users' understanding of phishing threats and enhance their digital resilience.

2.7.13 MONT Cartimia Cyber Threat Intelligence (CTI). CARTIMIA CTI (Cyber Threat Intelligence) is a cutting-edge service providing organizations with comprehensive insights into internet network communications. Using advanced analysis techniques and data integration, CARTIMIA CTI offers a complete view of communication routes, detects anomalies, and identifies malicious IPs in real-time. With its web-based interface, organizations can easily access key functionalities such as route mapping analysis, global network view, communication analysis, anomaly detection, and malicious IP detection. CARTIMIA CTI empowers organizations to strengthen their cybersecurity posture and effectively mitigate emerging threats.

2.7.14 Montimage Network Fuzzer. The Montimage Network Fuzzer is an advanced security testing tool aimed at identifying vulnerabilities and evaluating the resilience of networked systems against malicious traffic. Based on the open-source software 5Greplay, it enables organizations to preemptively defend against cyber threats by generating and mutating traffic to simulate potential attack scenarios. With its flexible capabilities and plugin architecture, the Montimage Network Fuzzer provides a comprehensive approach to fuzz testing, accommodating evolving network protocols and security needs. Key features include traffic mutation, various fuzzing techniques, and support for multiple protocols.

2.7.15 Sphynx Incident Response (SPH-IR). The Sphynx Incident Response (IR) platform is a versatile system designed to facilitate the manual or automated execution of Collaborative Automated Course of Action Operations (CACAO) security playbooks. It can function as either a standalone system or as a module integrated with the SPHYNX Security and Privacy Assurance Suite (SPA). In its standalone configuration, the IR platform can import, export, and execute CACAO security playbooks triggered by various third-party tools via their respective REST APIs. When integrated with the SPA Suite, it executes security playbooks triggered by SPA Suite components like EVEREST, utilizing information from the Asset Model and CTI component. Additionally, it orchestrates SPA Suite components. The platform features a user-friendly graphical interface for creating and editing CACAO security playbooks, which can be executed or exported as CACAO JSON files adhering to the CACAO specification. Furthermore, it offers an interactive dashboard providing real-time views of system status, playbook execution, logs, KPIs, user notifications, and other relevant information.

3 NERO USE CASES

This section dives into the three Use Cases (UCs) within the NERO project, each crafted to showcase the indispensable necessity and tangible value of the NERO Ecosystem for SMEs. The primary objective of the project is to highlight its effectiveness across three distinct sectors. UC1 aims to evaluate the application and efficacy of the NERO Ecosystem within the healthcare sector, while UC2 concentrates on the transportation and logistics industry, and UC3 targets the financial sector. These Use Cases serve as pivotal demonstrations of how the NERO framework can address sector-specific cybersecurity challenges and provide tailored solutions to enhance resilience and security posture.

3.1 UC1: Enhancing Patient Data Security in Healthcare through Cybersecurity tools.

Ensuring the augmentation of patient data security through the effective utilization of appropriate cybersecurity tools remains paramount. With the escalating digitization of medical records and the growing reliance on electronic health systems, safeguarding sensitive patient information against cyber threats is imperative to preserve patient privacy, uphold trust in healthcare institutions, and adhere to privacy regulations. Through the implementation of robust cybersecurity measures, healthcare organizations can mitigate the likelihood of data breaches, deter unauthorized access to patient records, and maintain the integrity and confidentiality of medical information. Ultimately, prioritizing patient data security not only safeguards individuals' sensitive data but also cultivates a safer and more resilient healthcare ecosystem for all stakeholders involved.

Considering all the aforementioned points, we contend that the added value of this particular use case transcends mere risk mitigation. It encompasses bolstered patient trust, compliance with privacy regulations, operational efficiency, and ultimately, improved healthcare delivery.

Additionally, within the current landscape of healthcare data management, numerous challenges pertaining to data security persist. Despite technological advancements, vulnerabilities to sophisticated cyber threats and unauthorized access attempts remain prevalent. Weaknesses in security protocols and outdated software leave patient data susceptible to breaches, posing significant risks to confidentiality and integrity. Furthermore, the interconnectivity of systems exacerbates the complexity of cybersecurity defense mechanisms.

To bolster cybersecurity within healthcare Small and Medium Enterprises (HSMEs), the process begins with an assessment of an HSME's objectives, requirements, current capabilities, and existing state. Subsequently, the collected information undergoes careful and thorough evaluation, encompassing compliance with privacy regulations, threat and risk analysis, and gap analysis. This information is then channeled through the ARCANA and CYBIT frameworks, with the deployment of cybersecurity tools provided by the involved partners. These tools, such as network monitoring, code auditing, intrusion detection systems, risk management, and incident response plans, collectively strengthen the system against potential threats. Ultimately, the primary objectives include safeguarding medical and healthcare personal data, enhancing operational efficiency, and fostering trust throughout the healthcare ecosystem.

Figure 2 illustrates the ecosystem of a healthcare system tailored to a specific use case, highlighting the intricate interconnections among the core infrastructure and its associated stakeholders. Within this portrayal, the primary core system, comprised of cloud, network, computer, and storage resources, serves as the foundation for facilitating interactions with key entities such as patients, hospitals, public health agencies, research institutions, pharmaceutical companies, financial institutions, wearable device manufacturers, and network operators. This complex network underscores the specialized integration required to support the targeted healthcare use

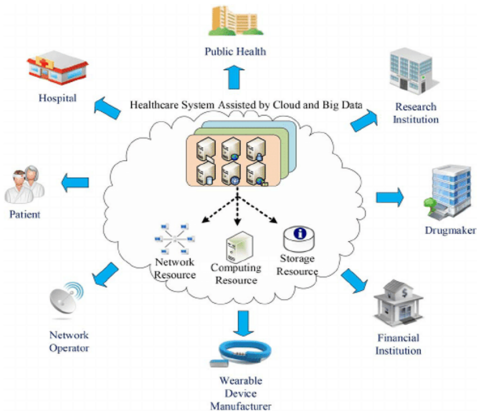

Figure 2: UC1 high-level Architecture.

case, encompassing patient care, data exchange, research collaboration, and financial transactions within its operational framework.

3.2 UC2: Strengthening Supply Chain Resilience through Cybersecurity Awareness in the Transportation and Logistics Industry.

Maritime logistics, serving as a crucial conduit for global trade, encounters distinctive cybersecurity hurdles owing to its diverse and international character. The NERO Framework, tailored to bolster cybersecurity defenses within this domain, presents a comprehensive strategy via its unique elements: VICTORIOUS, AUDACIOUS, CYBIT, ARCANA, and ASTRAS. Each element addresses specific cybersecurity facets, ranging from bug bounty initiatives to training via Gamification tailored to the nuanced requirements of maritime logistics stakeholders.

For example, a shipping firm utilizing the VICTORIOUS module initiates a Bug Bounty Program to uncover vulnerabilities within its IT infrastructure. This proactive step not only strengthens security protocols but also involves the cybersecurity community in a collaborative endeavor to protect vital maritime operations. Simultaneously, port authorities employ the AUDACIOUS module to scrutinize resilience mechanisms and conduct exhaustive application security testing scans, ensuring the resilience of both their digital and physical assets against evolving cyber threats.

Another scenario involves conducting a comprehensive threat analysis using the CYBIT module, concentrating on identifying, safeguarding against, detecting, responding to, and recovering from cybersecurity incidents. This is particularly critical for maritime logistics entities managing sensitive data, including cargo details and shipping schedules, housed in centralized databases and servers. By implementing advanced authentication mechanisms such as Multi-Factor Authentication and Biometric Verification, alongside robust access control measures, the integrity and confidentiality of this data remain intact.

Moreover, the integration of ARCANA and ASTRAS modules facilitates the deployment of cybersecurity tools and enhances personnel's cybersecurity awareness through gamified training environments. These initiatives not only strengthen the cybersecurity framework but also foster a culture of security awareness among individuals interacting daily with logistics systems, ranging from logistics managers to dockworkers.

Figure 3: UC2 high-level Architecture.

Figure 3 depicts the high-level Architecture of UC2, focusing on maritime logistics security, which is categorized into five key areas: Operational Efficiency, Compliance, Threat Analysis, Cybersecurity Measures, and Incident Response Planning.

The first category, Operational Efficiency, aims to bolster cybersecurity within the sector through effective technology integration. Additionally, it emphasizes the development of robust risk management strategies to proactively anticipate and mitigate potential incidents. Moreover, it introduces measures to enhance supply chain visibility.

In the second category, maritime logistics entities evaluate their security compliance with international maritime security regulations and port and shipping regulations. These regulations, established over time, are designed to strengthen security within the sector.

The third category conducts a comprehensive analysis of potential threats to the sector, encompassing both physical and cybersecurity aspects. It delves into detailed examinations of piracy, armed robbery, environmental hazards, and cybersecurity threats.

The fourth category focuses specifically on cybersecurity, employing measures such as network monitoring, data protection, and intrusion detection systems to safeguard against cyber threats.

Lastly, the fifth category is responsible for incident response planning. In the event of a physical threat, an emergency communication system is implemented. On the cybersecurity front, a security breach protocol is established to address potential breaches effectively.

3.3 UC3: Boosting Financial Security through Enhanced Cybersecurity Awareness Tools.

The adoption of the NERO cybersecurity framework within the financial sector emerges as a proactive measure against the evolving landscape of cyber threats. With the persistent increase in sophisticated attacks targeting financial institutions, NERO presents a comprehensive solution to mitigate risks and bolster defenses. By protecting sensitive financial data from unauthorized access and manipulation, NERO plays a crucial role in upholding the confidentiality, integrity, and availability of vital information. Additionally, its capabilities extend beyond mere protection to include proactive detection and prevention mechanisms aimed at preventing potential cyber threats before they escalate. As financial institutions strive to uphold their commitment to clients' security and

trust, the integration of NERO becomes a strategic necessity. It not only helps mitigate financial losses and reputational harm resulting from cyber incidents but also enhances resilience against emerging threats. Furthermore, by ensuring the stability and integrity of financial systems and transactions, NERO contributes to the overall resilience and credibility of the broader financial ecosystem. In essence, NERO stands as a cornerstone in defending against cyber threats in the financial sector, offering unmatched protection, risk mitigation, and trust reinforcement.

Among the dynamic environment of the financial sector, the implementation of the NERO cybersecurity framework emerges as a strategic necessity, embracing a multifaceted approach to strengthen defenses and protect critical assets. At the forefront of this defense strategy lies the Intrusion Detection System (IDS), a sophisticated tool finely tuned to monitor incoming network traffic in real-time. Through continuous analysis, the IDS meticulously examines patterns, behaviors, and signatures indicative of potential threats or intrusions. Leveraging the insights provided by NERO's training materials and programs, the cybersecurity team is poised to respond promptly to any alerts triggered by the IDS, taking a proactive stance to mitigate potential damage and prevent unauthorized access.

Moreover, recognizing that the human factor represents both a vulnerability and a defense line, NERO places significant emphasis on employee training and awareness. Through immersive training modules, interactive simulations, and real-world scenarios, employees are equipped with the knowledge and skills needed to identify, report, and mitigate cybersecurity threats effectively. By nurturing a culture of cybersecurity awareness and responsibility, financial institutions ensure that their staff remains vigilant guardians of sensitive data, contributing to the overall resilience and security posture of the organization.

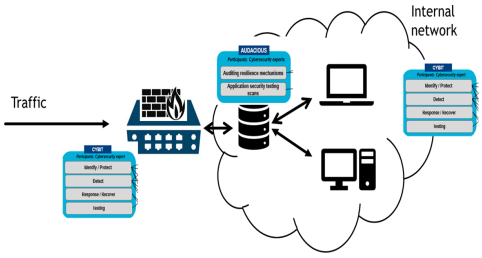

Figure 4: UC3 high-level Architecture.

Within the framework of an internal network tailored for a financial institution, several crucial components collaborate to maintain a robust cybersecurity infrastructure, as depicted in Figure 4. Leading the defense is a meticulously configured firewall, diligently scrutinizing incoming and outgoing traffic to establish a barrier against unauthorized access and potential threats attempting to breach the network's perimeter. NERO's CYBIT framework will complement the network's firewall, monitoring and safeguarding the network from unauthorized access.

Internally, the network incorporates servers hosting essential financial applications and services. These servers serve as the foundation of the company's infrastructure, hosting critical software utilized for the company's operations, as well as the source code of the company's product provided to other financial institutions. The software will undergo examination, and the source code will be scanned for vulnerabilities using the AUDACIOUS framework.

Furthermore, the workstations provided to employees, equipped with robust endpoint security software, act as the frontline interface, enabling secure access to network resources and executing daily tasks with steadfast reliability. These workstations, alongside the servers and all network equipment, constitute the internal network. Continuous monitoring by the CYBIT framework of the NERO project will ensure protection against any threats to the internal network.

4 CONCLCUSION

In Conclusion, the NERO ecosystem offers a proactive and comprehensive approach to cybersecurity, tailored to the needs of organizations, especially SMEs. Through integrated frameworks, advanced technologies, and alignment with international standards, NERO equips users with the tools and knowledge needed to combat emerging threats effectively. By fostering collaboration and innovation, NERO aims to strengthen cybersecurity defenses and safeguard critical assets in today's evolving digital landscape.

ACKNOWLEDGMENTS

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 of the European Commission or the partners in the above mentioned project. The authors declare that there are no conflicts of interest, including any financial or personal relationships, that could be perceived as potential conflicts.

REFERENCES

[1] CYNET. 2023. *Covid19 Cyberattack Analysis.* Retrieved April 23, 2024 from https://go.cynet.com/covid-19-cyberattack-analysis?utm_source=thn
[2] ENISA. 2021. *SME Cybersecurity.* Retrieved April 23, 2024 from https://www.enisa.europa.eu/topics/cybersecurity-education/sme_cybersecurity
[3] ENISA. 2022. *ENISA Threat Landscape 2022.* Retrieved April 23, 2024 from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
[4] ENISA. 2022. *Foreign Information Manipulation Interference (FIMI) and Cybersecurity - Threat Landscape.* Retrieved April 23, 2024 from https://enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape
[5] ENISA. 2022. *Volatile Geopolitics Shake the Trends of the 2022 Cybersecurity Threat Landscape.* Retrieved April 23, 2024 from https://www.enisa.europa.eu/news/volatile-geopolitics-shake-the-trends-of-the-2022-cybersecurity-threat-landscape
[6] Deloitte University Press. 2017. *Industry 4.0 and cybersecurity.* Retrieved April 23, 2024 from https://www2.deloitte.com/content/dam/insights/us/articles/3749_Industry4-0_cybersecurity/DUP_Industry4-0_cybersecurity.pdf
[7] Nisha Rawindaran, Ambikesh Jayal, and Edmond Prakash. 2022. Exploration of the Impact of Cybersecurity Awareness on Small and Medium Enterprises (SMEs) in Wales Using Intelligent Software to Combat Cybercrime. *Computers* 11, 12 (2022). https://doi.org/10.3390/computers11120174
[8] European Union. 2021. *SMEs and cybercrime.* Retrieved April 23, 2024 from https://op.europa.eu/en/publication-detail/-/publication/00fcf078-d19d-11ec-a95f-01aa75ed71a1

Received 30 April 2024; revised xx May 2024; accepted xx May 2024