

Project No. 101127411

Project start: 2023-12-01

Call: DIGITAL-ECCC-2022-CYBER-03

Project duration: 36 months



D2.1 - Cybersecurity Landscape and Threat Analysis, End-User Requirement Analysis, and Use Case Definition – Initial version

Document Identification	
Due date	2024-05-31
Submission date	2024-05-31
Version	1.0

Related WP	WP2	Dissemination Level	PU
Lead Participant	MINDS	Lead Authors	Ioannis Makris (MINDS), Pavlos Bouzinis (MINDS), Dimitrios Asimopoulos (MINDS)
Contributing Participants	MINDS, EBOS, TRUSTILIO, MONT, TRUST-IT, INFO, MDS, SPHYNX, ONE, COMMpla, UPRC, ILINK, SCS, AIN	Related Deliverables	D2.2

Abstract: This document provides an initial Cybersecurity Landscape and Threat Analysis, End-User Requirement Analysis, and Use Case Definition. It provides a concise examination of cybersecurity challenges affecting SMEs, detailing prevalent threats, impacts, and threats and analysing the literature review on the basis of NIST Cybersecurity Framework (CSF) 2.0. Additionally, the document encompasses an End-User Requirement Analysis conducted through the NERO questionnaire, the results of which are utilised to create an initial set of requirements tailored to the end-users' needs in combination with the insights from the literature review. Furthermore, D2.1 showcases the NERO Ecosystem through a high-level architecture, the functionality of each partner's tool that will be used within the NERO Ecosystem, and the demonstration of the tools in different use cases. These initial technical specifications intend to serve as a common reference and driver for the development and implementation in all other technical tasks of the project, including WP3, WP4, WP5 and WP6.



Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Digital Europe Program (DEP). Neither the European Union nor the Digital Europe Program (DEP) can be held responsible for them.

This document is issued within the NERO project. This project has received funding from the European Union's DIGITAL-2021-SKILLS-01 Programme under grant agreement no. 101127411. This document and its content are the property of the NERO Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license to the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the NERO Consortium and are not to be disclosed externally without prior written consent from the NERO Partners. Each NERO Partner may use this document in conformity with the NERO Consortium Grant Agreement provisions and the Consortium Agreement.

The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Executive Summary

The research work in NERO is structured in seven work packages working in parallel towards the development of the NERO Ecosystem fulfilling the needs of the end-users. To pave the way for understanding and clarifying the technical design and development, the present initial version of the Cybersecurity Landscape and threat Analysis was produced. This document's purpose is to be a reference to the project's tool providers and end-users, establishing a high-level of the NERO ecosystem.

This deliverable presents an initial version of the Cybersecurity Landscape and Threat Analysis, End-User Requirement Analysis, and Use Case Definition including the use case scenarios, together with some end-user requirements conducted through the cybersecurity analysis which will be monitored during the project. More specific, this deliverable begins with an introduction to the cybersecurity landscape for SMEs, detailing common threats and impacts. It outlines a threat assessment framework aligned with the NIST Cybersecurity Framework 2.0. The analysis includes end-user requirements derived from the NERO Questionnaire and interviews. It then describes the NERO ecosystem and tools, highlighting their functionalities and the NERO framework communication. Finally, the document provides an initial definition of the NERO use cases with the assets identification, scenarios and tools that will be validated into each use case.

The initial high-level specification will be further detailed in technical work packages developing the different components of the NERO solution. At M15, the final specification (D2.2) will reflect the actual final implementation of the integrated NERO Ecosystem, updating the present document and adding technology choices details.

Document Information

Contributors

Beneficiary	Short Name
MetaMind Innovations	MINDS
Trustilio BV	Trustilio
Ebos Technologies Limited	EBOS
Massive Dynamics Sweden AB	MDS
Montimage EURL	MONT
TRUST-IT SRL	TRUST-IT
Infotrend Innovations Company Limited	INFO
Sphynx Hellas Anonymi Etaireia	SPH
One Source Consultoria Informatica LDA	ONE
Commpla SRL	COMMpla
University Of Piraeus Research Center	UPRC
Ilink Nees Texnologies OE	ILINK
Pole Solutions Communicantes Securisees	SCS
Ainigma Technologies	AIN

Reviewers

Name	Beneficiary
Charalambos Klitis	EBOS

Alex Bensenousi	AIN
Cristina Mancarella	TRUST-IT

History

Version	Date	Contributor(s)	Comment(s)
0.1	2024-02-29	Ioannis Makris (MINDS), Pavlos Bouzinis (MINDS), Dimitrios Asimopoulos. (MINDS), Vasileios Gavresis (MINDS), Nikolaos Moschos (MINDS), Stefania Altini (MINDS)	D2.1 ToC
0.2	2024-03-27	All Participating Partners	Sections 2, 3, 4, 5
0.3	2024-04-25	All Participating Partners	Sections 1, 2, 3, 4, 5, 6
0.4	2024-04-30	Ioannis Makris (MINDS), Pavlos Bouzinis (MINDS), Dimitrios Asimopoulos. (MINDS)	Final Integration and Modifications of D2.1
0.5	2024-05-01	Ioannis Makris (MINDS), Pavlos Bouzinis (MINDS), Dimitrios Asimopoulos. (MINDS)	AIN, EBOS, and TRUST-IT received v1.0 on 01-05-2024 for review
-	2024-05-16	Charalambos Klitis (EBOS), Alex Bensenousi (AIN), Cristina Mancarella (TRUST-IT)	Deadline for reviewers to send their comments.
1.0	2024-05-24	Ioannis Makris (MINDS), Pavlos Bouzinis (MINDS), Dimitrios Asimopoulos. (MINDS)	MINDS sent the revised D2.1 for review by the coordinator and submission.

Schedule

Deliverable Action	Deadline
Partners inputs 1 st round (50% ready)	27/3/2024
QARM review / approval	31/3/2024
Partners inputs 2 nd round (100% ready)	25/4/2024
Deliverable Leader review	30/4/2024
QARM review / approval	1/5/2024
Send for 2-week review to Peer Reviewers	1/5/2024
Feedback from reviewers	15/5/2024
Deliverable Leader addresses reviewers feedback	24/5/2024
Deliverable Leader provides the final version to the PC	24/5/2024
PC reviews / approves	30/5/2024
PC submits deliverable to EC	31/5/2024

Table of Contents

1	Introduction	1
1.1	Objective of the document	1
1.2	Structure of the document.....	1
1.3	Relationship with other deliverables	1
1.4	Contributors	2
2	Cybersecurity Landscape and Threat Analysis	4
2.1	Cybersecurity Status of SMEs	4
2.1.1	Common Attacks and Threats on SMEs	4
2.1.2	Impact of Cyber attacks on SMEs.....	6
2.1.3	Cybersecurity Challenges for SMEs.....	7
2.2	Literature Review and Research Directions.....	8
2.2.1	Methodological Framework.....	8
2.2.2	Literature Analysis and NIST CSF 2.0 Mapping	10
2.3	Insights and Recommendations.....	17
3	End-user Requirements Analysis	21
3.1	Methodology for requirements collection and analysis	21
3.2	NERO Questionnaire Analysis.....	22
3.2.1	NERO Questionnaire General Information	22
3.2.2	NERO Questionnaire Results.....	22
3.2.3	Questionnaire Responses Analysis Summary	61
3.3	NERO Stakeholders.....	62
3.4	End-user Interviews Methodological Framework	63
3.5	Initial List of Requirements	64
4	NERO Ecosystem	67
4.1	High-Level Architecture Description	67
4.1.1	Market Oriented Cybersecurity Awareness Training (ARCANA)	67
4.1.2	Vulnerability Discovery TO Secure ICT Solutions (VICTORIOUS).....	68
4.1.3	Audit-Based Certification For Cybersecurity Preparedness (AUDACIOUS)	68
4.1.4	Cyber Immunity Toolkit Repository (CYBIT).....	68
4.1.5	Innovative Cybersecurity Awareness Training Mechanisms (ASTRAS).....	69
4.1.6	Tools and Frameworks Communications Methodology	69
4.1.7	NERO's external communication	72
4.2	Partner's Tools	73
4.2.1	ONE Holistic Security and Privacy Framework (HSPF)	73
4.2.2	MINDS Honeypot as a Service (M-HaaS).....	74
4.2.3	MINDS RADAR (M-RADAR).....	76
4.2.4	Montimage Monitoring Tool (MMT).....	78
4.2.5	MDS Digital Education platform for cybersecurity training (KIOKU AI).....	80
4.2.6	SNYK	84
4.2.7	TRUSTILIO Practical Human Centric Risk Management (HRM) methodology	87
4.2.8	PLUR Seer Box	93

4.2.9	Montimage Attack Detect React (ADR).....	97
4.2.10	TRUST-IT, COMMpla Cyber Range & Capacity Building in Cybersecurity (CyberWiser).....	98
4.2.11	TRUST-IT, COMMpla CyberSecurity & Privacy Marketplace.....	100
4.2.12	Montimage Anti-phishing Cyber Range	101
4.2.13	Montimage Cartimia Cyber Threat Intelligence (CTI)	102
4.2.14	Montimage Network Fuzzer	104
4.2.15	Sphynx Incident Response (SPH-IR)	105
4.2.16	Sphynx Security and Privacy Assurance (SPH-SPA).....	108
4.3	Tools Relation to NERO Ecosystem	111
5	Use Cases Definitions	113
5.1	UC1: Enhancing Patient Data Security in Healthcare through Cybersecurity tools.	113
5.1.1	UC1 Description.....	113
5.1.2	System Architecture and Assets Identification	113
5.1.3	Scenarios Definition	116
5.1.4	NERO frameworks and tools to be validated	119
5.2	UC2: Strengthening Supply Chain Resilience through Cybersecurity Awareness in the Transportation and Logistics Industry.....	120
5.2.1	UC2 Description.....	120
5.2.2	System Architecture and Assets Identification	122
5.2.3	Scenarios Definition	125
5.2.4	NERO Frameworks and tools to be Validated	128
5.3	UC3: Boosting Financial Security through Enhanced Cybersecurity Awareness Tools.....	129
5.3.1	UC3 Description.....	129
5.3.2	System Architecture and Assets Identification	130
5.3.3	Scenarios Definition	131
5.3.4	NERO Frameworks and tools to be Validated	134
6	Conclusion and Future Work.....	135
	References.....	136

List of Figures

Figure 1: Frequency of cybersecurity incidents [1].	5
Figure 2: Illustration of the adopted methodology.	8
Figure 3: NIST CSF 2.0 Core Structure [13].	10
Figure 4: Statistics of Mapping between NIST CSF 2.0 and literature review.	18
Figure 5: Response to Q1.	23
Figure 6: Responses to Q2.	23
Figure 7: Responses to Q3.	24
Figure 8: Responses to Q4.	24
Figure 9: Responses to Q5.	25
Figure 10: Responses to Q6.	25
Figure 11: Responses to Q7.	26
Figure 12: Responses if “Out-of-scope” is selected for Q7.	26
Figure 13: Responses to Q8.	27
Figure 14: Responses if “Out-of-scope” is selected for Q8.	27
Figure 15: Responses to Q9.	28
Figure 16: Responses if “Out-of-scope” is selected for Q9.	28
Figure 17 : Responses to Q10.	29
Figure 18: Responses if “Out-of-scope” is selected for Q10.	29
Figure 19: Responses to Q11.	30
Figure 20: Responses if “Out-of-scope” is selected for Q11.	30
Figure 21: Responses to Q12.	31
Figure 22: Responses if “Out-of-scope” is selected for Q12.	31
Figure 23: Responses to Q13.	32
Figure 24: Responses if “Out-of-scope” is selected for Q13.	32
Figure 25: Responses to Q14.	33
Figure 26: Responses if “Out-of-scope” is selected for Q14.	33
Figure 27: Responses to Q15.	34
Figure 28: Responses if “Out-of-scope” is selected for Q15.	34
Figure 29: Responses to Q16.	35
Figure 30: Responses if “Out-of-scope” is selected to Q16.	35
Figure 31: Responses to Q17.	35
Figure 32: Responses if “Out-of-scope” is selected for Q17.	36
Figure 33: Responses to Q18.	36
Figure 34: Responses if “Out-of-scope” is selected for Q18.	37

Figure 35: Responses to Q19.	37
Figure 36: Responses to Q20.	38
Figure 37: Responses if “Out-of-scope” is selected for Q20.	38
Figure 38: Responses to Q21.	39
Figure 39: Responses if “Out-of-scope” is selected for Q21.	39
Figure 40: Responses to Q22.	40
Figure 41: Responses if “Out-of-scope” is selected for Q22.	40
Figure 42: Responses to Q23.	41
Figure 43: Responses if “Out-of-scope” is selected for Q23.	41
Figure 44: Responses to Q24.	42
Figure 45: Responses if “Out-of-scope” selected for Q24.....	42
Figure 46: Responses to Q25.	42
Figure 47: Responses if “Out-of-scope” is selected for Q25.	43
Figure 48: Responses to Q26.	43
Figure 49: Responses if “Out-of-scope” is selected for Q26.	44
Figure 50: Responses to Q27.	44
Figure 51: Responses if “Out-of-scope” is selected for Q27.	45
Figure 52: Responses to Q28.	45
Figure 53: Responses if “Out-of-scope” is selected for Q28.	45
Figure 54: Responses for Q29.....	46
Figure 55: Responses if “Out-of-scope” is selected for Q29.	46
Figure 56: Percentage of Responders who answered Technical Questions.	47
Figure 57: Responses to Q30.	47
Figure 58: Responses to Q31.	48
Figure 59: Responses if “Out-of-scope” is selected for Q31.	48
Figure 60: Responses for Q32.....	49
Figure 61: Responses if “Out-of-scope” is selected for Q32.	49
Figure 62: Responses to Q33.	50
Figure 63: Responses if “Out-of-scope” is selected for Q33.	50
Figure 64: Responses to Q34.	51
Figure 65: Responses to Q35.	51
Figure 66: Responses if “Out-of-scope” is selected for Q35.	52
Figure 67: Responses to Q36.	52
Figure 68: Responses if “Out-of-scope” is selected for Q36.	52
Figure 69: Responses to Q37.	53
Figure 70: Responses if “Out-of-scope” is selected for Q37.	53

Figure 71: Responses to Q38.	54
Figure 72: Responses if “Out-of-scope” is selected for Q38.	54
Figure 73: Responses to Q39.	55
Figure 74: Responses if “Out-of-scope” is selected for Q39.	55
Figure 75: Responses to Q40.	56
Figure 76: Responses if “Out-of-scope” is selected for Q40.	56
Figure 77: Responses to Q41.	57
Figure 78: Responses if “Out-of-scope” is selected for Q41.	57
Figure 79: Responses to Q42.	58
Figure 80: Responses if “Out-of-scope” is selected for Q42.	58
Figure 81: Responses to Q43.	59
Figure 82: Responses if “Out-of-scope” is selected for Q43.	59
Figure 83: Responses to Q44.	60
Figure 84: Responses if “Out-of-scope” is selected for Q44.	60
Figure 85: Responses to Q45.	61
Figure 86: Responses if “Out-of-scope” is selected for Q45.	61
Figure 87: NERO high-level ecosystem	67
Figure 88: HSPF Architecture.....	74
Figure 89: Game Theory Intelligence (GTI) Architecture.....	75
Figure 90: M-HaaS - NeuralPot Architecture.....	76
Figure 91: M-RADAR Architecture.	77
Figure 92: MMT Architecture.....	79
Figure 93: KIOKU AI architecture.	83
Figure 94: Application Security architecture.	84
Figure 95: Visual of how Snyk's Toolkit Fits into Application Security.....	85
Figure 96: ENISA RM Toolbox and RM process.....	89
Figure 97: Determining a risk's severity [54].....	90
Figure 98: HRM architecture.	93
Figure 99: Seer Box architecture.....	95
Figure 100: Example of Installation architecture_01.....	95
Figure 101: Example of Installation architecture_02.....	96
Figure 102: ADR architecture.....	97
Figure 103: CYBERWISER.eu training platform architecture.....	99
Figure 104: Cyberwatching Marketplace architecture.	100
Figure 105: Anti-phishing cyber range screens.	102
Figure 106: CARTIMIA CTI service Web site.....	103

Figure 107: Montimage Network Fuzzer architecture.....	105
Figure 108: Sphynx Incident Response (IR) platform architecture.	106
Figure 109: CACAO Playbooks.....	107
Figure 110: Sphynx IR key features.....	108
Figure 111: Security & Privacy Assurance platform (SPA) Architecture.	109
Figure 112: UC1 Healthcare Interactions.	114
Figure 113: UC1 system architecture diagram 1.....	115
Figure 114: UC1 System Architecture Diagram 2.....	115
Figure 115: UC2 Maritime logistics interaction.	122
Figure 116: UC2 Maritime logistics interactions with authentication mechanism.....	122
Figure 117: UC2 system architecture.....	123
Figure 118: UC3 system architecture.....	130

List of Tables

Table 1: Mapping of the reviewed literature to NIST CSF 2.0.....	15
Table 2 : List of requirements.....	65
Table 3: Background assets used within HSPF.....	74
Table 4: List of background assets used within M-HaaS.....	76
Table 5: List of background assets used in M-RADAR.	78
Table 6: List of background assets used in MMT.....	80
Table 7: List of background assets used within KIOKU AI.	83
Table 8: List of background assets used within SNYK.	86
Table 9: HRM-multi dimensional profile of users with secure behaviour.	90
Table 10: List of background assets used within HRM.	93
Table 11: List of background assets used within Seer Box.	96
Table 12: List of background assets used in ADR.....	98
Table 13: List of background assets used within CyberWiser.eu.	99
Table 14: List of background assets used in Cyberwatching Marketplace.....	101
Table 15: List of background used in Anti-phising cyber range.....	102
Table 16: List of background assets used in CARTIMIA CTI.	104
Table 17: List of background assets used in Montimage Network Fuzzer.	105
Table 18: List of background assets used in SPH IR.	108
Table 19: List of background assets used in SPH SPA.....	111
Table 20: Tools Relation to NERO Ecosystem.....	111
Table 21: UC1 assets description.....	115
Table 22: UC1 - Scenario 1 (SC1.1).....	116
Table 23: UC1 - Scenario 2 (SC1.2).....	117
Table 24: UC1 - Scenario 1 (SC1.3).....	118
Table 25: UC1 Frameworks and Tools to be validated.....	120
Table 26: UC2 Asset Description.	124
Table 27: UC2 - Scenario 1 (SC2.1).....	125
Table 28: UC2 - Scenario 2 (SC2.2).....	127
Table 29: UC2 Frameworks and Tools to be validated.....	128
Table 30: UC3 Asset Description.	131
Table 31: UC3 - Scenario 1 (SC3.1).....	131
Table 32: UC3 - Scenario 2 (SC3.2).....	132
Table 33: UC3 - Scenario 3 (SC3.3).....	133
Table 34: UC#3 Frameworks and Tools to be validated.....	134

Introduction

List of Acronyms

AEDNN	Autoencoder-based Deep Neural Network
API	Application Programming Interface
AI	Artificial Intelligence
BGP	Border Gateway Protocol
BPM	Business Process Modeling
BCP	Business Continuity Process
CACAO	Collaborative Automated Course of Action Operations
CD	Continuous Deployment
CIA	Confidentiality Integrity Availability
CI	Continuous Integration
CLI	Command-Line Interface
CMS	Content Management System
CPE	Common Platform Enumeration
CSVDD	Crowdsourcing Vulnerability Discovery and Disclosure
CTI	Cyber Threat Intelligence
DDoS	Distributed Denial of Service
DNN	Deep Neural Network
ECSF	European Cybersecurity Skills Framework
EES	Enhanced Encryption Standard
EVEREST	Event REaSoning Toolkit
FR	Functional Requirement
GAN	Generative Adversarial Network
GTI	Game Theory Intelligence

Introduction

HSME	Healthcare Small and Medium Enterprise
IAST	Interactive Application Security Testing
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IT	Information Technology
KNN	K-Nearest Neighbor
KPI	Key Performance Indicator
LCMS	Learning Content Management System
LMS	Learning Management Systems
ML	Machine Learning
MLC	Maritime Logistics Company
MISP	Malware Information Sharing Platform
NFR	Non-Functional Requirement
NLP	Natural Language Processing
NVD	National Vulnerability Database
OSINT	Open Source Intelligence
PC	Personal Computer
PLC	Programmable Logic Controllers
SPA	Privacy Assurance Suite
RTU	Remote Terminal Unit
RM	Risk Management
SIEM	Security Information and Event Management System
SME	Small and Medium-Sized Enterprise

Introduction

SQL	Structured Query Language
SSO	Single Sign On
TRL	Technology Readiness Levels
UI	User Interface
VM	Virtual Machines
WAF	Web Application Firewall

1 Introduction

1.1 Objective of the document

This document is deliverable D2.1 named “*Cybersecurity Landscape and Threat Analysis, end-user Requirement Analysis and Use Case Definition – Initial version*” of the NERO project.

This document aims to provide a thorough overview and analysis of the current cybersecurity challenges faced by small and medium-sized enterprises (SMEs). The document reflects the outcome of the initial analysis made in the context of WP2. It commences with a critical analysis of cyber threats specific to SMEs, paving the way for strategic defence mechanisms. Building on the insights collected through the analysis, the document focuses on the identification of end-user requirements by taking into consideration a detailed analysis of questionnaire responses from end-users and key stakeholders in different SMEs. Also, the document provides high-level design of the NERO architecture, describing the individual tools contributed by each partner and mapping in this way the initial configuration of the NERO ecosystem.

Finally, this document aims to identify and clearly outline what the NERO Ecosystem should deliver and meet the needs of SMEs by analysing target user roles and determining their specific requirements, as well as determining the functionalities and features that the NERO Ecosystem must provide. The result of this will be an initial definition of the NERO Ecosystem's use cases and end-user requirements that will serve as a foundation for the development and implementation of the system.

1.2 Structure of the document

This document is structured as follows. After the introductory section, Section 2 describes the cybersecurity landscape as it relates to SMEs, detailing common threats and the impact of cyber attacks. It outlines a methodological framework employed for threat assessment and correlates these findings with insights from the latest literature, particularly with the standards of the NIST Cybersecurity Framework 2.0. Then, Section 3 builds on this foundation by presenting an analysis of end-user requirements through various aspects, including the first version of the NERO Questionnaire, the corresponding results, and the methodological frameworks of the interviews that will be conducted to identify the end-user requirements. In Section 4, a high-level description and presentation of the NERO ecosystem is provided, followed by the presentation of NERO tools that will be used in the project, encapsulating their functionalities and roles within the ecosystem. Finally, use case definitions in Section 5 embody the practical application of the NERO framework, illustrating how it enhances cybersecurity in critical domains such as healthcare, transportation, and finance. The document concludes with Section 6, summarising the findings and outlining the trajectory for future developments and refinements within the NERO project.

1.3 Relationship with other deliverables

The D2.1 relates to the following deliverables:

- D2.2 - Cybersecurity landscape and threat analysis, end-user requirement analysis and use case definition – Final version: This document will include the description of the integration and deployment of the initial version of the NERO framework.

Introduction

- D3.1 - Market-based technology and readiness assessment of cybersecurity tools, and Marketplace – Initial version: This document will provide initial results from the market-based technology and readiness assessment of cybersecurity tools and development of an initial version of a marketplace for the tools described in D2.1.
- D3.2 - Market-based technology and readiness assessment of cybersecurity tools, and Marketplace – Final version: This document will provide final results from the market-based technology and readiness assessment of cybersecurity tools and development of a final version of a marketplace for the tools described in D2.1.
- D4.1 – Framework for cybersecurity testing and auditing: This document provides a description of the framework for cybersecurity testing and auditing, including a standardised methodology for assessing the security of systems based on the end-user requirements from D2.1.
- D5.1 – NERO training planning: This document will provide a report on the comprehensive NERO cybersecurity training plan based on the results of the D2.1 questionnaire.
- D5.2 – NERO training results and evaluation – Initial version: This document will include an initial report of the results and evaluation of the NERO cybersecurity training program implemented based on the results of the questionnaire and the requirements marked in D2.1.
- D5.3 – NERO training results and evaluation – Final version: This document will include a final report of the results and evaluation of the NERO cybersecurity training program implemented based on the results of the questionnaire and the requirements marked in D2.1.
- D6.1 - Integration and use case planning: D6.1 will find the baseline of the NERO Framework specification in D2.1 including the use case scenarios and KPIs to be used during the validation and demonstration phase.

1.4 Contributors

D2.1 is the result of the collaboration of the Project Coordinator, Technical Manager, WP2 Leaders, Tool providers and Use Case leaders. The contents of the deliverable are the result of multiple discussions not only among the technical WP leaders but also among all individual participants in the technical tasks, including components research and development, integration and use case piloting.

The following partners have contributed to this deliverable:

- MINDS
- EBOS
- TRUSTILIO
- MONT
- TRUST-IT
- INFO
- MDS
- SPHYNX
- ONE

Introduction

- COMMpla
- ILINK
- SCS
- UPRC
- AIN

2 Cybersecurity Landscape and Threat Analysis

The objective of this section is to shed light on the current cybersecurity landscape of SMEs, including the threats they are facing, the direct impacts of those threats and the challenges to comply with cybersecurity best practices and policies. Moreover, a literature review was conducted that aimed to categorising ongoing research directions regarding cybersecurity in SMEs, based on their compliance with cybersecurity frameworks, and specifically the NIST CSF 2.0. The aim of this literature review and gap analysis is to identify the current challenges and gaps, highlight potentially neglected research areas and define the future common strategies and best practices to fill-in the gaps efficiently.

2.1 Cybersecurity Status of SMEs

SMEs form the foundation of the EU's economy, constituting 99% of all businesses and employing approximately 100 million individuals [1]. These enterprises contribute to over half of Europe's GDP and play a significant role in adding value across a plethora of sectors within EU's economy. Furthermore, they facilitate digital transformation and constitute a key element of the EU's social fabric.

Since the outbreak of the COVID-19 pandemic, many companies adopted a remote working approach, which gave rise to the extensive use of online platforms, such as e-commerce, e-banking, e-government services, and e-learning for educational purposes. This rapid transition to e-services has persisted even in the post-COVID era, highlighting the expanding digitalisation of processes and its increasing significance across various sectors. Along with the rise of digitalisation, malicious actors exploited the underlying gaps, as evidenced from the surge in malicious emails, fishing, scams and malware. Moreover, an increase in the number of cyber attacks was witnessed, affecting not only large industries, but also targeting SMEs. The latter, since the transitioning to remote working, prioritised the timely deployment of systems to meet customer demands, while overlooking the security aspects and cyber-shielding of their solutions. As a matter of fact, SMEs are still prone to cyber threats. Below, the common security threats that SMEs are facing, along with the consequent impacts of cyber attacks, are discussed.

2.1.1 Common Attacks and Threats on SMEs

Despite the common belief that cyber attacks exclusively target large enterprises, organisations of all sizes can become victims. As a matter of fact, SMEs are facing growing susceptibility to cyber attacks. According to [2], 61% of SMEs were exposed to malware attacks in 2017. Also, 67% of SMEs experienced a cyber attack and 58% a data breach in 2018. Industry, academia and organisation's research suggest that the most common attacks on SMEs include phishing and social engineering, web-based attacks, malware, denial of service, hacking, and others. Moreover, in accordance with the 2021 ENISA report [1], Figure 1 summarises the common threats and the corresponding frequency of occurrence across SMEs.

Cybersecurity Landscape and Threat Analysis

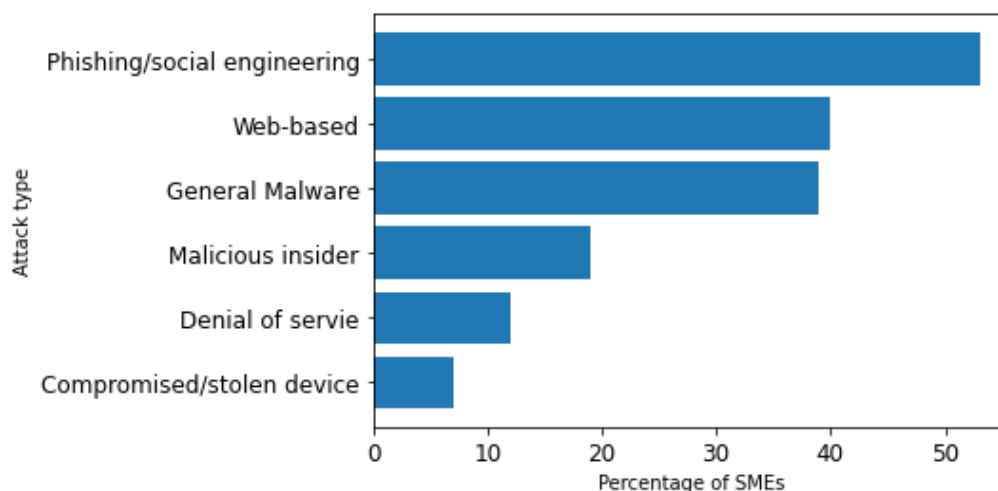


Figure 1: Frequency of cybersecurity incidents [1].

Besides the attacks presented in the above figure, a description of common attacks on SMEs is provided below:

- **Phishing/social engineering:** Phishing and social engineering attacks are types of cyber attacks that try to manipulate individuals into revealing sensitive information, such as passwords and data, and ultimately gaining access to this information. These attacks usually rely on human psychology rather than technical schemes. Therefore, human factor is a prerequisite to render these attacks successful, while at a subsequent stage, security incidents based on technical skills may be triggered.
- **Web-based:** Web-based attacks refer to malicious activities or exploits, targeting potential vulnerabilities in websites, web-applications, and web-servers. The considered attacks can be observed in several forms, e.g., stealing data, compromising systems, and disrupting services. Examples of such attacks are Structured Query Language (SQL) injection, cross-site scripting and various zero-day attacks.
- **Malware:** Malware or malicious code, is a term used to describe any software or firmware that is designed to execute unauthorised actions, resulting in detrimental effects on the confidentiality, integrity, or availability of a system.
- **Malicious insider:** A person who has authorised access to the organisation's data, systems, or networks, owing to their position within the company. Unlike to external threats, malicious insiders have privileged access, and thus, may exploit this opportunity to cause damage or benefit from such actions. These attacks may include data theft, disrupting operations, espionage, fraud, etc.
- **Denial of Service:** A malicious action which aims to interrupt the normal operation of a targeted system, network, or server, usually by overwhelming it with multiple illegitimate requests or traffic. The goal of this attack is to render the targeted system out of service, and thus, inaccessible to legitimate and intended users.
- **Compromised/stolen device:** This attack refers to a situation where a device, usually a laptop or tablets, are accessed, manipulated, or stolen by unauthorised individuals. This can happen through malware infections, hacking, or physical theft.

- **Ransomware:** The attacker gains unauthorised access to a computer system or network and encrypts the victim's data or files. In exchange for restoring access to those files or data via decryption, the attacker demands a ransom from the victim.
- **Supply chain attacks:** A supply chain attack includes at least two interconnected attacks. Firstly, the supplier is targeted, which serves as a gateway to launch a subsequent attack on the ultimate target to obtain access to its resources. This target may be either the end customer or another entity within the supply chain. Consequently, for an attack to be classified as a supply chain attack, it should target both the supplier and the customer.

As demonstrated in Figure 1, phishing/social engineering, web-based, and malware are the most common attacks experienced by SMEs. Although this result stemmed from the sixteen participants of the ENISA report, it aligns with the Ponemon Institute survey conducted in 2019 [3], which highlights the same threats as being the most frequently encountered, with minor deviations compared to the ENISA report. Furthermore, it is worth mentioning that social engineering is the predominant threat in general, with 84% of cyber attacks relying on this tactic, as indicated by ENISA [4] in 2020. In addition, the ANSSI report [5] indicated that 40% of the ransomware attacks that took place between 2021 and 2022 targeted SMEs, highlighting once again the frequent phenomenon of attacking SMEs. Also, according to [3], cyber attacks are becoming more targeted, sophisticated, and severe in terms of detrimental consequences, since the year 2017. This was evident from the increase of the costs for recovering from business disruptions, caused by the identified attacks. Finally, the most targeted assets within SMEs seem to be web application servers, mail servers, mobile devices, and laptops, followed by IoT devices and cloud systems [6], [3].

2.1.2 Impact of Cyber attacks on SMEs

Cyber attacks have the potential to cause severe harm to any enterprise, with SMEs being particularly vulnerable to this impact. In the aftermath of a cyber attack, SMEs that lack preparedness may face significant financial losses, loss of reputation and customer trust, as well as data breaches.

Concerning the financial losses, as per IBM findings [7], enterprises with fewer than 500 employees face an average data breach cost of 2.98 million dollars, with an average cost of 164 dollars per breached record. Also, the healthcare and finance industries presented the highest cost. Although the financial impact on SMEs will fluctuate depending on the specific incident, it is unlikely that there won't be any financial impact. According to the 2023 ENISA report [8], approximately one-fifth of security incidents result in financial losses. These cyber attack costs may include addressing immediate damages, covering ransom costs, employing customer service staff to manage inquiries, and hiring Information Technology (IT) security specialists and physical security experts. Besides direct expenses, cyber attacks may also incur costs associated with unforeseen downtime and reduced productivity. Furthermore, [7] indicated that 60% of businesses raise prices after cyber attacks, which is a direct consequence of covering expenses.

Apart from financial costs, cyber attacks may harm SMEs' reputations. Future customers may hesitate to support a targeted SME, while potential investors may avoid or postpone any investing actions, by perceiving that being a cyber attack victim is a sign of naivety. A survey conducted in 2021 by Cisco, [9], showed that 57% of the targeted SMEs declared a loss of trust with customers, and 66% reported a negative impact on their reputation.

Finally, it is a common phenomenon that cyber attacks lead to data breaches, a situation that particularly harms the targeted SME. A survey conducted in 2021 by Cisco [9], showcased that 75% of SMEs that experienced a cybersecurity incident, claimed that it resulted in loss of customer data. In addition to this, over 60% of SMEs indicated cases of breach of internal emails, employee data, intellectual property, and financial and sensitive business information. It is also highlighted that the average cost of data breaches reached a record high in 2022. This is also related to the fact that 83% of the organisations in the study [7], experienced more than one data breach. Particularly, the healthcare sector suffers the most from breach cost, exhibiting a 41.6% cost increase from 2020 to 2022 [7].

2.1.3 Cybersecurity Challenges for SMEs

SMEs may face several challenges regarding their cybersecurity preparedness. The key factors behind these challenges stem from awareness and proper management. Below, the primary challenges encountered by SMEs in the context of cybersecurity are highlighted:

- **Limited Cybersecurity Awareness:** Due to the technical nature of the cybersecurity field, individuals without a technical background often assume that cybersecurity exclusively concerns IT experts. However, this is not always the case. As already mentioned, a large proportion of cyber attacks rely on phishing and social engineering. Taking this into consideration, each person should have a minimal knowledge of fundamental awareness regarding cybersecurity. For instance, employees should understand phishing and social engineering attacks, as well as basic rules for using their devices to access the company's network.
- **Lack of Resources:** Cybersecurity preparedness relies on investments towards initiating training programs, requiring services from third-party experts, or hiring specialised staff that will engage in cybersecurity tasks. Moreover, dedicated cybersecurity solutions and platforms, such as security information and event management systems (SIEM), also incur costs. According to Ponemon report [3], 55% of the participating SMEs cited insufficient budget as a main challenge that keeps the IT posture from being fully effective.
- **Lack of Guidelines:** Another challenge that SMEs face, is the lack of guidelines in terms of standards and well-defined practices. According to [1], although there are several EU bodies that provide cybersecurity guidelines [1], [10], [11], SMEs are not always aware of this information or consider some of it outdated, while these reports highlight theoretical and not practical aspects of cybersecurity solutions. Furthermore, SMEs stated that some of the available guidelines target mainly large enterprises and are not suitable for SMEs.
- **Lack of Cybersecurity Expertise:** Many cybersecurity solutions require the involvement of IT experts to leverage them effectively. However, it is common in SMEs that IT staff have multiple roles [1], [12]. Apart from cybersecurity-related tasks, IT personnel may undertake tasks such as managing server and cloud infrastructure, implementing communication and collaboration tools, being responsible for web presence, etc.

Besides the for the aforementioned challenges, additional burdens may include underestimating the risks, the outdated skillset of already existing IT staff, the constant change in the cybersecurity landscape, shadow IT devices, and limited management support [1], [3], [12].

2.2 Literature Review and Research Directions

2.2.1 Methodological Framework

The objective of the conducted literature review is to map the focus of the research into cybersecurity best practices and guidelines for SMEs. The methodology followed to collect and assess information included desktop research. The collected literature consisted mainly of peer-reviewed publications, including journal papers, conferences, and white papers/reports. Specific keywords were used throughout the literature search, such as “cybersecurity of SMEs”, “cyberthreats of SMEs”, while the search was conducted across the following widely used platforms:

- Google Scholar
- Scopus
- IEEE Xplore
- Elsevier Science Direct
- SpringerLink

The majority of the selected works published from 2021 and onwards, with the aim of offering the most up-to-date information possible, enabling the construction of a cybersecurity landscape that accurately reflects the present state.

As mentioned previously, the goal of this section is to investigate the current cybersecurity landscape of SMEs, including the identification of potential threats, means of detection and protection against those threats, as well as mitigation plans. In this direction, existing cybersecurity frameworks can facilitate this process, since they define optimal practices that organizations, including SMEs, can adopt for managing cybersecurity risks, establishing unified language for common understanding and standardising the delivery of services. To this end, the taxonomy of the reviewed literature was aligned with the NIST CSF 2.0 [13]. The purpose of this approach is to investigate based on the research perspective of the corresponding sources in the literature how SMEs address cybersecurity challenges and adhere to the established best practices, particularly those outlined in NIST CSF 2.0. This methodology aims to gather information on the current practices adopted by SMEs, evaluate the maturity of their strategies regarding cybersecurity threats, and identify any potential gaps the SMEs may overlook. It is noted that the literature sources reviewed do not explicitly reference the NIST CSF 2.0 and do not necessarily align their methods under its guidance. Nonetheless, after thorough examination, the underlying connections to NIST CSF 2.0 were identified and reported in all of the works. Figure 2 provides an illustrative summary of the adopted methodology.

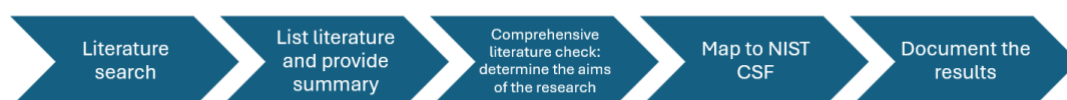


Figure 2: Illustration of the adopted methodology.

2.2.1.1 NIST Cybersecurity Framework

The NIST CSF 2.0 offers direction for industries, governmental bodies, and other organisations in handling cybersecurity threats. It offers a taxonomy of high-level security goals that are applicable to a variety of organisations, regardless of their size, type, and resources, to better comprehend, evaluate,

prioritise, and communicate its cybersecurity efforts. More specifically, it helps organisations describe their current and target cybersecurity posture, identify shortcomings, and assess the progress toward overcoming those gaps. Furthermore, it facilitates the identification and prioritisation of actions for mitigating cybersecurity threats, in accordance with the organisation's mission and risk management. Finally, it offers a standardised means of communication both internally and externally within the organisation about cybersecurity risks, capabilities, requirements, and outcomes.

The core components of the NIST CSF 2.0 are a hierarchy of **Functions**, **Categories**, and **Subcategories**, describing a set of cybersecurity outcomes. The first tier of this hierarchy, the **Functions**, are the foundational cybersecurity outcomes that the **Categories** and **Subcategories** rely on. Figure 3 provides the above-mentioned core structure of NIST CSF 2.0, including the NIST Functions and their respective Categories. In the continue, the definition of the NIST CSF 2.0 functions are presented [13]:

- **Govern (GV):** *The organisation's cybersecurity risk management strategy, expectations, and policy, are established, communicated, and monitored.* The Govern Function provides outcomes to guide an organisation in determining actions to accomplish and prioritise the outcomes of the other five Functions of the framework, in terms of its goal and stakeholder expectations. The Govern function consists of the following categories 1) Organisational Context (GV.OC), 2) Risk Management Strategy (GV.RM), 3) Cybersecurity Supply Chain Risk Management (GV.SC), 4) Roles Responsibilities and Authorities (GV.RR), 5) Policies, Processes, and Procedures (GV.PO), and 6) Oversight (GV.OV).
- **Identify (ID):** *The organisation's current cybersecurity risks are understood.* The action of identifying the organisation's assets, e.g., data, software hardware, systems, personnel, etc., suppliers and underlying cybersecurity threats, enables the alignment of its efforts with its risk management strategy and the mission requirements outlined by Govern Function. Furthermore, this Function includes the identification of opportunities for enhancing the organisation's policies, plans, processes, practices that facilitate cybersecurity risk management. The categories within the Function are 1) Asset Management (ID.AM), 2) Risk Assessment (ID.RA), and 3) Improvement (ID.IM).
- **Protect (PR):** *Safeguards to manage the organisation's cybersecurity risks are used.* With the identification and prioritisation of assets and risks, Protect Function aims at securing those assets to prevent or mitigate the likelihood and impact of adversarial cybersecurity attacks. Outcomes that accompany this Function include identity management, access control, and authentication. The categories of the Function are 1) Identity Management, Authentication, and Access Control (PR.AA), 2) Awareness and Training (PR.AT), 3) Data Security (PR.DS), 4) Platform Security (PR.PS), and 5) Technology Infrastructure Resilience (PR.IR).
- **Detect (DE):** *Possible cybersecurity attacks and compromises are found and analysed.* Detect Function enables the detection and analysis of intrusions, anomalies, and any potential cybersecurity attack in a timely manner. The Function also supports incident response and recovery activities. The categories are 1) Continuous Monitoring (DE.CM), and 2) Adverse Event Analysis (DE.AE).
- **Respond (RS):** *Actions regarding a detected cybersecurity incident are taken.* Respond Function enables the mitigation of the impact of cybersecurity incidents. The outcomes within this function include incident management, analysis, mitigation, reporting, and communication. The categories within respond are given namely as 1) Incident Management (RS.ID), 2) Incident

Cybersecurity Landscape and Threat Analysis

Analysis (RS.AN), 3) Incident Response, Reporting and Communication (RS.CO), and 4) Incident Mitigation (RS.MI).

- **Recover (RC):** *Assets and operations affected by a cybersecurity incident are restored.* Recover is responsible for the restoration of normal operations to minimise the impact of cybersecurity incidents and promote effective communication during the restoration procedure. The categories of this Function are 1) Incident Recovery Plan Execution (RC.RP) and 2) Incident Recovery Communication (RC.CO).

The methodology used throughout this section includes the categorisation of the reviewed literature according to the NIST Functions and Categories. This task involves the mapping of each paper/source to one or more specific Functions and Categories, according to the topics, research questions and goals, and aspects presented in the respective work.

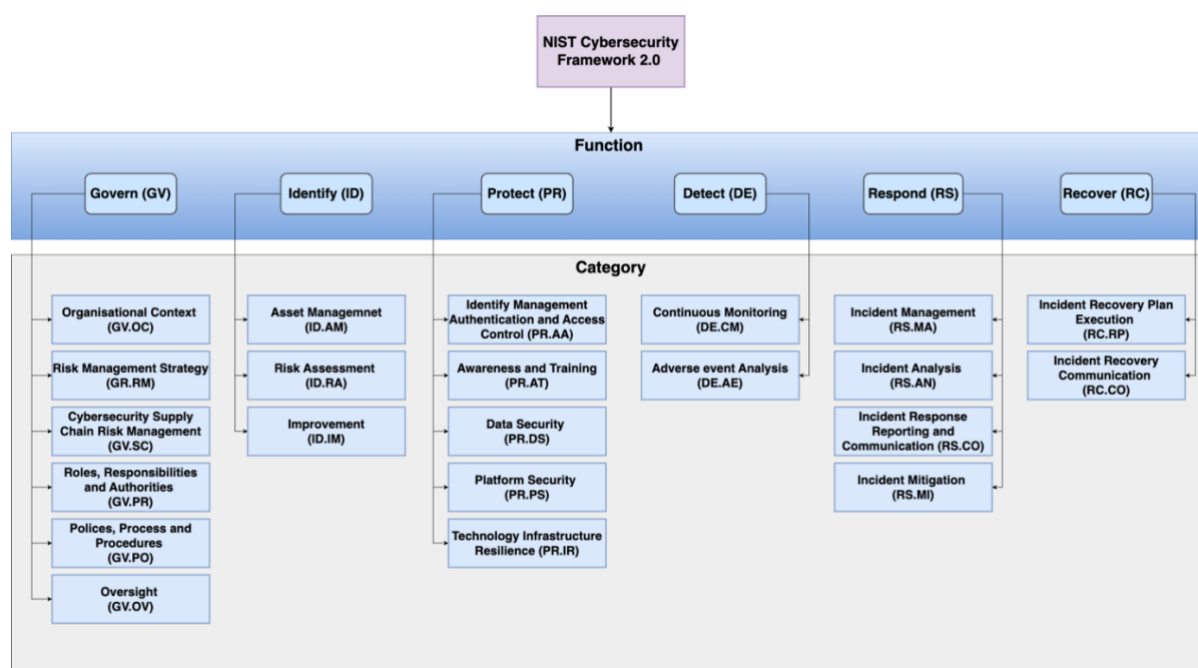


Figure 3: NIST CSF 2.0 Core Structure [13].

2.2.2 Literature Analysis and NIST CSF 2.0 Mapping

In this subsection the literature analysis regarding research on SME cybersecurity is presented. For each source, the objectives, research directions and findings are discussed, along with the corresponding mapping to the NIST CSF 2.0.

Firstly, [14] discusses the increasing threat of cyber attacks for SMEs in Switzerland. It emphasises that around one-third of these SMEs have experienced cyber attacks where phishing is being a common entry point due to employee errors. The research incorporates conducting interviews with employees of Swiss SMEs with the goal of comprehending their perspectives on cyber attacks and offering practical recommendations for enhancement. Raising awareness, empowering employees, implementing recovery mode training are the research's main recommendations. Due to these recommendations the approach in this study is mapped to the Protect NIST function.

In [15], the report describes findings from a comprehensive study, focusing on understanding the nature and extent of three categories of insider incidents, namely malicious, negligent, and well-meaning, as

well as their correlation with the employment of cybersecurity measures. The study involved 496 SMEs who participated by completing a questionnaire. Results indicate that although insider incidents are infrequent, a small subset of the SMEs reported a higher-than-average occurrence, which often leads to detrimental consequences. Also, it lies in the NIST function Identify, as it aimed to record the frequency of different types of insider incidents on Dutch SMEs, as well as the impact of such incidents and their consequences. This outcome falls into the category of risk assessment, as threat likelihood and impacts are used to understand the inherent risk. Finally, participating SMEs were asked to determine their implemented measures for preventing and mitigating cyber security incidents, mainly related to insider threats, capturing the function Protect.

Moreover, [16] introduces a novel and refined taxonomy of security threats in FinTech and conducts a comprehensive systematic review of defensive strategies. This comprehensive examination provides useful insights for stakeholders, including banks, enterprises and global governmental entities. It also highlights the existing challenges within FinTech and proposes efficient strategies to address them. The primary goal of the survey is to identify the most recent cyber threats, aligning with the function Identify. The aforementioned function is also used through the SME's asset identification, as described in the paper. Finally, the study focuses on defining the way that SMEs detect and employ defence mechanisms to these threats, capturing the functions Detect and Protect.

[17] focuses on how SMEs in the Nordic Baltic Region should face cybercrime. Interviews primarily focusing on the IT security measures employed by SMEs are conducted to assess their cybersecurity status. These measures include, among others, systematic software updates, access control for networks and strong passwords for authentication. Additionally, according to SMEs in the survey, it was concluded that the advice and recommendations provided by public and international organisations are mainly aimed at larger companies. Moreover, the awareness raising on cybersecurity for SMEs by organisations in the Baltic sea region has been limited so far. Finally, the survey indicated the vulnerability of SMEs to cyber attacks, emphasizing the necessity to enhance cybersecurity measures. As a final remark, authors highlighted that the current cybersecurity status of SMEs, which is in a relative low level, hinders the digitalisation process. The study aimed at collecting the SMEs security measures, capturing the Protect function, as well as discovering the threats, which falls into Identify function.

The research in [18] aims to identify entrepreneurs' primary concerns regarding cybersecurity and highlight the main factors contributing to cybersecurity risks in micro, small, and medium-sized enterprises (SMEs). The researchers conducted a survey with an online questionnaire to find out why cybersecurity risks exist in small and medium-sized businesses. Findings include the imperative to enhance defence mechanisms against cyber attacks for SMEs. The study asked participants regarding their roles and responsibilities in cybersecurity, as well as information about risk factors. Therefore, the study used Govern and Identify functions.

Furthermore, in [19], a methodology utilizing use journey is adopted to analyse human behaviour and visually represent the procedures and vulnerabilities within SMEs. Also, an illustration of sociotechnical actor network is generated, focusing particularly on the risks identified in the user journey. The proposed framework consisted of identifying assets and threats, evaluate the impact of asset failure, communicating potential cybersecurity incidents and mitigating them. Thus, the study targeted the Identify, Protect and Respond NIST functions.

Also, [20] implemented a program to assist SMEs in Belgium in enhancing their defences against cybersecurity threats. More specifically, various methodologies are examined, and findings are

presented from the authors' involvement in a cybersecurity awareness initiative directed at the SMEs. Based on this analysis, insights and recommendations are offered. Since the study focused mainly on cybersecurity awareness, it falls under the Protect function and under the respective category.

The study in [21] examines different devices presently available in the market for detecting intrusions. It investigates how these devices implement prevention strategies for SMEs in both home and office environments. The analysis focuses on evaluating their reliability in addressing zero-day attacks relative to the associated costs. A cost model was employed to assess SMEs' decision-making outcomes when establishing an appropriate framework for securing their data. In conclusion, achieving a satisfactory trade-off between IT expertise and the cost-effectiveness of products is critical for SMEs aiming to protect their data. The adoption of a more intelligent controlled environment, integrating machine learning (ML) techniques, can enhance data protection without compromising on cost. The paper falls under Detect and Protect NIST functions, since the research includes intrusion detection systems (IDS) and protection of hardware and software. Govern function is also invoked, since the study includes prioritisation of cost related with risks.

In what follows, [22] focuses on the challenges faced by SMEs in implementing effective information security and cybersecurity measures. It specifically addresses the context of SMEs in Portugal. The study highlights the limited resources and funding available to SMEs, which often leads to a lower level of cybersecurity awareness among employees. To address these challenges, the paper proposes a methodology based on the ISO-27001:2013 standard. This methodology includes the use of controls, actions, and countermeasures to improve information security management in SMEs. The controls are categorised into 14 thematic categories, such as information security policies, organisation of information security, human resource security, and access control. The methodology was implemented in fifty SMEs as a case study. The study analysed the results of the implementation and found that the methodology had a positive impact on the information security management and cyber awareness of the audited SMEs. The study also identified the controls that were most easily achieved by SMEs and those that posed more technical challenges.

In [23], the main focus of the paper lies in answering the following questions: 1) What factors lead to cyberthreats for SMEs, 2) What is the current equipment and know-how regarding cybersecurity in SMEs, and 3) What assistance from third parties (external) do SMEs need in order to better protect themselves against cyberthreats. To this end, questionnaires were circulated to SMEs in Germany. The results demonstrated deficiency in cybersecurity awareness in SMEs, even though most SMEs use IT security measures such as firewalls, backups or two factor authentication. Moreover, it is evident that the majority of SMEs have limited time to dedicate to understanding existing information regarding on cybersecurity and the available material often uses quite technical language. Finally, a significant portion of SMEs lack of an emergency plan for responding to security incidents. Therefore, the paper addresses Protect and Respond function, as it also includes incident response plan targeted questions.

[24] mainly focuses on ways of upgrading the knowledge base and practices of cybersecurity in Finnish podiatry SMEs. The research recognises that phishing attempts are common cyber threats that can adversely affect SMEs including putting them into bankruptcy due to their limited financial resources as well as internal control. Moreover, this research emphasizes that data protection is extremely vital within the health and welfare sector with a focus on business continuity and patient safety. In this regard, the authors have developed a list of low-cost cyber hygiene activities for SMEs through an inclusive review. Such measures are designed to greatly improve an organization's security status by making employees more aware and ensuring they adhere to straightforward security precautions. As such, these

Cybersecurity Landscape and Threat Analysis

conclusions offer important insights for healthcare and welfare professionals seeking to guard against cyber threats while building overall resilience within their organisations. The paper falls into the NIST functions Identify, Protect, and Detect, as its research questions addressed threat identification, data backup, and detection of potential malicious attacks.

Moreover, [25] introduces a cybersecurity solution tailored for SMEs, focusing on automated processing and prioritisation of cyber threats through shared Cyber Threat Intelligence (CTI). By leveraging advanced data analytics and ML techniques, it transforms shared CTI into actionable insights. A prototype application was developed, demonstrating the practical application of these concepts by automatically processing MISP (Malware Information Sharing Platform) data, prioritising threats, and providing SMEs with actionable, context-specific recommendations. This approach aims to enhance cybersecurity resilience in SMEs, addressing their unique challenges and resource constraints. As the paper refers to detecting intrusions, prioritising the threats, and sharing threat information with third parties, it is related with Detect, Respond and Recover functions.

[26] explores a specialised cybersecurity solution for SMEs in Malaysia, employing an Autoencoder-based Deep Neural Network (AEDNN) to detect cyber threats efficiently. By utilising the NSL-KDD dataset for training, the study advances a novel IDS that capitalizes on Artificial Intelligence (AI) to monitor network traffic in real-time, aiming to pinpoint potential cyber intrusions. The core of this methodology lies in the integration of autoencoders with a deep neural network (DNN), a strategy designed to enhance the precision of threat detection by focusing on the most significant network traffic features. The experimental outcomes underscore the system's high efficacy, with detection accuracies ranging between 96% and 99%. This indicates a significant step forward in deploying AI-driven security mechanisms within the cybersecurity domain, especially for SMEs lacking extensive IT resources. Taking the aforementioned into consideration, the paper captures the Detect NIST function.

In addition, [27] outlines a strategic framework for SMEs to strengthen their cyber defences, focusing on the detection, mitigation and elimination of malware threats. Using tools such as Cuckoo Sandbox and Wazuh, the study demonstrates effective malware detection and mitigation strategies, with an emphasis on rapid incident resolution to prevent significant damage. It details the setup of an integrated security stack, presenting a proactive approach to cybersecurity through ML, user behaviour analysis, and integration of an identity and access management solution. Since the proposed framework is equipped with IDS and security incident response policy, including mitigation and communication, it covers the functions Detect and Respond.

[28] presents a survey conducted with responses from 141 SMEs located in UK. The objective was to collect insights to improve comprehension regarding their cybersecurity awareness levels and potential threat mitigation actions. The findings showcased that while SMEs implement some basic cybersecurity protocols, a deficiency in cybersecurity awareness exists along with the lack of tools for enhancing cybersecurity practices. According to the previous discussion, and also based on the questionnaire that was used, the study examines the Identify, Prevent and Govern NIST functions.

In [29], the paper proposes an AI-powered cyber security strategy that makes use of the K-Nearest Neighbour (KNN) algorithm and the Enhanced Encryption Standard (EES) cypher and decryption algorithm, for applications in the financial sector management. The considered method is used to detect and stop malware attacks, and thus, capturing the Detect function.

The study in [30] conducted research in SMEs in Saudi Arabia, aiming at measuring the cybersecurity practices adopted by the respective participants. The paper applied regression models to evaluate

Cybersecurity Landscape and Threat Analysis

cybersecurity practices in the context of financial damage, loss of sensitive data, and incident restoration time interval. The study captured a wide range of the NIST functions since it focused on cybersecurity awareness and training, protection systems, cybersecurity governance and policies, roles and responsibilities regarding cybersecurity issues, management of resources, and restoration and recovery plan.

[31] presented a tool for visualising cybersecurity related use cases. The goal of the tool is to improve cybersecurity awareness, by pointing out potential gaps and facilitating best cybersecurity practices. The tool targets employees with various technical background and expertise. It was evaluated by 29 participants and proved to be of satisfactory usability. Therefore, the considered tool captures the Protect function, as it is meant for training and awareness.

The research paper [32], aimed at capturing SMEs employees awareness of cybersecurity risks, via testing their knowledge in cybersecurity best practices. The study included 164 participants and the questions referred to current security measures, awareness, asset identification, tools for vulnerability discovery and cybersecurity roles in the company. Taking this into account, the survey used Govern, Identify, Protect and Detect functions.

In [33] the authors conducted interviews and workshops across three healthcare organisations in Italy, Greece and Ireland. The main findings included critical requirements for future cybersecurity interventions. In this direction, a toolkit was developed to facilitate the identification of problematic behaviours in healthcare organisations. The tool encompasses the evaluation of effectiveness and reassessing security position and priorities and identifying risks and insecure behaviour. That it falls into the functions Identify, Protect and Govern.

In a large healthcare system, [34] launched a phishing simulation for raising awareness and identifying risks. Although, the simulations were conducted on an Italian hospital with over 6000 staff, the proposed simulation environment could also target SMEs, since phishing attacks are not restricted to large organisations. Finally, the study covers Identify and Protect functions.

[35] aimed at evaluating the cybersecurity readiness level in Italian SMEs. Initially, a survey was used for quantitative assessment, and subsequently interviews were conducted to further explore the critical points indicated in the initial study. Results showcased that SMEs have not accomplished high levels of organisational readiness. As such, the study focused on the Identify, Govern and Protect functions, since the interviews addressed vulnerability discovery, threat identification, communication of cybersecurity policies and training.

An interesting cybersecurity framework, which is the outcome of a EU Horizon 2020 programme, is the SEMSEC [36], [37]. The considered framework is tailored to SMEs and provides awareness and training tutorials, vulnerability discovery and resolution tools, threat protection and response tools, and thus, capturing the Govern, Identify, Protect, Detect and Response functions.

Additionally, in [38], an overview of cybersecurity in the field of process control, process operation, and supply chain was presented. Emphasis was given to the detection of attacks through ML techniques and model predictive control to detect and handle cyber attacks. Furthermore, a novel control architecture with native robustness to prevent attacks is proposed, as well as recovery strategies to enable operation in a stable state upon the detection of attacks. As such, the paper captures the Detect and Prevent, Respond functions.

Cybersecurity Landscape and Threat Analysis

[39] identified and evaluated the use of AI with potential high impact on cybersecurity and focusing specifically in SMEs. Several AI-based methods were outlined that are capable of improving cybersecurity in SMEs. The aspects that the paper addressed included malware and intrusion detection, endpoint protection and response, and security information and event management systems. Therefore, the paper is aligned with the Detect, Protect, and Response functions.

[40] conducted a study to estimate how efficiently SMEs are handling cybercrime. The questionnaire was answered by 122 SMEs in Wales and mainly included questions regarding awareness and knowledge of using intelligent software. Also, particular attention was given to the integration of ML in the current cybersecurity technologies of the SMEs, along with the levels of knowledge of this action. Thus, the study addressed the Protect function through the evaluation of awareness levels.

[41] focused on the assessment of cyber risks in SMEs. The paper employed a sample of 124 SMEs in UK and took advantage of a multi-criteria decision analysis method. Afterwards, a mixed strategy was proposed for facilitating risk assessment, which considered the metrics of step-wise assessment ratio and best-worst method. Hence, the paper addressed the Identify function through risk assessment methods.

Also, [42] proposed a novel framework aimed at strategically mitigating malware risks by incorporating best practices and leveraging the National Institute of Standards and Technology (NIST) cybersecurity standards. This framework is structured around five key phases: Preparation and Deployment, Malware Monitoring and Detection, Notification Action, Mitigation and Remediation Actions, and Data Analysis and Report. It emphasises a comprehensive approach to improving SMEs' cybersecurity postures by enhancing malware detection, monitoring, and eradication capabilities. The research concludes that SMEs require a robust countermeasure strategy to protect against and efficiently manage malware attacks, offering a detailed blueprint for achieving enhanced cyber resilience. Thus, it captures the NIST functions Identify, Detect, Recover, Respond

[43] proposed a platform for optimising detection and recovery of attacks in a SME environment. To this end, they proposed the fusion of ML and blockchain with proactive security techniques, with the ultimate goal of providing security in each phase of an attack. Emphasis was given also to attack prevention and helping SMEs' system to recover in a normal state of operation. Based on these the paper captures Detect, Prevent and Respond functions.

Finally, [44] conducted a survey on 50 SME IT leaders to rate their companies' cybersecurity preparedness level. The questionnaire used for the survey contained 35 questions that aimed to capture all functions in the NIST CSF. As a matter of fact, the considered survey is fully aligned with the NIST CSF, making a usage of all functions.

Given the summary of each source as discussed above, Table 1 summarizes the correlation between the reviewed literature and the functions and categories within the NIST CSF 2.0.

Table 1: Mapping of the reviewed literature to NIST CSF 2.0.

Paper	Year	Govern	Identify	Protect	Detect	Respond	Recover
[14]	2021			PR.AT			
[15]	2023	GV.PO	ID.RA	PR.AA			

Cybersecurity Landscape and Threat Analysis

[16]	2024		ID.AM ID.RA	PR.AA PR.AT	DE.CM		
[17]	2023		ID.RA	PR.AA PR.AT			
[18]	2020	GV.RR	ID.RA				
[19]	2021		ID.AM ID.RA	PR.AA PR.PS		RS.CO RS.MI	
[20]	2019			PR.AT			
[21]	2021	GV.RM		PR.PS	DE.CM DE.AE		
[22]	2021	GV.OC GV.PO	ID.AM	PR.AA		RS.MA	
[23]	2023			PR.AA PR.AT PR.DS		RS.MA	
[24]	2023		ID.RA	PR.DS	DE.CM		
[25]	2021				DE.CM	RS.MA	RC.CO
[26]	2021				DE.CM		
[27]	2023				DE.CM DE.AE	RS.MA RS.AN RS.CO RS.MI	
[28]	2023	GV.RR	ID.RA	PR.AA PR.AT			
[29]	2023				DE.CM		
[30]	2021	GV.RR GV.PO		PR.AA PR.AT			RC.RP

Cybersecurity Landscape and Threat Analysis

		GV.RM					
[31]	2023			PR.AT			
[32]	2021	GV.RR	ID.AM	PR.AA PR.AT	DE.CM		
[33]	2021	GV.RR GV.PO	ID.RA	PR.AT			
[34]	2023		ID.RA	PR.AT			
[35]	2022	GV.PO	ID.RA	PR.AT			
[36]	2020	GV.PO	ID.RA ID.AM	PR.AA PR.AT	DE.CM	RS.MA	
[38]	2023			PR.AA	DE.CM DE.AE		RC.RP
[44]	2020	GV	ID	PR	DE	RS	RC
[39]	2022			PR.AA	DE.CM DE.AE	RS.MA	
[40]	2022			PR.AT			
[41]	2023		ID.RA				
[43]	2020			PR.AA	DE.CM DE.AE		RC.RP RC.CO
[42]	2021		ID.RA		DE.CM DE.AE	RS.MA RS.AN RS.CO RS.MI	RC.CO

2.3 Insights and Recommendations

The current subsection presents insights stemmed from the literature review and its mapping to NIST CSF 2.0, as well as recommendations proposed by governmental bodies and cybersecurity frameworks to facilitate optimal cybersecurity practices and policies within SMEs.

Firstly, the histogram in Figure 4 presents the percentage of the literature that addressed the respective NIST CSF 2.0 functions through its research objectives.

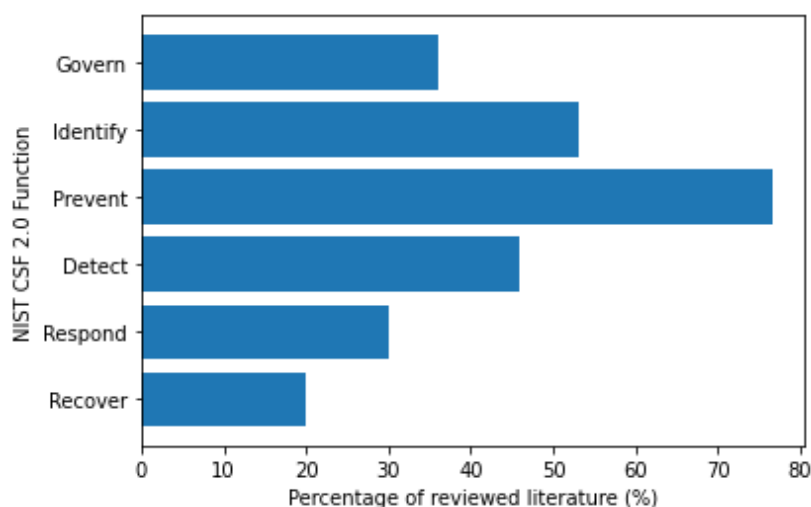


Figure 4: Statistics of Mapping between NIST CSF 2.0 and literature review.

As can be observed in Figure 4, the most common NIST function that research papers address is **Prevent**, withholding 76.6% of the reviewed literature. The **Identify** function follows with 53% and **Detect** with 46%. Finally, **Govern**, **Respond**, and **Recover** are covered in 36%, 30%, and 20% of the literature, respectively.

According to the aforementioned literature analysis, it is evident that focusing on safeguards to manage the SMEs cybersecurity risks through the Prevent function, is one of the most critical topics recognised by the research community. More specifically, the identity management, authentication, access control along with awareness and training of SMEs seem to be the most important aspects. Regarding awareness and training, emphasis was given both to the training of personnel without cybersecurity expertise and individuals with more specialised roles in cybersecurity field.

Furthermore, considerable effort has been made in understanding the cybersecurity risks of SMEs via the Identify function. The research focuses mainly on asset management, including data, hardware, software, and systems. Also, risk assessment is well represented by the reviewed literature, through the discovery of vulnerabilities in assets and frequency and impact of threats, towards understanding potential risks.

Moreover, approximately the half of the reviewed literature focuses on strategies and techniques for detecting cyber attacks, through the continuous monitoring of network and assets. ML and AI seems to play a critical role in this regard, as referenced multiple times. However, less attention is given to the analysis of potential adverse events and intrusions.

As regards Govern function, the one third of the reviewed literature address its practices. Here, the focus of the research was to identify SMEs priorities, risk tolerance and organisation missions. Also, among the papers that used Govern function, the majority stressed the organizational cybersecurity policy, along with its communication and enforcement. Similarly, adequate attention was given to the cybersecurity roles and responsibilities within the participant SMEs. Finally, the category related to supply chain risk management was not represented in the literature.

Cybersecurity Landscape and Threat Analysis

Finally, the functions Respond and Recover are the less represented. However, more studies were aligned with Respond function, capturing all the included categories, with particular focus on incident response plan, report, and categorization. Recover, being the less examined function was mainly addressed for restoring the attacked system to a normal state and communicating the respective incidents.

The above discussion indicates that the research and studies on SME cybersecurity mainly address threat identification, prevention, and detection. Less but considerable focus is given to the organisation's cybersecurity policies and expectations. Finally, recovery and response to cyber attacks practices received less attention.

Following the overview of the cybersecurity landscape of SME's and the focus of the cybersecurity research activities in compliance with the NIST CSF 2.0, a set of recommendations is described below, that will assist SMEs to engage with cybersecurity best practices.

Firstly, it is evident that numerous cybersecurity agencies worldwide have consensus on common cybersecurity practices that should be adopted by SMEs [1], [8], [45], [13], [46], [47]. These practices include:

- **Training and awareness:** The employees, regardless of the level of expertise, should undergo regular training sessions to enable them to identify and deal with cybersecurity threats. Moreover, individuals in IT roles should receive specialised training to ensure they possess the required skills.
- **Secure access to systems:** Access to business computers should be restricted solely to authorised individuals. Laptops, being prone to theft or misplacement, should be securely locked when not in use. Moreover, each employee should possess a separate user account with strong passwords. Finally, administrative privileges should be granted to IT personnel and essential staff members.
- **Secure devices:** Utilising the most recent security software, web browser, and operating system constitutes the most effective defence against viruses, malware, and other threats. Organisations should configure antivirus software to perform scans following each update and promptly install other critical software updates as they become available. Moreover, with the increase of remote working, measures such as devices passwords, encryption, and access control should be employed.
- **Network security:** Firewalls monitoring incoming and outgoing network traffic, play a critical role in safeguarding the systems of SMEs. It's imperative to deploy firewalls to protect all essential systems, with particular attention to the use of a firewall to shield the SME's network from Internet threats.
- **Secure backups:** Regularly or automatically backing up crucial information should be a common practice of SMEs. These backups should be stored separately from the organisation's production environment. Without consistent backups, recovering data in case of cybersecurity incidents may prove impossible.
- **Incident response plan:** Roles and responsibilities should be carefully allocated to ensure timely response to security incidents, as well as appropriate handling. The incident report plan should be accompanied by well-defined guidelines and facilitated by tools that can trigger alerts in case of an upcoming threat.

Cybersecurity Landscape and Threat Analysis

Although the above recommendations are critical and should serve as the basis for maintaining a robust cybersecurity posture, particular emphasis should be given on recommendations tailored specifically for SMEs, ensuring that they can effectively adhere to the suggested guidelines. In this direction, ENISA [1] has identified recommendations towards policy makers and governmental bodies to assist SMEs. These recommendations are described below.

- **Promote cybersecurity at a broader level:** Relevant authorities, in collaboration with business representative organisations, should initiate targeted awareness campaigns on cybersecurity issues, specifically tailored for SMEs' owners, managers, employees, and shareholders. Despite previous efforts, it's evident that many SMEs remain unengaged, necessitating future campaigns to be more SME-focused.
- **Provide targeted guidelines and templates:** Many SMEs are not familiar with precise standards and strategies for enforcing cybersecurity measures. Therefore, it is critical to create straightforward and well-defined guides, plans, procedures, and exercises to help SMEs overcome this situation. Handbooks and reports with best practices should present practical examples and plain language.
- **Design cybersecurity standards tailored for SMEs:** Although, multiple cybersecurity standards exist, SMEs fail to adopt them for various reasons. The major reason lies in the perception of SMEs that these standards only target large enterprises. Hence, SMEs ought to be motivated to follow cybersecurity standards. To facilitate this, specialised guidelines and standards should be developed that target SMEs, focusing on effectively adopt them.
- **Provide affordable cybersecurity solutions:** Cost is a significant burden for SMEs when it comes to applying cybersecurity solutions. These costs may include the purchasing of cybersecurity products, services, and external advisory. Excessive expenses may discourage SMEs from seeking cyber-shielding services. Due to this reason, the provision of cybersecurity tools with a low and reasonable cost should be considered.

In conclusion, this section presented the cybersecurity landscape of SMEs, by presenting common attacks alongside their impacts, and the cybersecurity challenges that SMEs face. The conducted literature review identified the research directions and trends, while the research objectives were mapped to the NIST CSF 2.0 framework. Finally, insights from the literature analysis were collected, accompanied by recommendations of governmental organisations and agencies for strengthening the SMEs' cybersecurity posture. The above analysis aimed to offer valuable perspectives on the existing cybersecurity environment, facilitating the next steps and directions that NERO will follow, towards providing cyber immunity, resilience and awareness training in SMEs.

3 End-user Requirements Analysis

End user requirements ensures that the final product delivered, including all the individual sub-components meet the needs and the expectations of the user stakeholders. As a part of a contractual agreement, the user requirement protects the developer from demands of a user for features that are not documented or non-contractual and prevents developers from claiming software to be ready if it does not fulfil the requirements. In the scope of IT, end-user requirements are used to clarify for whom an IT software product is developed. The term “end-user” determines how the identified end-users and any other interested party will benefit from the developed product and how they will finally use it. User requirements analysis within NERO includes the following characteristics:

- are verifiable, clear, concise, complete, consistent, traceable, viable, necessary, and implementation manageable,
- are precise and well-defined.
- are prioritised following the MoSCoW (Must, Should, Could, Would) method as a prioritization technique

To move forward with the NERO system design and architecture, the system requirements that will be the result of the end-user requirements will be classified as functional or non-functional, and prioritised based on MOSCOW methodology. Furthermore, the business requirements will be identified, aiming to construct a solid business plan and conduct a deep market analysis.

3.1 Methodology for requirements collection and analysis

The requirements collection is an iterative process, undergoing multiple rounds spanning from insights and findings from the current cybersecurity landscape of SMEs, questionnaires publicly distributed, and targeted interviews with carefully selected interviews. The partners in charge of developing and integrating the technological components need to understand the needs of the pilots represented by the application domains as well as get an insight into SMEs' needs in general. Unfortunately, the partners hosting the pilots do not necessarily have the ability to translate their needs for protecting their assets, to specific requirements without any support related to the research context and the available technologies. This support is crucial in order to avoid ending up with generic requirements that look more or less similar to the project objectives. In order to overcome this issue, a detailed concise, and user-friendly questionnaire was constructed and circulated which in combination with the future face-to-face interviews with pilot users, will clearly bring out the state of the art of cybersecurity issues, norms, protocols, vulnerabilities being faced by the SMEs as well as the best practices to deal with these issues.

Once the requirements are identified, they should be traceable. This means that the requirements will be documented in a way enabling the NERO partners to determine the requirements' origins. Furthermore, it is important to note that all the identified requirements will be prioritized using MOSCOW methodology and will be presented in D2.2.

3.2 NERO Questionnaire Analysis

3.2.1 NERO Questionnaire General Information

By making use of the extensive networks of the consortium members, the questionnaire that was formulated, was disseminated to organisations of all sizes in the industry, in order to gather useful information about the current state of Cyber-security in SMEs and in turn verify that the followed approach for the pilot use cases, as well as the NERO portfolio of solutions offered are in the right direction. Having achieved an adequate and reliable number of responses, **72 in total**, the results and conclusions are presented in the following paragraphs.

A key part of the work in this task was the design and circulation of a “structured” and targeted questionnaire related to the field of cybersecurity and how to tackle the specific dimensions of awareness, training, and education and fostering a culture of cybersecurity awareness and resilience within both organisations and individuals. This questionnaire was mainly circulated to a wider audience of people and organizations involved in software development and the responses provided were analysed, grouped, and helped in further defining and refining the project’s use case scenarios. Structured questionnaires were designed, developed, and distributed on a case-by-case basis to specific audiences. The use of a properly designed questionnaire for the collection of data results in the collection of important and different data from multiple sources which, if properly exploited, can be an important parameter in the development of relevant intervention proposals. Particular attention has been paid to the structure and content of the questionnaire to ensure:

- The collection of both qualitative and quantitative data from correspondingly designed questions.
- The ease of completing it and the objectivity of the answers. The majority of questions were "closed", to facilitate respondents in their answers.
- The ease of statistical analysis of the data, to avoid any answers that may distort the results.

The questionnaire has been developed in a way to ensure, as far as possible, both the collection of all the necessary data, as well as ensuring the participation of members completing it (increasing the response rate). Before distributing the questionnaires, the questionnaire was piloted to a small sample of selected respondents, so that it was tested for understanding and ease of completion (Pilot Test). Based on the results of the test and the relevant proposals, the necessary modifications have been made and its finalisation granted.

3.2.2 NERO Questionnaire Results

This section illustrates the graphical representation of the answers collected from the aforementioned questionnaire along with the corresponding interpretation of the results. The questionnaire begins with some demographical questions, followed by general questions aimed at understanding the cybersecurity posture of SMEs. Subsequently it progresses with more technically focused questions tailored for specialised personnel with technical skills. Therefore, the questionnaire has been designed to address both SMEs with technical expertise and those without.

It is clarified that a subset of the questions included an “out of scope” option for selection. In this case, the reasons for selecting “out of scope” have been also collected and presented alongside the initial question. For each question a pie chart is provided, demonstrating the percentage of the received responses, accompanied by discussions and interpretation of the illustrated results.

End-user Requirements Analysis

Q1: Job Role

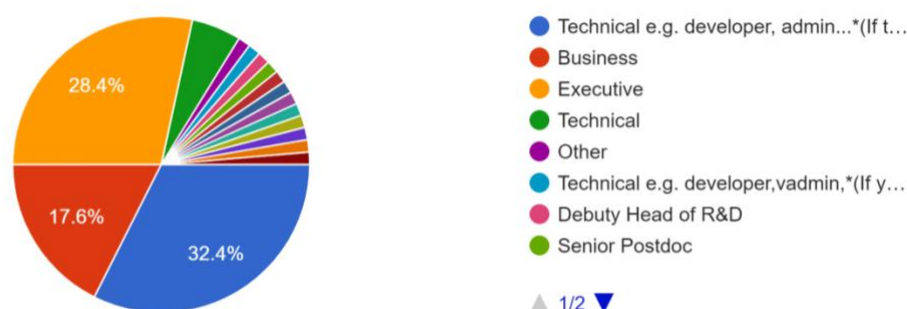


Figure 5: Response to Q1.

As shown in Figure 5, Out of the responders, 28.4% are executives responsible for making strategic decisions and overseeing the overall operations and direction of the organisation. 17.6% of the responders are business people and 32.4% are technical people (administrators, developers, etc). This implies that NERO should tackle business and technical profiles within an organisation.

Q2: Company Size

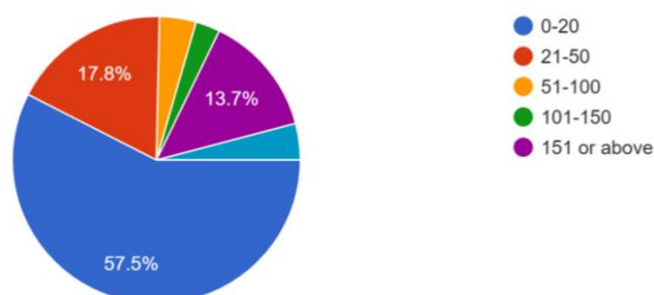


Figure 6: Responses to Q2.

The questionnaire is addressed to SMEs and as shown in Figure 6, the majority of the organisations (57.5%) that responded, employ less than 20 employees whereas 17.8% employ up to 50 people. 13.7% are over 150 employees. The responses received will provide insights into their unique needs, challenges, and pain points. This implies that the focus should be on SMEs with up to 50 personnel.

End-user Requirements Analysis

Q3: Country

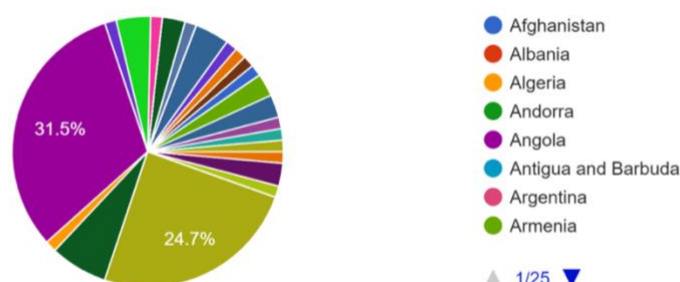


Figure 7: Responses to Q3.

As shown in Figure 7, the majority of the answers received are within the EU, comprising nearly 90% of the total responses, suggesting a strong engagement or targeted reach within this region. The remaining 10% is spread across Africa and the Far East, indicating a lesser degree of participation or possibly different levels of access to the survey from these areas.

Q4: Are your employees required to have a strong password* in their company accounts (e.g., email, operating system user etc)?

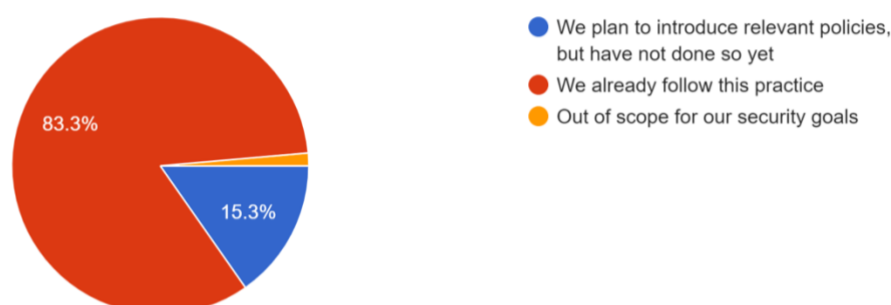


Figure 8: Responses to Q4.

As shown in Figure 8, 83.3% have strong password policy in place, whereas 15.3% they plan to introduce this policy and 1.4% consider that this is out of scope of their security goals. Even for this 16.7% that doesn't have such a policy, it is crucial to make efforts for creating awareness.

End-user Requirements Analysis

Q5: Are your employees required to regularly change their company accounts' passwords (e.g., email, operating system user, etc.)?

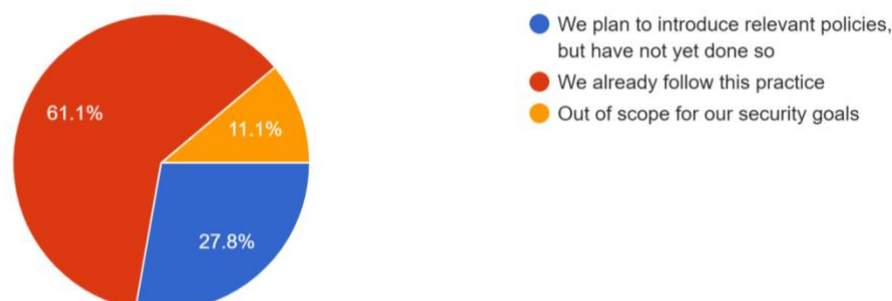


Figure 9: Responses to Q5.

As shown in Figure 9, out of the responses received, 61.1% are required to regularly required to change their company accounts' passwords, 27.8% plan to introduce relevant policies and 11.1% consider that this practice is out of scope of their security goals. Awareness is needed for employees to further abide by this policy.

Q6: Do you train your employees in the area of cybersecurity?

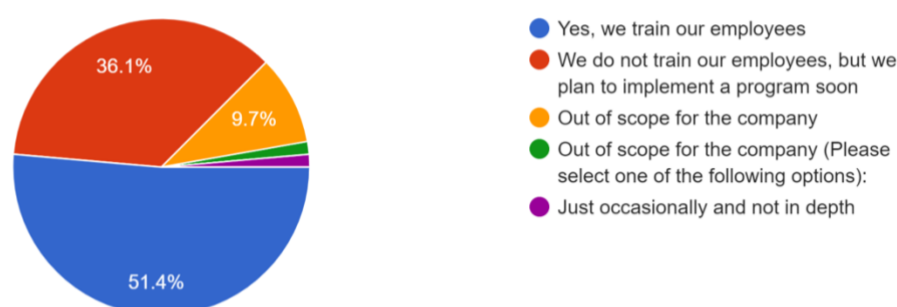


Figure 10: Responses to Q6.

As shown in Figure 10, only 51.4% of the companies train their employees, whereas 36.1% do not train their employees and another 9.7% of the responders consider training as out of scope for the company and another 1.4% they train them only occasionally and not in depth. Out of those companies that train their employees, 62.2% train them once a year, 21.6% train them twice a year, 2.7% train them every time cybersecurity knowledge evolves, 2.7% on special milestones, 2.7% per quarter, 2.7% every 3 months and 2.7% not scheduled-discussed as AOB maybe once a quarter. More intensive efforts are needed for further training.

For those who have answered out of scope, 37.5% indicate lack of time, another 37.5% indicate limited expertise, 12.5% indicate that they have employees that work with cybersecurity and 12.5% indicate lack of funds to support training.

Q7: Are you protecting the endpoints (PCs, Laptops, Mobile Phones, Equipment) in your digital infrastructure?

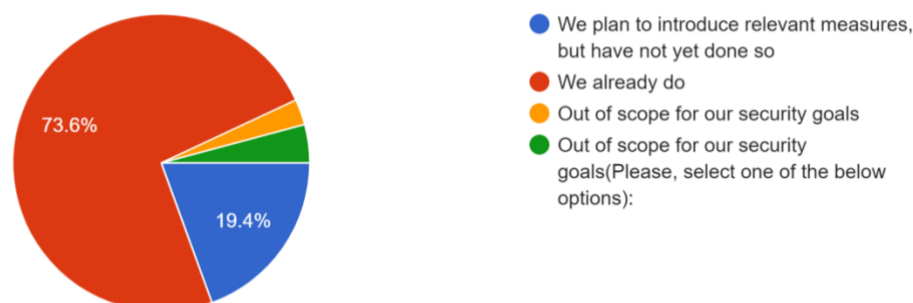


Figure 11: Responses to Q7.

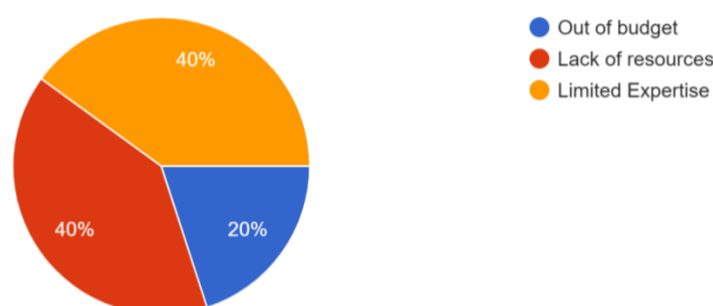


Figure 12: Responses if “Out-of-scope” is selected for Q7.

As shown in Figure 11, 73.6% of the responders indicated that they are protecting their endpoints, 19.4% are planning to introduce relevant measures to protect their endpoints. The remaining 6% consider this as out of scope of their security goals. Hence, almost 30% reply that no end point protection exists which is very risky and dangerous for SMEs operation. This is an opportunity for NERO to penetrate the market and offer a competitive and user-friendly solution.

For those who answered out of scope, as shown in Figure 12, 40% indicate that they lack resources to protect their endpoints, 40% lack expertise and 20% lack the necessary budget. This implies that SMEs require a robust, very competitive, nearly fully automatic solution to be applied with minimum if not zero skilled effort required.

Q8: Have you defined procedures to monitor and protect against insider threats?

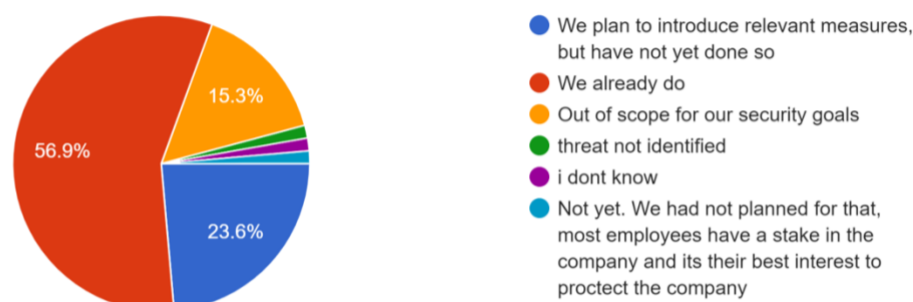


Figure 13: Responses to Q8.

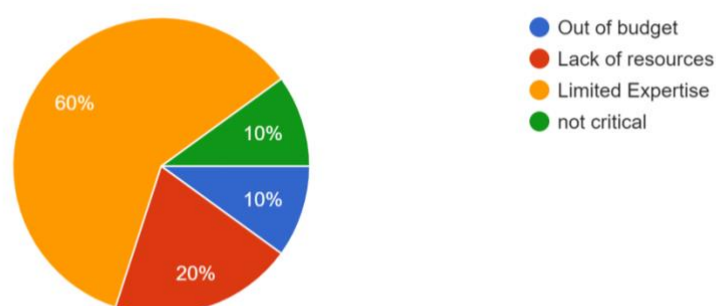


Figure 14: Responses of “Out-of-scope” is selected for Q8.

As shown in Figure 13, 56.9% of the responders indicated that they have defined procedures within the company to monitor and protect against insider threats. Another 23.6% the plan to define such procedures and 15.3% consider this as out of scope of their security goals. Another 4.2% indicated that threats were not identified, they do not know if their company has any defined procedures for monitoring or they did not plan for that.

As shown in Figure 14, 60% of the responders that answered out of scope, indicated that they have limited expertise, 20% indicated that they lack resources and 10% indicated lack of budget. Another indicator validating that NERO concept is viable and that SMEs require simple and effective solutions and targeted training.

End-user Requirements Analysis

Q9: Do you apply risk assessment to your third-party vendors?

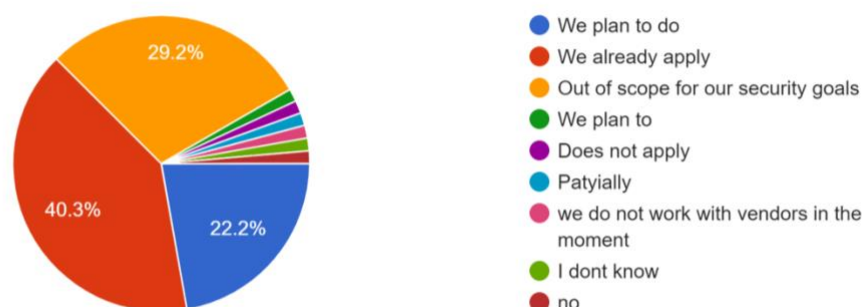


Figure 15: Responses to Q9.

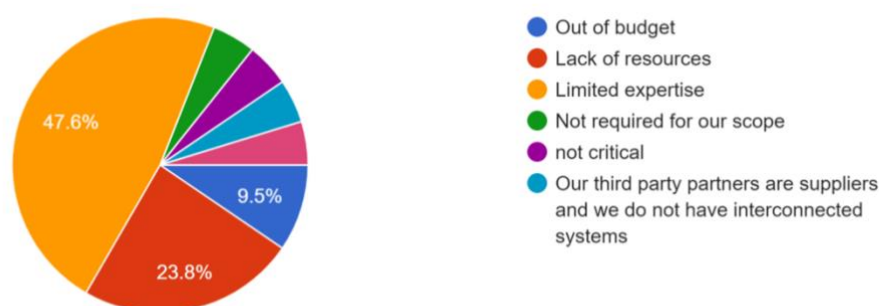


Figure 16: Responses if “Out-of-scope” is selected for Q9.

As shown in Figure 15, out of the responders 40.3% indicated that they already apply risk assessment to their third-party vendors, 22.2% they plan to introduce risk assessment, 29.2% consider this as out of scope for their security goals. Only 1.4% plan to introduce risk assessment for their 3rd party vendors and another 1.4% they partially do it.

As shown in Figure 16, out of those who answered out of scope 47.6% indicated limited expertise, 23.8% indicated lack of resources, 9.5% indicated out of budget, 4.8% indicated that this is not required for their scope, 4.8% consider this as not critical, 4.8% indicate that their third-party partners are suppliers and do not have interconnected systems.

Q10: Do you provide limited access to sensitive data only to authorised parties/personnel?

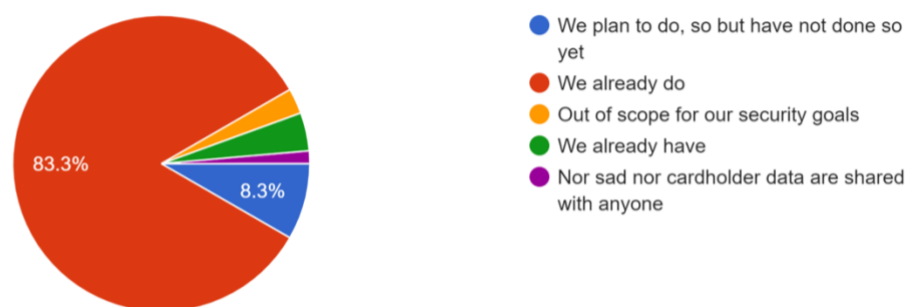


Figure 17 : Responses to Q10.



Figure 18: Responses if “Out-of-scope” is selected for Q10.

As shown in Figure 17, 83.3% of the responders indicated that they provide limited access to sensitive data only to authorised personnel. Another 8.3% plan to enforce this policy and 2.8% indicate that this is out of scope for their security goals. Although the majority is careful about this sensitive issue, still a small percentage proves the need for a system like NERO to create awareness, train and provide solutions.

As shown in Figure 18, it is noteworthy that for the category of respondents who indicated the project was out of scope, all have attributed this to a lack of expertise, not to financial constraints or resource availability. This unanimous response underscores a critical gap in skills or knowledge within the group surveyed.

End-user Requirements Analysis

Q11: Is your internal hardware/network (PCs, routers, firewall, etc.) monitored?

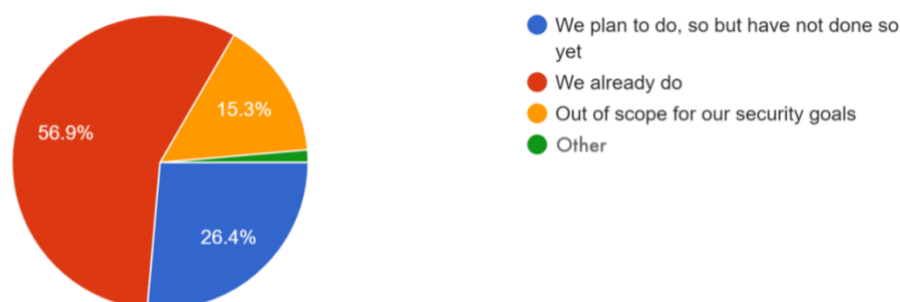


Figure 19: Responses to Q11.

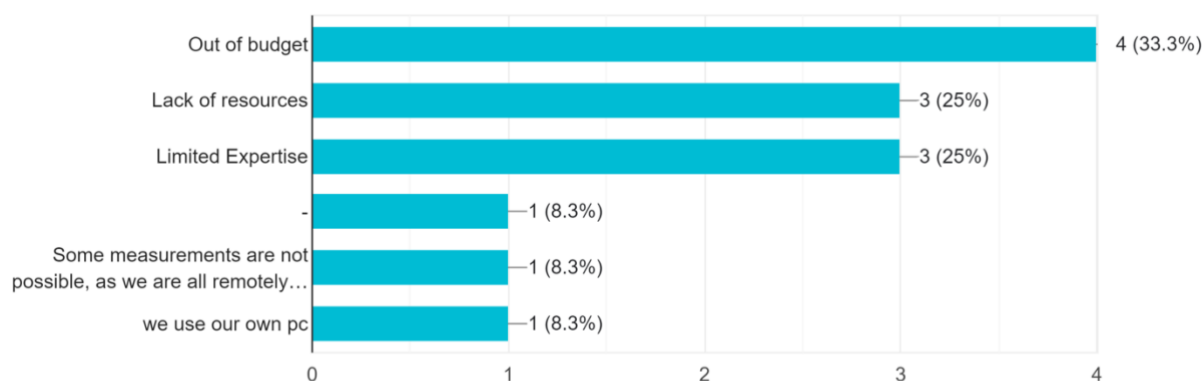


Figure 20: Responses if “Out-of-scope” is selected for Q11.

As shown in Figure 19, out of the responses received, 56.9% responded that their internal hardware/network are monitored. 26.4% plan to monitor their hardware/infrastructure and 15.3% consider this as out of scope.

As shown in Figure 20, 33.3% of the responders indicated out of budget, another 25% indicated that they lack resources and have limited expertise, 8.3% are not in a position to measure/monitor the hardware as they are working remotely, 8.3% use their own Personal Computer (PC). A very crucial point and key to maintain secure operations. It proves that SMEs need to clearly consider cloud-based solutions for their applications, but at competitive pricing.

End-user Requirements Analysis

Q12: Have you (as a company) limited admin accounts access only to specific personnel that absolutely require that access as part of their job position/role?

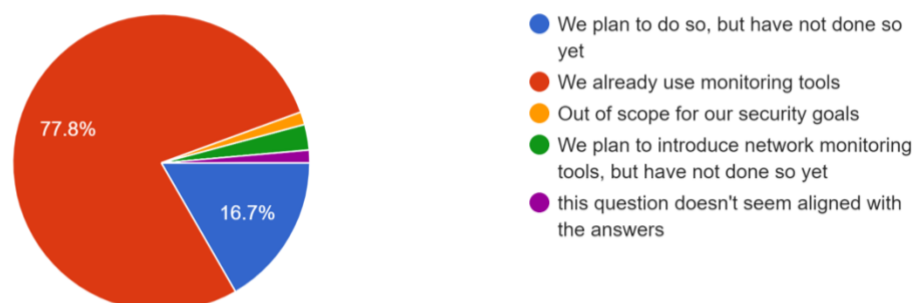


Figure 21: Responses to Q12.



Figure 22: Responses if “Out-of-scope” is selected for Q12.

As shown in Figure 21, out of the responses received, 77.8% indicated that they limit admin account access only to specific personnel that they absolutely require that access. 16.7% plan to limit this access 2.8% indicate that they plan to introduce monitoring tools and 1.4% consider this as out of the scope of their security goals.

As shown in Figure 22, it is clear that every respondent who reported the project as out of scope did so due to a lack of resources. This points to a potentially widespread issue where the constraints are material or logistical rather than financial or skill-based, which could suggest the need for a strategic review of resource allocation and project management.

End-user Requirements Analysis

Q13: Are you requesting proof (e.g., penetration testing) for validating the security of the 3rd party software tools that you use within the organisation?

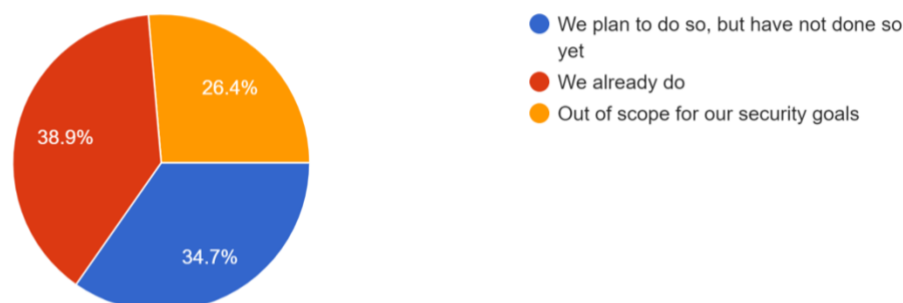


Figure 23: Responses to Q13.

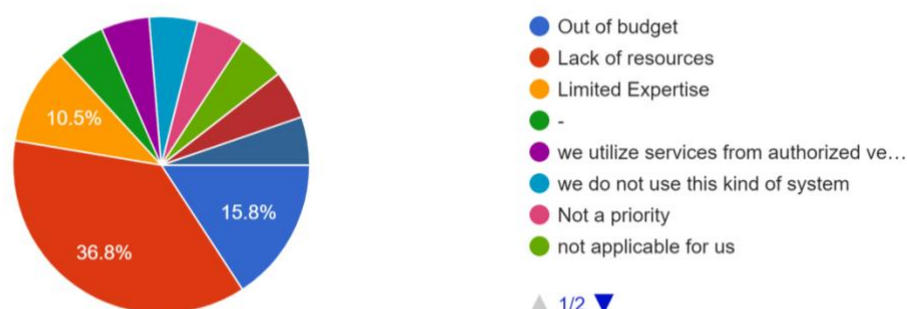


Figure 24: Responses if “Out-of-scope” is selected for Q13.

As shown in Figure 23, 38.9% indicated they are requesting proof such as pen tests for validating the security of 3rd party software tools, 34.7% indicate that they plan to request proof and 26.4% consider this as out of scope of their security goals. A key issue to be considered and be part of NERO in the context of training SMEs to ask from third-party vendors proof of penetration tests from an accredited party.

As shown in Figure 24, the chart indicates that the primary concern for 36.8% of the respondents is a lack of resources, which could highlight issues such as inadequate equipment, insufficient manpower, or a deficiency in materials necessary to achieve their goals. This significant proportion suggests a common bottleneck that could limit the potential of many entities, underscoring the need for a review of resource distribution or a strategy to enhance resource acquisition and management.

End-user Requirements Analysis

Q14: Are you validating the security of the third-party hardware equipment that you use within the organisation? (e.g., data comms devices, medical devices, POS, etc)

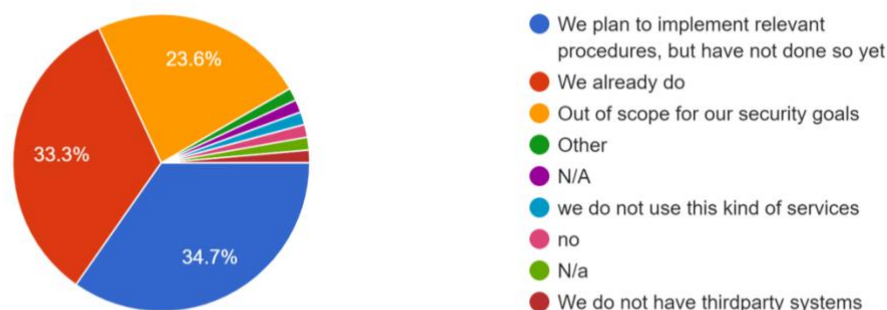


Figure 25: Responses to Q14.

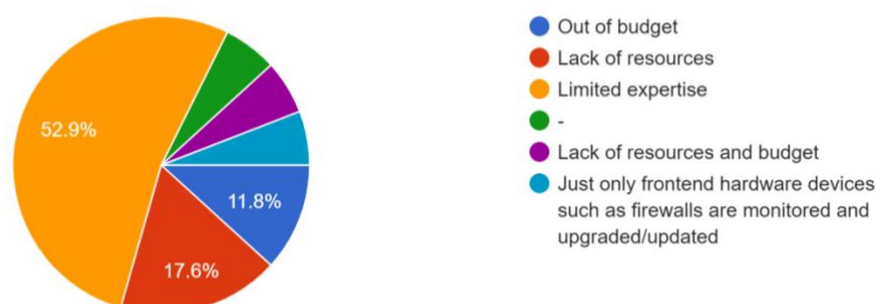


Figure 26: Responses if "Out-of-scope" is selected for Q14.

As shown in Figure 25, only 33.3% of the responders indicated that they are validating the security of third-party hardware equipment that they use within the organisation. 34.7% are planning to introduce security validation of third-party hardware and another 23.6% consider this as out of scope for their security goals. The low percentage of organisations validating the security of third-party hardware underscores the importance of prioritising robust security practices throughout the supply chain. Security vulnerabilities in one component can potentially cascade throughout the supply chain, affecting multiple organisations. Validating the security of third-party hardware helps mitigate these supply chain risks.

As shown in Figure 26, 52.9%, indicates "Out of budget" as a key issue, pointing to financial constraints as a prevalent challenge. This is followed by "Lack of resources" at 17.6%, suggesting that beyond financials, there are significant material or infrastructural deficiencies to address.

End-user Requirements Analysis

Q15: Are your employees adequately trained in security awareness by internal or external specialists? (e.g., in recognising phishing emails)

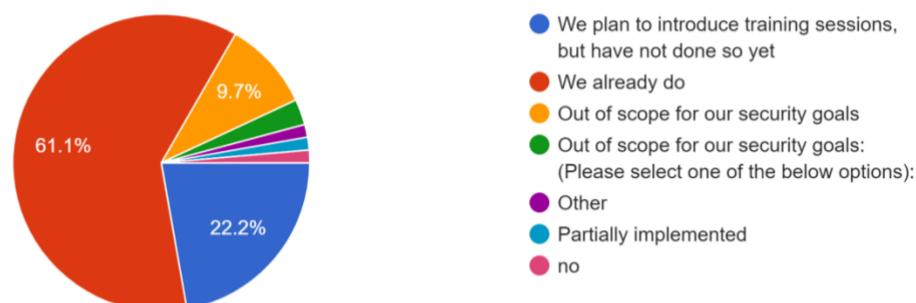


Figure 27: Responses to Q15.

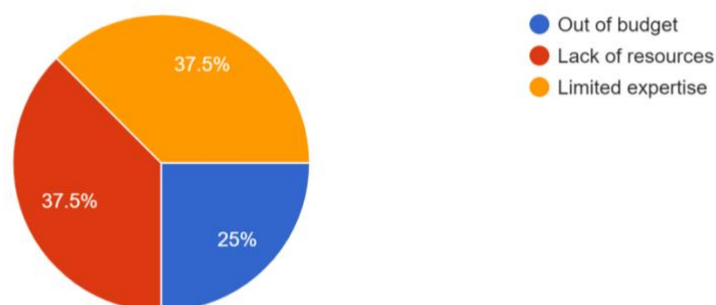


Figure 28: Responses if “Out-of-scope” is selected for Q15.

Figure 27, highlights the gap in security awareness training with 61.1% of participants yet to receive it. This underscores the need for organisations to prioritize and expedite such educational programs to enhance their overall security posture.

As shown in Figure 28, an equal division between respondents facing budgetary constraints and those with limited expertise, each accounting for 37.5%. A smaller 25% cite budget constraints as their primary challenge, suggesting a more pronounced need for financial and educational investments over material ones.

End-user Requirements Analysis

Q16: Are the employees of your company trained in emergency response procedures following a cyber attack?

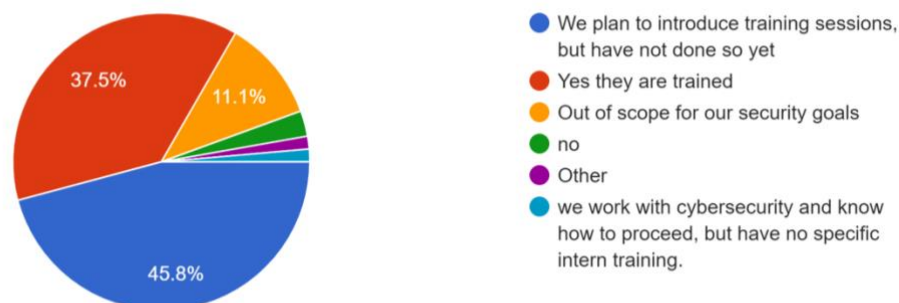


Figure 29: Responses to Q16.

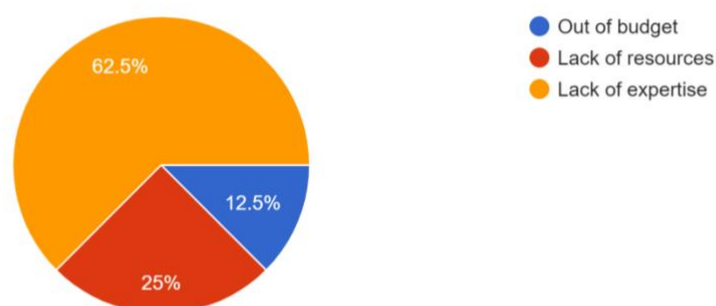


Figure 30: Responses if “Out-of-scope” is selected to Q16.

The aftermath of an attack is also a crucial event, and SMEs need to have some knowledge of how to react and especially bear in mind the need to speak with experts and get advice. As shown in Figure 29, the responses indicate that 45.8% plans to introduce training sessions, while the 37.5% of the participants are currently training the employees to be prepared for emergency response procedures. SMEs that do not employ such policies mainly cite lack of expertise as a reason, according to Figure 30.

Q17: Do you encrypt internal databases and customer information?

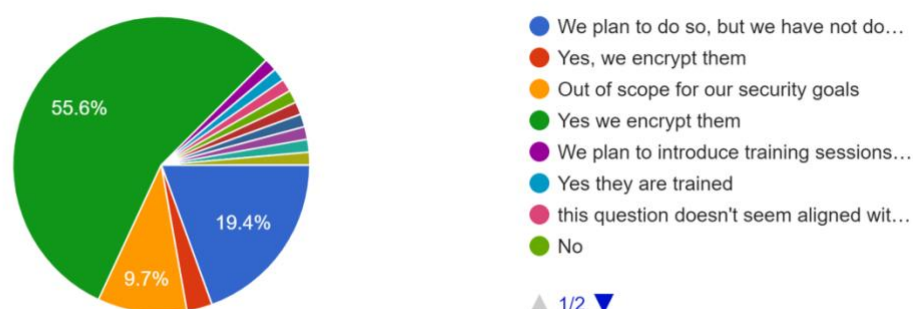


Figure 31: Responses to Q17.

End-user Requirements Analysis

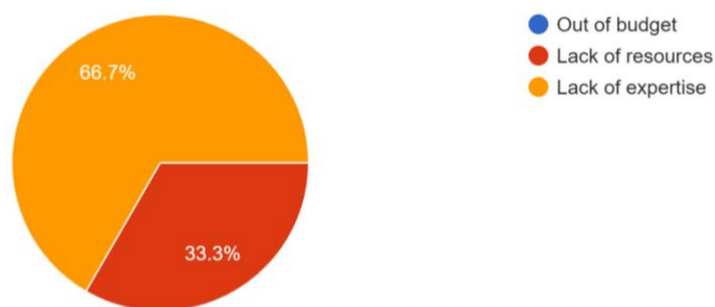


Figure 32: Responses if “Out-of-scope” is selected for Q17.

According to Figure 31, 55.6% of respondents indicated that they encrypt internal databases and customer information; a notably important action in security measures within these organisations. The 19.4% planning to implement encryption highlights a recognition of the importance of such measures, but the lack of implementation suggests a need for prioritisation or resource allocation.

Regarding the out-of-scope responses (Figure 32), the majority attributing it to a lack of expertise (66.7%) indicates a potential knowledge gap within these organizations, while a smaller proportion (33.3%) cite resource constraints. Interestingly, none mentioned budgetary limitations, implying that the issue primarily lies in knowledge and resource allocation rather than financial constraints. Addressing these gaps through education and resource allocation could significantly enhance data security measures and mitigate risks.

Q18: Is your intranet network periodically tested for vulnerabilities?

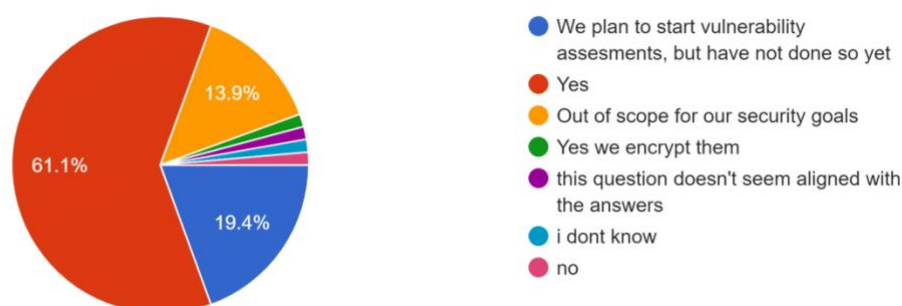


Figure 33: Responses to Q18.

End-user Requirements Analysis

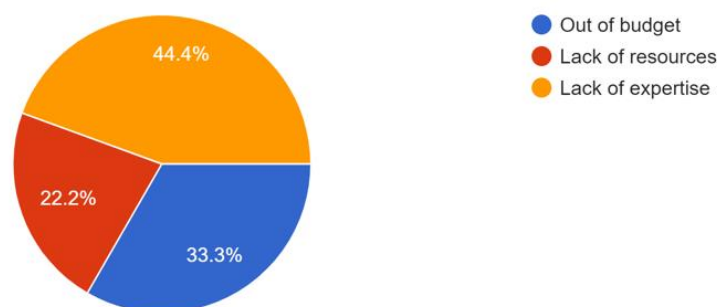


Figure 34: Responses if “Out-of-scope” is selected for Q18.

According to Figure 33, 61.1% of respondents affirm that their intranet networks undergo periodic vulnerability testing, and there's a substantial commitment to maintaining the security of these systems. This proactive approach suggests a recognition of the importance of identifying and addressing potential weaknesses before they can be exploited by malicious actors, thereby bolstering overall network resilience. The 19.4% planning to commence vulnerability assessments but haven't done so yet indicates an awareness of the need for such measures, with intentions to align with best practices. However, the 13.9% citing the task as out of scope for security goals reveals a concerning oversight, potentially leaving these organizations vulnerable to undetected vulnerabilities.

According to Figure 34, among the out-of-scope responses, the majority attribute it to a lack of expertise (44.4%), emphasising the importance of investing in training and upskilling to bridge this gap. Additionally, a significant proportion cite budget (22.2%) and resource constraints (22.2%), highlighting the need for adequate allocation of funds and manpower to effectively address security objectives. By addressing these gaps in knowledge, budget, and resources, organizations can strengthen their intranet security posture and mitigate potential risks more effectively.

Q19: Do the employees of your company use their personal smartphones for work purposes?

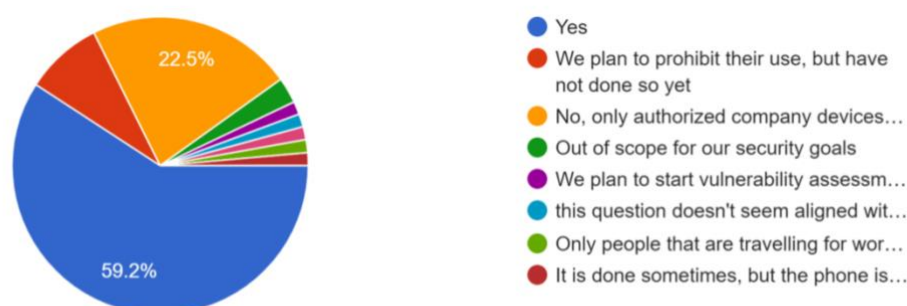


Figure 35: Responses to Q19.

According to Figure 35, 59.2% of respondents indicated that employees use their personal smartphones for work purposes; a prevalent trend of blending personal and professional technology within these organisations. While this can enhance flexibility and productivity, it also introduces potential security risks, as personal devices may lack the same level of security controls as company-issued ones. The 22.5% who restrict work activities to authorised devices demonstrate a proactive approach to mitigating such risks, ensuring that only devices meeting specified security standards are utilised for work-related tasks. However, the smaller percentage intending to prohibit personal device use but haven't implemented this policy yet suggests a recognition of the security implications but a delay in enforcing measures to address them. It's crucial for organisations to strike a balance between flexibility and

End-user Requirements Analysis

security by implementing clear policies, providing secure alternatives, and offering education on safe device usage to mitigate potential risks effectively.

Q20: Do you frequently back-up your data?

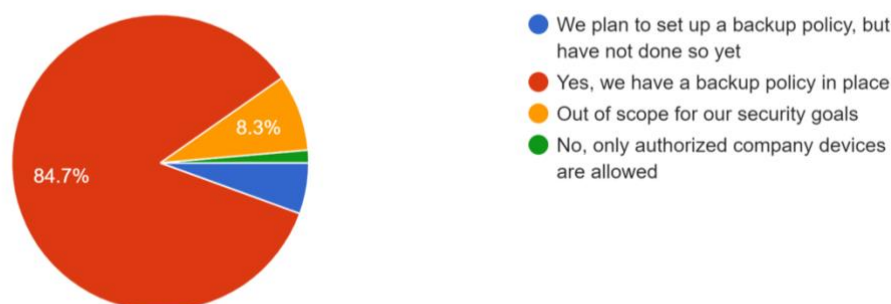


Figure 36: Responses to Q20.



Figure 37: Responses if “Out-of-scope” is selected for Q20.

According to Figure 36, with an overwhelming 84.7% of respondents affirming the presence of a backup policy in place, there's a strong commitment to data protection within these organisations. This proactive approach to data backup indicates a recognition of the importance of safeguarding critical information against loss or corruption, thereby ensuring business continuity and mitigating potential disruptions. However, the 8.3% considering data backup out of scope for security goals raises concerns about potential blind spots in risk management strategies.

According to Figure 37, among the out-of-scope responses, the majority cite resource and knowledge limitations (48.1%), emphasizing the importance of investing in training and infrastructure to support robust backup procedures. Additionally, a significant proportion mentions budget constraints (18.5%), highlighting the need for adequate allocation of funds to support data protection initiatives. By addressing these challenges through education, resource allocation, and strategic planning, organisations can enhance their resilience against data loss and minimize the impact of potential incidents.

End-user Requirements Analysis

Q21: Do you have a data recovery plan?

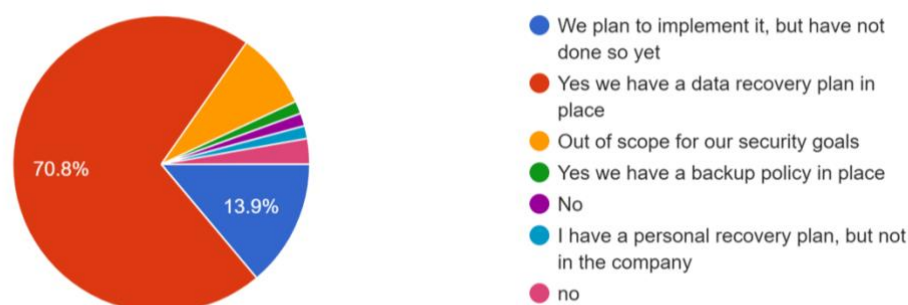


Figure 38: Responses to Q21.

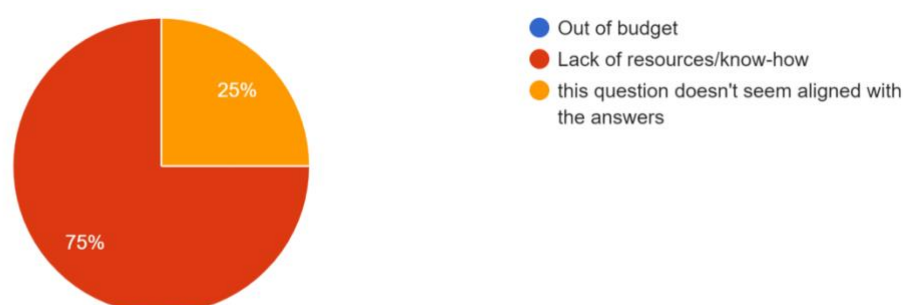


Figure 39: Responses if “Out-of-scope” is selected for Q21.

According to Figure 38, with more than 79% of respondents affirming the existence of a data recovery plan, these organisations exhibit a commendable commitment to mitigating the consequences of data loss incidents. This proactive stance reflects an understanding of the importance of swiftly restoring operations to minimise disruptions and mitigate potential losses. However, the almost 14% intends to implement such a plan but yet to do so highlights a gap between recognition and action, potentially leaving them vulnerable to prolonged downtime and significant data loss in the absence of a formal strategy.

According to Figure 39, among those considering it out of scope, the predominant reason cited is a lack of resources and expertise, underscoring the importance of investing in training and infrastructure to bolster data recovery capabilities. By addressing these challenges, organisations can enhance their readiness to navigate data loss events effectively.

Q22: Do you have an incident response team or policy in case of a cyber attack?

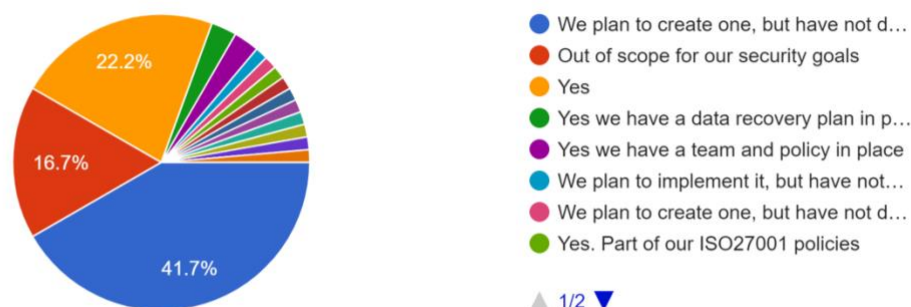


Figure 40: Responses to Q22.

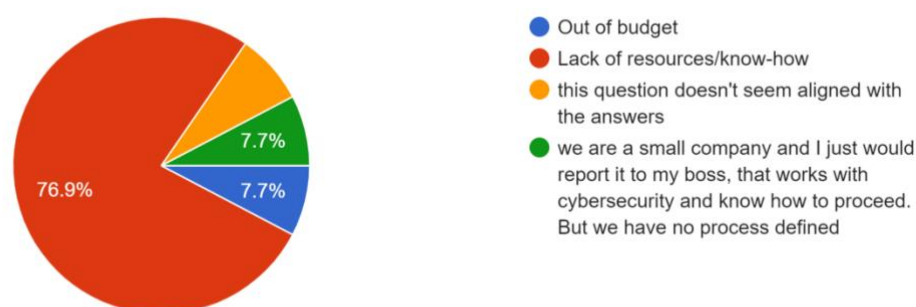


Figure 41: Responses if “Out-of-scope” is selected for Q22.

According to Figure 40, with only 22.2% of respondents confirming the presence of an incident response team or policy in case of a cyber attack, there appears to be a significant gap in preparedness within these organisations. Having a dedicated team or policy is crucial for swiftly and effectively responding to cyber threats, minimising the potential damage and facilitating recovery. The 41.7% planning to create such a team or policy reflects an awareness of the importance of preparedness but also highlights a current deficiency.

According to Figure 41, among those considering it out of scope, the overwhelming majority (76.9%) cite a lack of resources and know-how, indicating a critical need for investment in training and infrastructure to establish robust incident response capabilities. Additionally, a small proportion mention budget constraint, although this is less frequently cited, suggesting that the primary challenge lies in knowledge and resource availability. By addressing these barriers, organisations can strengthen their ability to detect, respond to, and recover from cyber attacks effectively, thereby enhancing their overall cybersecurity posture.

End-user Requirements Analysis

Q23: Are your system updates enforced and frequently executed?

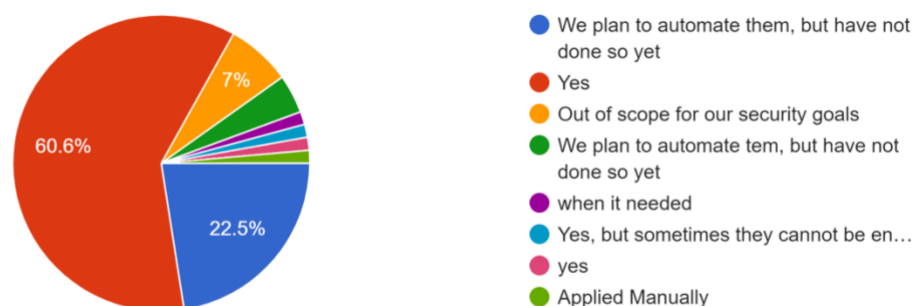


Figure 42: Responses to Q23.

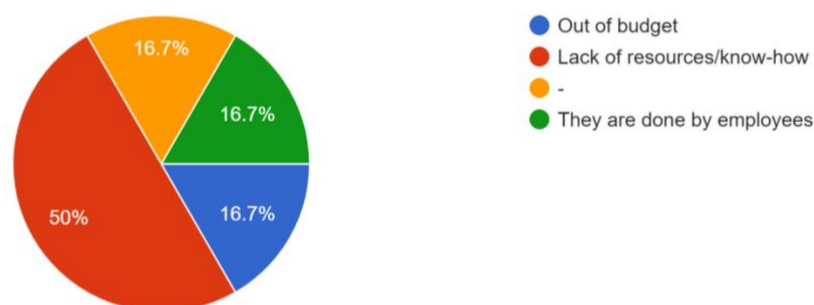


Figure 43: Responses if “Out-of-scope” is selected for Q23.

According to Figure 42, 60.6% of the participants prioritise regular system updates, which is crucial for system security. Another 22.5% plan to enforce updates, showing an intent to align with best practices. However, 7% consider updates out of scope, highlighting a concerning oversight in cybersecurity hygiene.

The significant barrier appears to be a lack of expertise, cited by 50% of respondents, while only 16.7% mention budget constraints, according to Figure 43. This underscores the need for education and skill development to address knowledge gaps. Automating update procedures could streamline processes and ensure systems remain secure. Overall, focusing on both knowledge enhancement and automation can bolster cybersecurity measures effectively.

End-user Requirements Analysis

Q24: Is your company regularly audited for physical and digital vulnerabilities?

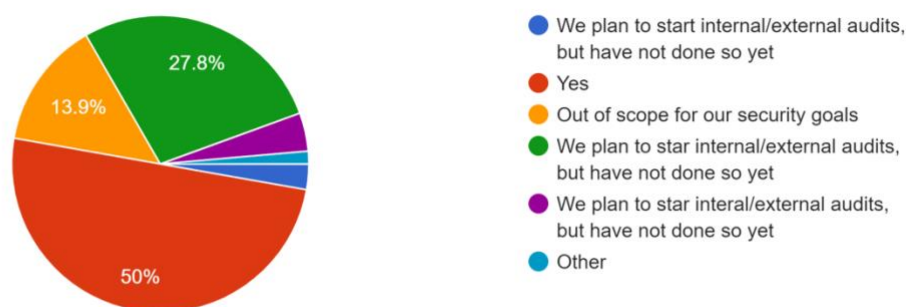


Figure 44: Responses to Q24.

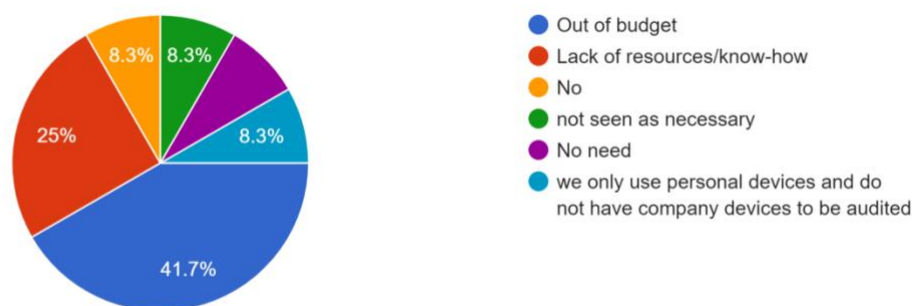


Figure 45: Responses if “Out-of-scope” selected for Q24.

According to Figure 44, among the respondents, 50% confirmed regular audits for physical and digital vulnerabilities, while 27.8% plan to initiate internal and external audits. Surprisingly, according to Figure 44, 13.9% consider audits out of scope, with 41.7% citing budget constraints and 25% lacking resources and expertise. This indicates a potential gap in security measures within these organisations, with a significant portion either unable or unwilling to prioritise audits. Regular audits are crucial for identifying and addressing vulnerabilities, ensuring robust defences against potential threats.

Q25: Are your company employees and/or customers automatically notified in case of suspicious system/account activity?

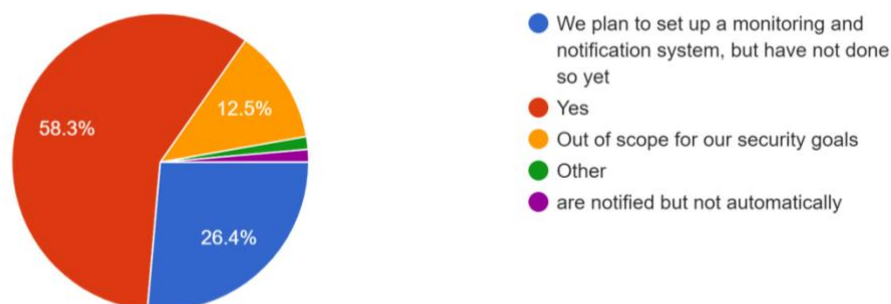


Figure 46: Responses to Q25.

End-user Requirements Analysis

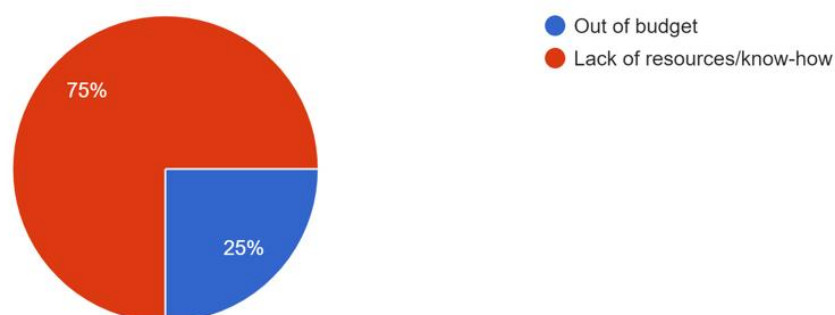


Figure 47: Responses if “Out-of-scope” is selected for Q25.

According to Figure 46, 58.3% confirm automatic notifications for employees and/or customers in case of suspicious system or account activity, indicating a proactive approach to security incident response. Additionally, 26.4% plan to establish monitoring and notification systems, showcasing an intent to enhance security measures in the future.

According to Figure 46, 12.5% consider this practice out of scope, with the majority attributing it to a lack of resources or expertise (75%), while a smaller proportion cite budget constraints (25%) (Figure 47). This highlights a potential gap in security readiness within these organisations, as automatic notifications play a crucial role in promptly addressing security incidents and mitigating potential damages. Investing in resources, expertise, and budget allocation to implement monitoring and notification systems can significantly enhance incident response capabilities and bolster overall security posture, ensuring the protection of both company assets and customer trust.

Q26: In case your company makes use of specialised technical equipment, has its security and interaction with the rest of the company systems been taken into account?

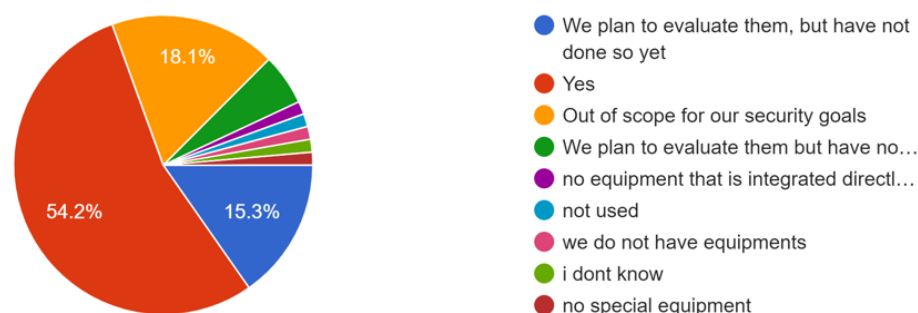


Figure 48: Responses to Q26.

End-user Requirements Analysis

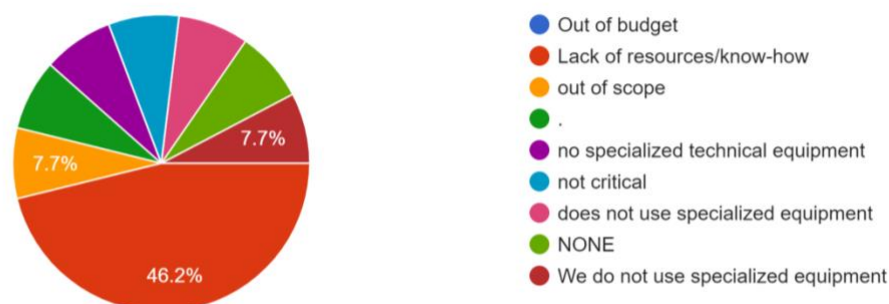


Figure 49: Responses if “Out-of-scope” is selected for Q26.

According to Figure 48, 54.2% affirm that their company has taken into account the security and integration of specialised technical equipment with the rest of the company systems. This demonstrates a proactive approach to ensuring the compatibility and security of these tools within the broader infrastructure. Additionally, 15.3% plan to evaluate their specialised equipment but haven't done so yet, indicating an awareness of the importance of such assessments and a commitment to addressing potential security risks.

According to Figure 48, 18.1% consider this aspect out of scope, with the majority citing a lack of resources or expertise (46.2%) as the primary barrier (Figure 49). A smaller proportion (7.7%) mention lack of expertise, suggesting a potential oversight or a reliance on more general-purpose tools. Addressing the challenges related to resource constraints and expertise is essential to comprehensively assess and mitigate security risks associated with specialised equipment, ensuring the resilience and integrity of the overall company infrastructure.

Q27: Are your products/services tracked in real-time for status and location?

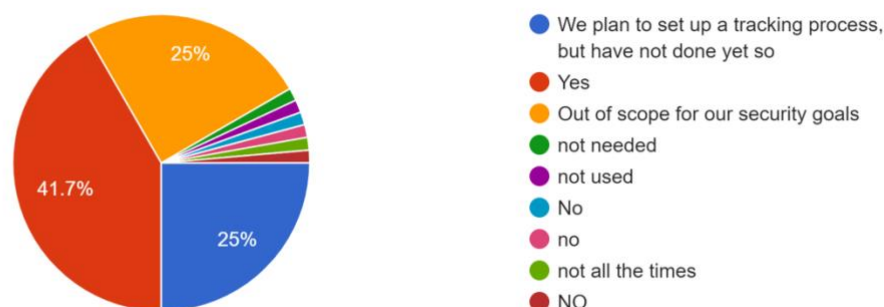


Figure 50: Responses to Q27.

End-user Requirements Analysis

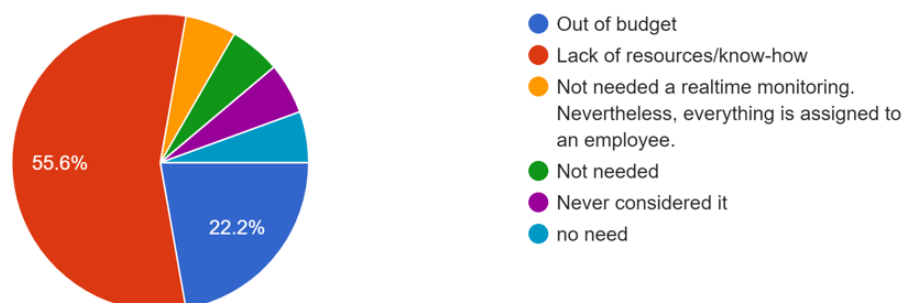


Figure 51: Responses if “Out-of-scope” is selected for Q27.

According to Figure 50, 41.7% confirm that their products/services are tracked in real-time for status and location, indicating a proactive approach to monitoring and management. Additionally, 25% plan to set up a tracking process but have not done so yet, reflecting an awareness of the importance of real-time tracking and intent to implement such systems in the future, and 25% consider this aspect as out of scope for their security goals.

According to Figure 51, the majority cited a lack of resources or expertise (55.6%) as the primary barrier. A smaller proportion (22.2%) mention budget constraints, suggesting potential challenges in allocating funds for tracking solutions.

Q28: Do you have a Business Continuity Plan (BCP)?

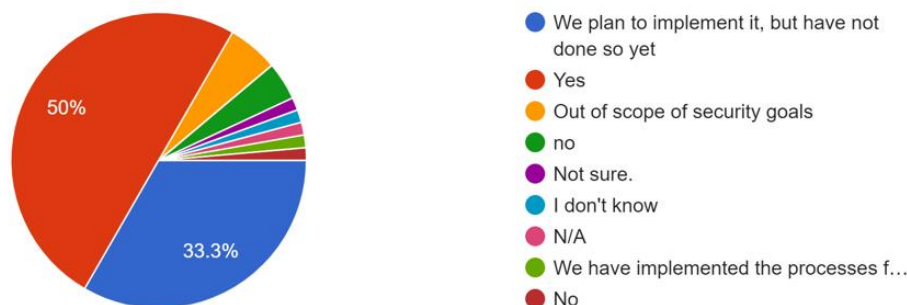


Figure 52: Responses to Q28.

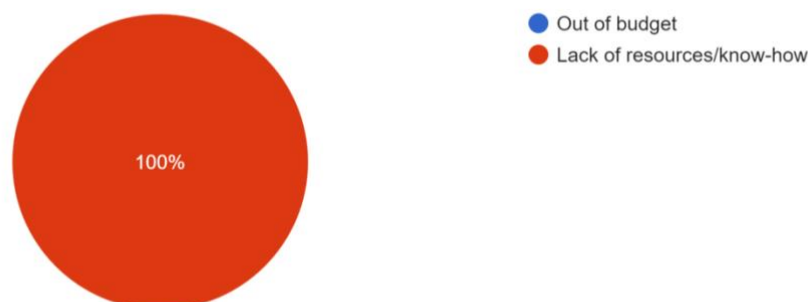


Figure 53: Responses if “Out-of-scope” is selected for Q28.

End-user Requirements Analysis

According to Figure 52, 50% of the respondents have implemented a Business Continuity Process (BCP), a critical framework for safeguarding organisational activities from disruptions. However, it's essential to recognize that a BCP is not just a checklist, but a comprehensive management process designed to identify potential threats and ensure resilience. Management plays a crucial role in assigning resources and conducting thorough planning and verifications to prepare the organisation for unforeseen events. Without such readiness, the organisation risks significant disruptions to essential activities or data losses. By prioritising BCPs and allocating resources accordingly, organizations can enhance their ability to withstand and recover from disruptions, ensuring the continuity of operations and safeguarding their long-term interests.

As shown in Figure 53, it is worth mentioning that the lack of resources and expertise holds that 100% of the responses that they consider BMC is out of the scope of their security goals, indicating that more business-oriented personnel maybe needed instead of technical experts.

Q29: Are your security-related policies and procedures readily available to your employees?

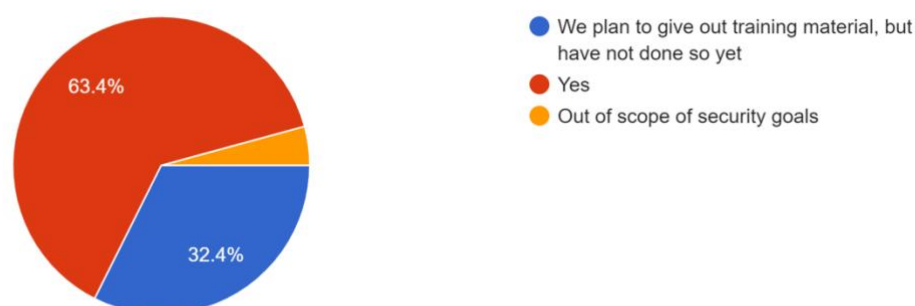


Figure 54: Responses for Q29.

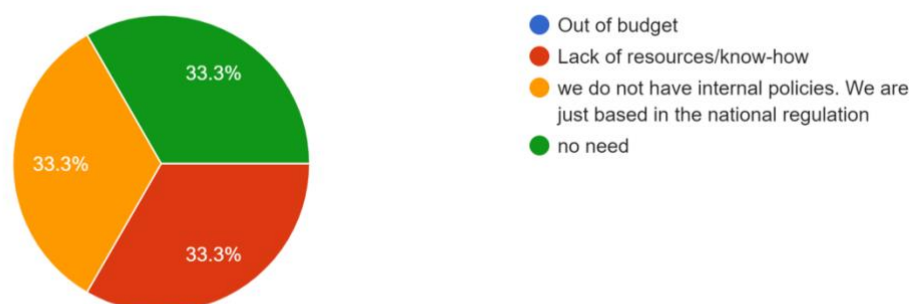


Figure 55: Responses if “Out-of-scope” is selected for Q29.

According to Figure 54, 63.4% confirm that their security-related policies and procedures are readily available to employees, reflecting a proactive approach to ensuring awareness and adherence to security protocols. Additionally, 32.4% plan to provide training material but haven't done so yet, indicating an intent to improve accessibility and understanding of security policies. However, for the remaining respondents, security policies are deemed out of scope for various reasons.

According to Figure 55, some cite national regulations as the basis for this decision (33.3%), suggesting that compliance with external requirements takes precedence over internal policies. Others mention a lack of resources and expertise (33.3%), highlighting potential challenges in implementing and communicating security measures effectively. Interestingly, a portion consider security policies

End-user Requirements Analysis

unnecessary (33.3%), although ensuring clarity and consistency in security practices is essential for mitigating risks and maintaining a secure environment.

Q: The proportion of respondents that continued to the technical-oriented questions.

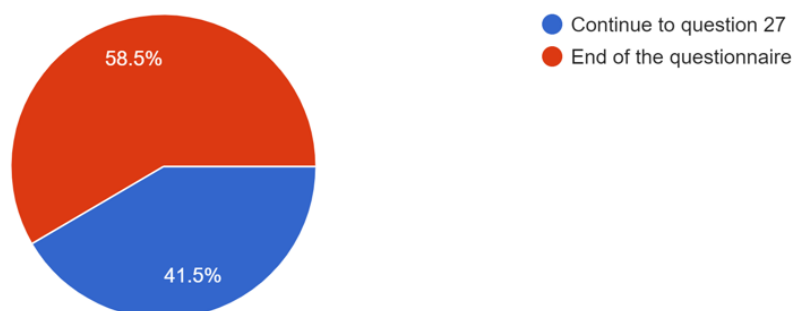


Figure 56: Percentage of Responders who answered Technical Questions.

According to Figure 56, 41.5% of the respondents continued to the technical-oriented questions of the questionnaire, while the remaining 58.5% ended the questionnaire.

Q30: Do you use/plan to use version control tools (e.g., Jira, Git) for source code maintenance?



Figure 57: Responses to Q30.

According to Figure 57, the significant majority of respondents, comprising 81.3%, have adopted version control systems, showcasing a commitment to efficient code management practices within their development workflows. These systems empower developers to manage changes to source code seamlessly, enabling them to track modifications and maintain a comprehensive history of alterations over time. By providing a centralised platform for collaboration, version control systems facilitate smooth teamwork among developers working on the same codebase, promoting transparency, accountability, and productivity. This adoption underscores a recognition of the importance of structured and organised code management processes, which are essential for ensuring code integrity, enhancing development efficiency, and fostering a culture of collaboration and innovation within development teams.

End-user Requirements Analysis

Q31: Do you use/plan to use continuous integration tools (e.g., Jenkins)?

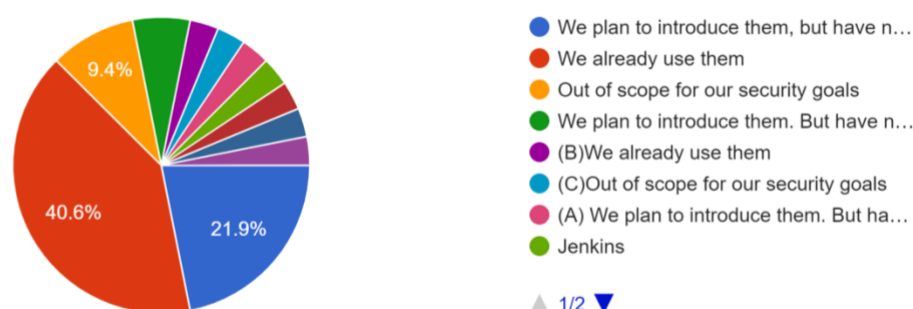


Figure 58: Responses to Q31.

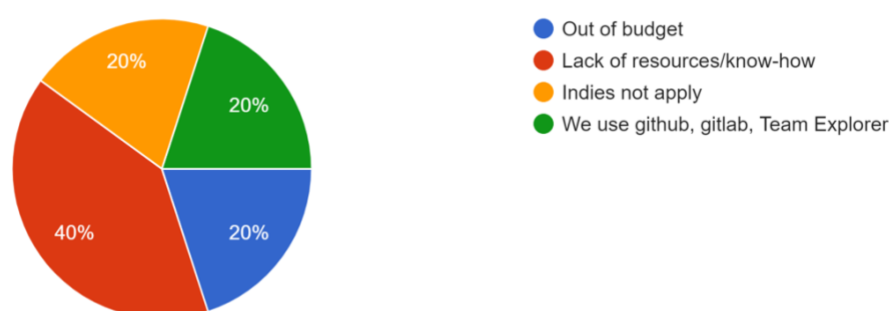


Figure 59: Responses if “Out-of-scope” is selected for Q31.

According to Figure 58, 40.6% of the responders are adopting Continuous Deployment/ Continuous Integration (CI/CD) practices and tools that can help them streamline their software development processes, improve efficiency, and deliver high-quality software more reliably and quickly, whereas the remaining 21.9% are planning to introduce CI/CD tools to ensure that code changes are integrated and tested automatically, reducing the risk of integration errors and ensuring consistent build environments across different development environments.

According to Figure 59, among the responders that answered that this aspect is out of the scope of their company’s security goals, 40% indicated a lack of resources and know-how, 20% out of budget, and 20% indicated the tools they use (GitHub, Gitlab, and Team Explorer).

End-user Requirements Analysis

Q32: Do you use/plan to use continuous testing tools (e.g., Selenium)?

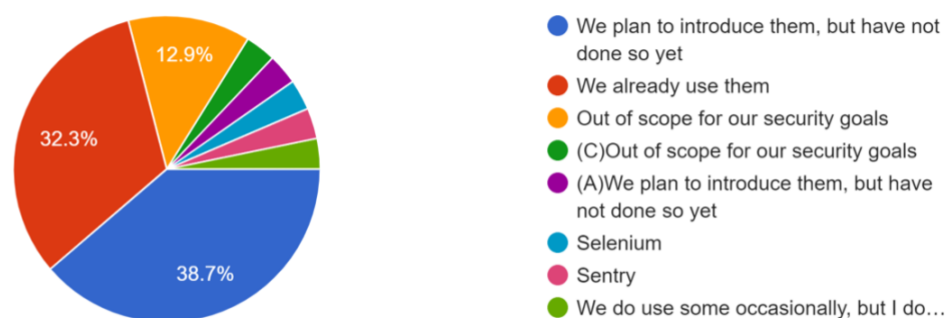


Figure 60: Responses for Q32.

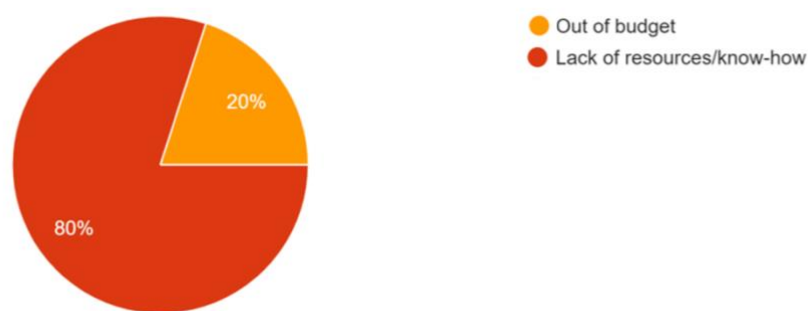


Figure 61: Responses if “Out-of-scope” is selected for Q32.

According Figure 60 out of the responders, only 32.3% use continuous testing tools, and another 38.7% plan to introduce them, whereas 12.9% consider the use of these tools as out of scope for their security goals. There is a lot of room to encourage the use of such tools that can be integrated seamlessly with CI pipelines, allowing automated tests to be triggered automatically whenever new code changes are made and ensuring that tests are executed consistently and continuously throughout the development process.

As shown in Figure 61 for those who answered out of scope, the main reason is lack of know-how and therefore there is a need to raise awareness.

End-user Requirements Analysis

Q33: Do you use/plan to use continuous monitoring tools (e.g., Nagios)?

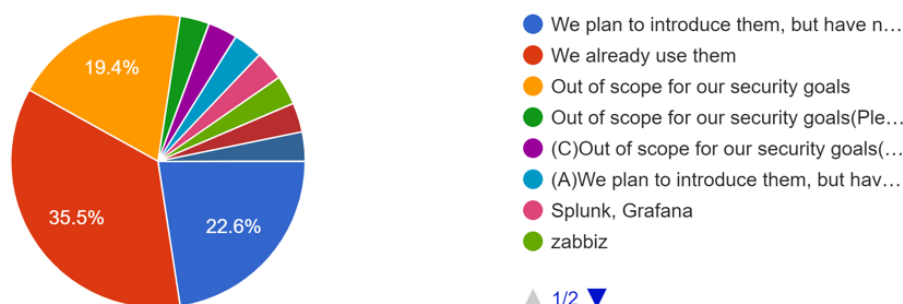


Figure 62: Responses to Q33.

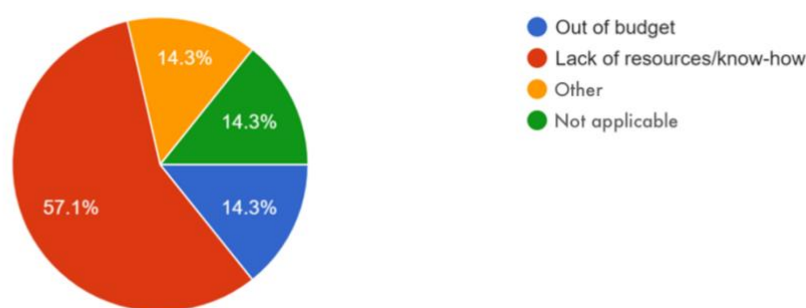


Figure 63: Responses if “Out-of-scope” is selected for Q33.

As shown in Figure 62, only 35.5% of the responders make use of continuous monitoring tools whereas another 22.6% are planning to introduce such tools. It is important to create awareness that the use of such tools allows proactive issue detection, improved reliability and availability, customisable alerting and notification, and compliance and reporting capabilities. Use of such tools helps maintaining the health, performance, and security of IT infrastructure and ensuring business continuity and operational efficiency.

As shown in Figure 63, lack of resources and know how are the main reasons for considering these tools to be out of scope, therefore developers should be aware and trained on the use of such tools.

End-user Requirements Analysis

Q34: Where do you host your apps, on-premises vs cloud?

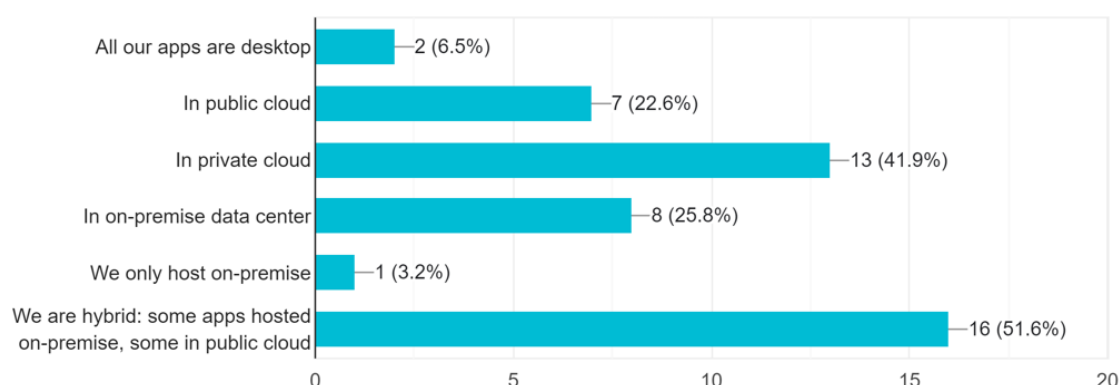


Figure 64: Responses to Q34.

As shown in Figure 64, most of the organisations choose to host their Apps on cloud, 22.6% in public cloud, 41.9% in private cloud, 25.8% in on premise data centres and only 3.2% host their apps only on premise. 51.6% are hybrid hosting some Apps on premise and some Apps in public cloud.

With an increased use of cloud services, organisations should become aware that they should enforce cloud security which is critical to protect data, comply with regulations, mitigate cybersecurity threats, ensure business continuity, manage risks effectively, maintain reputation and trust and securely leverage the benefits of cloud computing while safeguarding at the same time their assets and interests.

Q35: Regarding threat modelling, which approach would be most relevant to your organization?

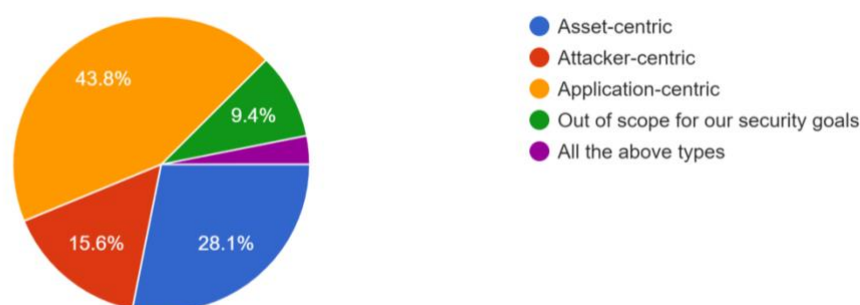


Figure 65: Responses to Q35.

End-user Requirements Analysis

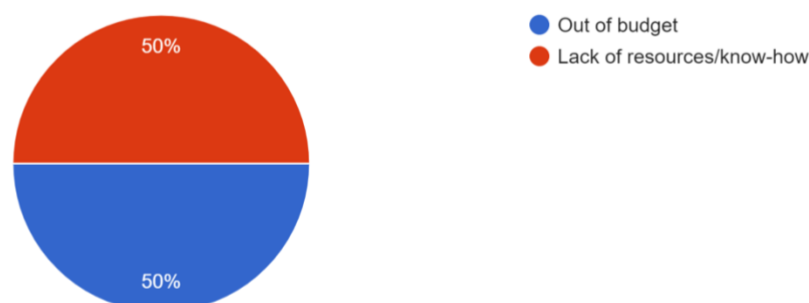


Figure 66: Responses if “Out-of-scope” is selected for Q35.

Regarding threat modelling, responders have identified application-centric threat modelling by 43.8%, 15.6% attacker centric, 28.1% asset-centric and 9.4% as out of scope, as shown in Figure 65. It is important to improve the knowledge and expertise of security teams in order to be in a better position to improve the security posture of systems and applications by systematically identifying and mitigating potential security risks.

As shown in Figure 66, lack of resources/know how and equally out of budget are the main reasons for considering threat modelling as out of scope. This equal split suggests that while threat modelling is recognised, both economic and educational barriers are significant in equal measure, affecting its implementation.

Q36: Are your software engineers trained in secure coding?

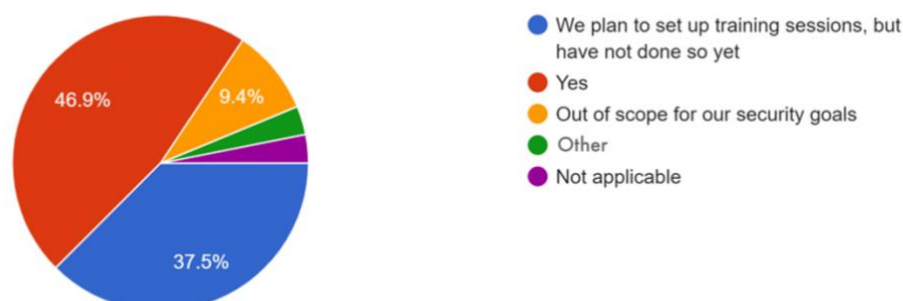


Figure 67: Responses to Q36.

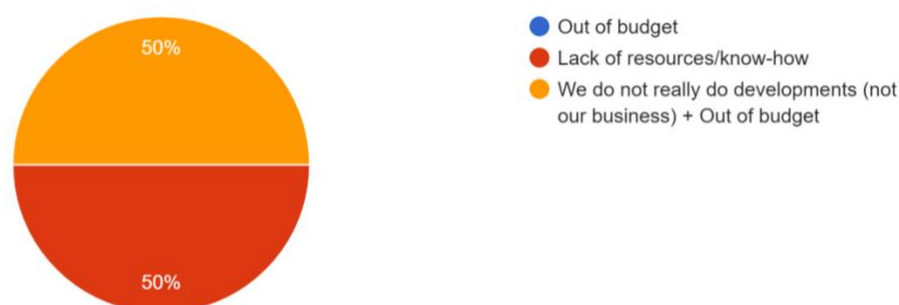


Figure 68: Responses if “Out-of-scope” is selected for Q36.

End-user Requirements Analysis

According to Figure 67, Software Engineers are trained in secure coding by 46.9% and 37.5% of the responders indicated that they are planning to set up training sessions on the same recognising the importance of it. NERO solutions can help organisations foster a culture of security awareness and collaboration, enabling teams to deliver secure, high-quality software more rapidly and responsively and align with the principles of DevSecOps.

Figure 68 depicts an even split for those who consider secure coding training for software engineers out of scope. Half of the respondents attribute their stance to being out of budget, indicating financial constraints prevent them from investing in such training. The other half combines two reasons: a lack of resources or know-how, and not engaging in development as it's not their core business. This reflects a balanced divide between financial limitations and organisational relevance as reasons for not pursuing secure coding education.

Q37: Do you use/plan to use pre-commit hooks to prevent secrets from entering your codebase?

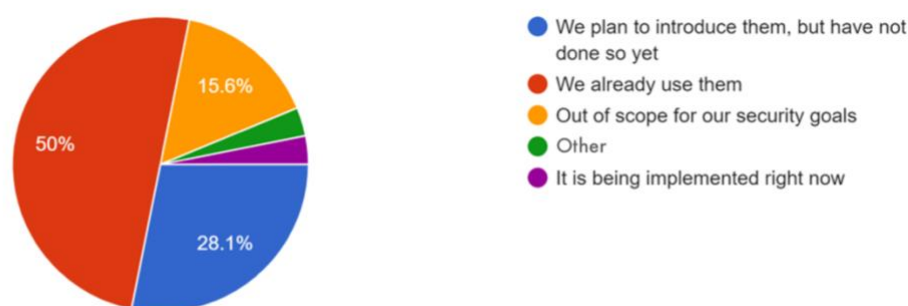


Figure 69: Responses to Q37.

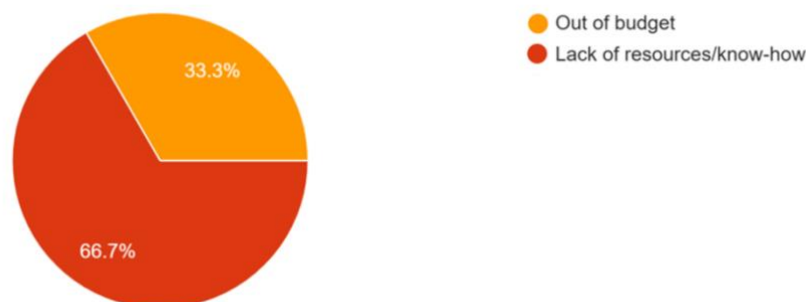


Figure 70: Responses if “Out-of-scope” is selected for Q37.

As shown in Figure 69, 50% of the responders indicated that they use pre-commit hooks to prevent secrets from entering their codebase and 28.1% are planning to introduce them and 3.1% are in the process of implementing it now. 15.6% have responded that this is out of scope of their security goals mainly due to lack of resources/know how. Developers should be encouraged to use these procedures as it is important to catch and address issues in their code before committing changes to the version control system. By incorporating pre-commit hooks into their development workflows, organisations can improve code quality, accelerate development cycles, and deliver more reliable and secure software solutions.

Figure 70 represents the answers of those who indicated that the answer was out of scope. A large portion, 66.7%, identified a lack of resources or know-how as their primary challenge, and the remaining 33.3% pointed to budget constraints as the limiting factor. This indicates that while two-thirds of the

End-user Requirements Analysis

respondents hindered by non-financial resources, including knowledge or technical capability., a third are restricted by financial issues.

Q38: Do you use/plan to use lint tools to inspect your code for errors?

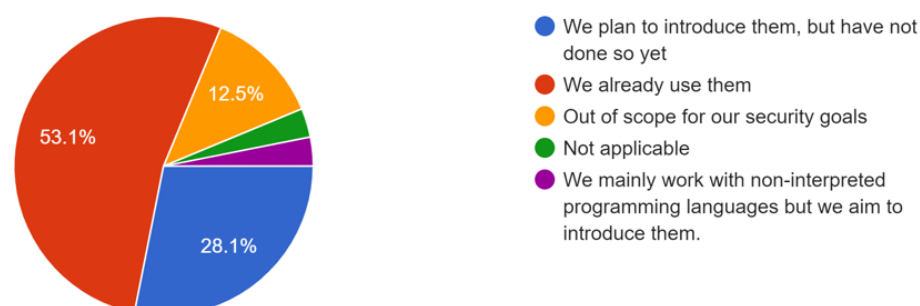


Figure 71: Responses to Q38.

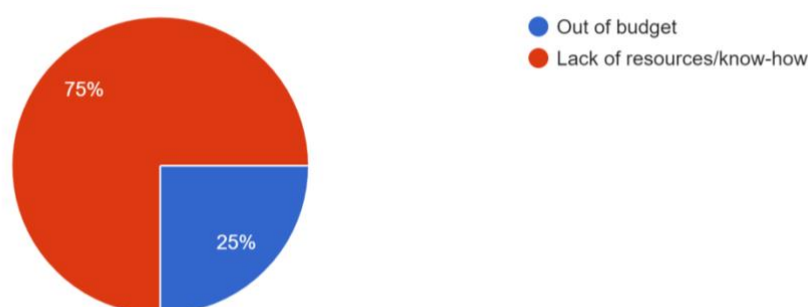


Figure 72: Responses if “Out-of-scope” is selected for Q38.

As shown in Figure 71, 53.1% of the developers use lint tools to inspect the code for errors and 28.1% are planning to introduce them. 12.5% consider the use of these tools as out of scope due to lack of resources/know how. By encouraging developers to integrate linting into their development workflows, organisations can ensure that their codebases are clean, maintainable, and consistent, ultimately leading to more reliable, secure and efficient software applications.

Figure 72 presents responses from the group for whom lint tools are considered out of scope. A significant majority, 75%, the lack of resources/known-how as the reason for not using lint tools to check their code for errors. The remaining 25% points to out of budget. This distribution suggests that while some are aware of linting benefits, the primary barrier to its implementation is the lack of knowledge of the finances.

End-user Requirements Analysis

Q39: Do you use/plan to use Static Code Analysis (e.g., SonarQube) tools to inspect yours for security flaws?

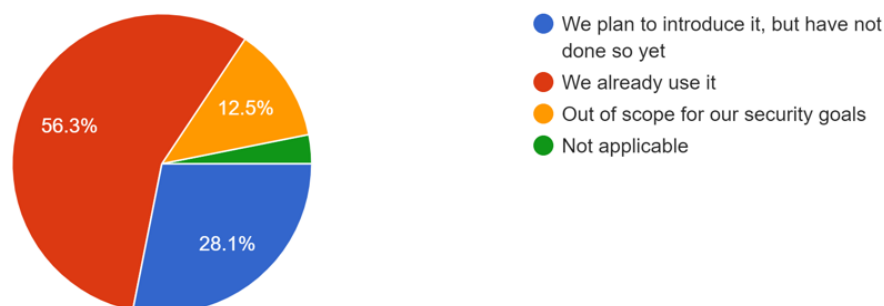


Figure 73: Responses to Q39.

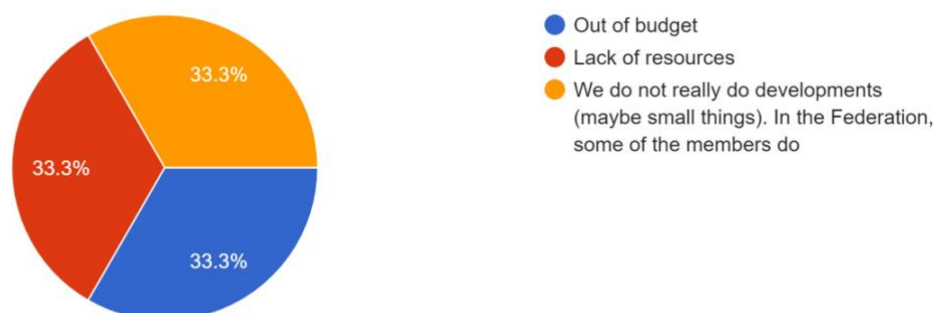


Figure 74: Responses if “Out-of-scope” is selected for Q39.

As shown in Figure 73, 56.3% of the responders are already using Static Code Analysis tools to inspect the code for security flaws and 28.1% are planning to introduce the use of it. 12.5% consider the use of Static code analysis as out of scope due to lack of resources/know-how. By encouraging developers to use Static Code Analysis to inspect the code for security flaws they improve code quality, detect issues early, enforce coding standards, identify performance bottlenecks, detect security vulnerabilities, integrate with development workflows, automate code review, and facilitate continuous improvement.

As shown in Figure 74 one-third attribute this to being out of budget, another third to a lack of resources, and the final third to not engaging significantly in development work within their federation, with only some members doing so. This even split highlights diverse challenges that are equally impactful, suggesting that addressing the scope of tool use in security requires multifaceted solutions that consider financial, resource, and organizational activity levels.

End-user Requirements Analysis

Q40: Do you use/plan to use Dynamic Code Analysis (e.g., Burp Suite) to detect flaws in your applications?

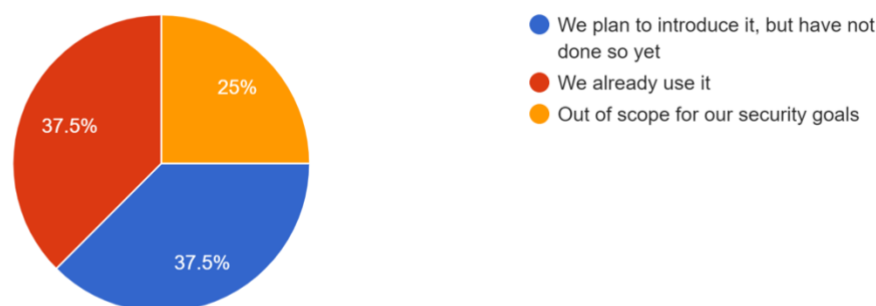


Figure 75: Responses to Q40.

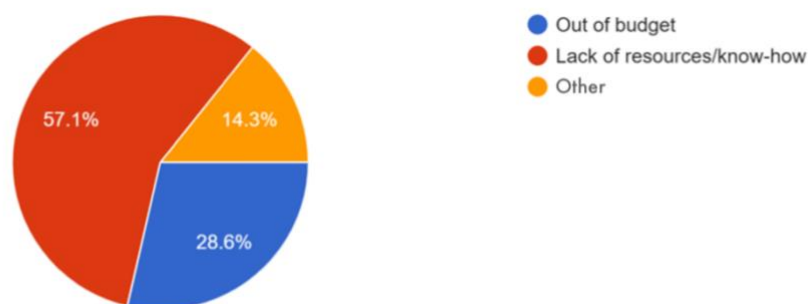


Figure 76: Responses if “Out-of-scope” is selected for Q40.

As shown in Figure 75, 37.5% of the responders are using Dynamic Code Analysis whereas an equal % is planning to use it. 25% of the responders consider this as out of scope mainly due to lack of resources/know-how 57.1% whereas 28.6% indicated budget constraints and the remaining % for other reasons. Developers should be encouraged to use Dynamic Code Analysis to detect flaws in their applications and identify runtime errors, memory leaks, performance bottlenecks, security vulnerabilities, and other issues that may affect the behaviour, performance, and security during execution. By incorporating dynamic analysis into their development and testing workflows, developers can ensure the reliability, scalability, and security of their software products.

As shown in Figure 76, the chart reflects resources and know-how constraints as the main impediment, with 57.1% citing this as a barrier and the further 28.6% are hindered out of budget, suggesting a need for education on such tools' utility and potential cost-effective solutions. This data underscores financial and informational gaps that may be obstructing the adoption of vital application security measures.

End-user Requirements Analysis

Q41: Do you use/plan to use Interactive Application Security Testing (e.g., HCL AppScan) to test your applications?

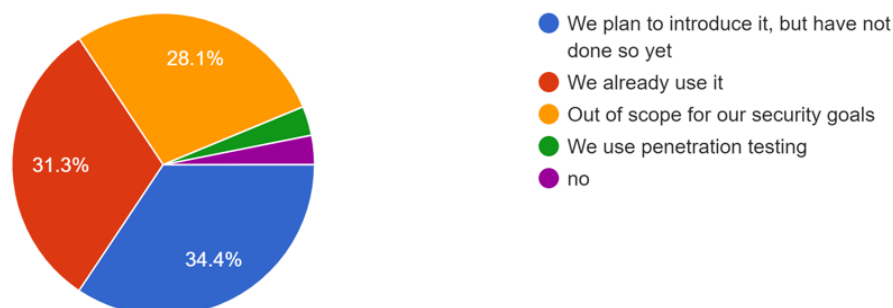


Figure 77: Responses to Q41.

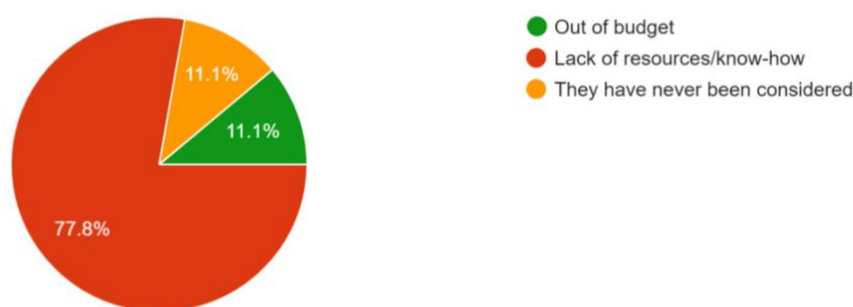


Figure 78: Responses if “Out-of-scope” is selected for Q41.

As shown in Figure 77, out of the responders, 31.3% indicated that they use Interactive Application Security Testing (IAST) to test their application and another 34.4% plan to use it. 28.1% consider this testing to be out of scope for their security goals. It is important that developers understand that Interactive Application Testing Scan can help organisations identify, remediate, and manage security vulnerabilities throughout the software development lifecycle. By integrating security testing into their development processes and leveraging the advanced capabilities of such tools, organisations can improve the security posture of their applications, protect sensitive data, and mitigate the risk of security breaches and compliance violations.

According to Figure 78, out of these who have indicated that IAST is out of scope for their security goals, the majority (77.8%) indicates lack of resources/know-how and 11.1% never considered using it. The remaining 11.1% indicated that they have budget constraints.

End-user Requirements Analysis

Q42: Do you use/plan to use Component Analysis (e.g., Hakiri) to detect vulnerable components in your codebase?

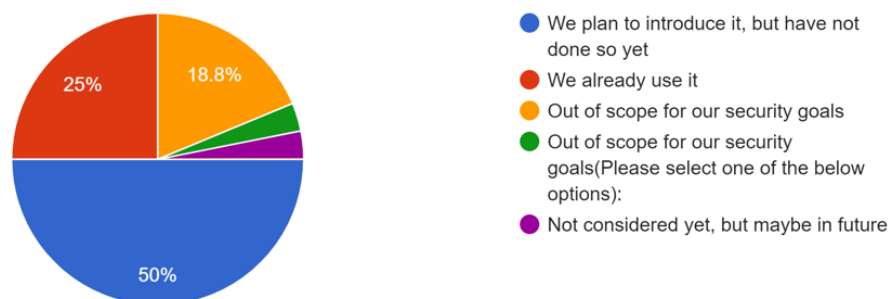


Figure 79: Responses to Q42.

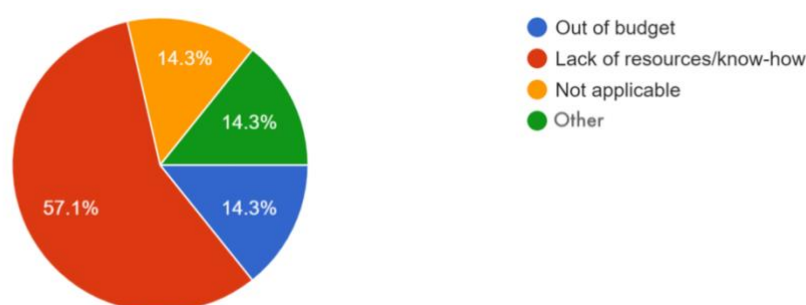


Figure 80: Responses if “Out-of-scope” is selected for Q42.

As shown in Figure 79, 50% of the responders are planning to use Component Analysis to detect vulnerable components in the codebase and 25% is already using it. 18.8% consider this to be out of scope for their security goals. Developers should be encouraged more to use component analysis tools like Hakiri to manage dependencies, identify and address security vulnerabilities, ensure compliance with industry standards, and reduce technical debt in their applications. By incorporating automated dependency analysis and management into their development workflows, developers can enhance the security, stability, and maintainability of their software projects.

Figure 80 indicates that among those who find Component Analysis tools out of scope for their operations, the majority, at 57.1%, point lack of resources and know-how as the primary reason. An equal fraction of 14.3% budget constraints, or they deem such tools not applicable to their workflows. This data suggests that since know-how and lack of resources are the main hurdles to adopting Component Analysis, a non-trivial segment may require further education on the applicability and benefits of such security practices.

End-user Requirements Analysis

Q43: Do you use/plan to use Infrastructure Vulnerability Scanning (e.g., Nessus) to detect vulnerable components in your codebase?

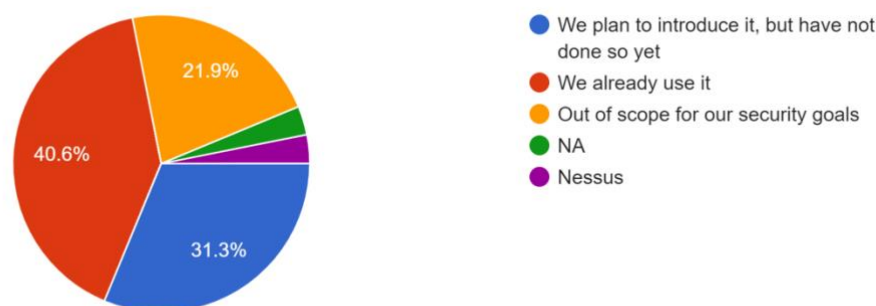


Figure 81: Responses to Q43.

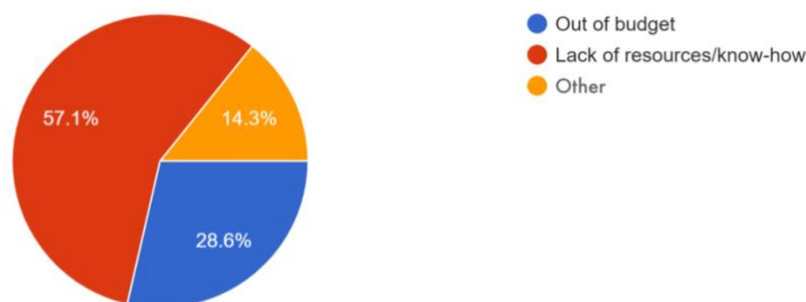


Figure 82: Responses if “Out-of-scope” is selected for Q43.

As shown in Figure 81, 40.6% are using Vulnerability Scanning to detect vulnerable components in the codebase and 31.3% are planning to introduce it. 21.9% of the responders consider infrastructure vulnerability scanning to be out of scope for their security goals.

According Figure 82, 57.1% are indicating lack of resources/know-how and 28.6% indicate insufficient budget and another 14.3% have not specified any particular reasons. It is important to raise awareness and stress the importance of using such tools to identify security weaknesses and mitigate risks and provide organisations with continuous visibility into their security posture, allowing them to monitor for new vulnerabilities and emerging threats over time.

Q44: Do you use/plan to use Container Vulnerability Scanning (e. g., Anchore) to detect insecure containers?

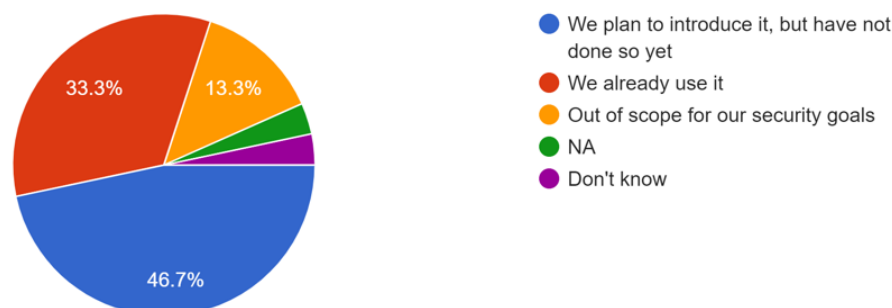


Figure 83: Responses to Q44.

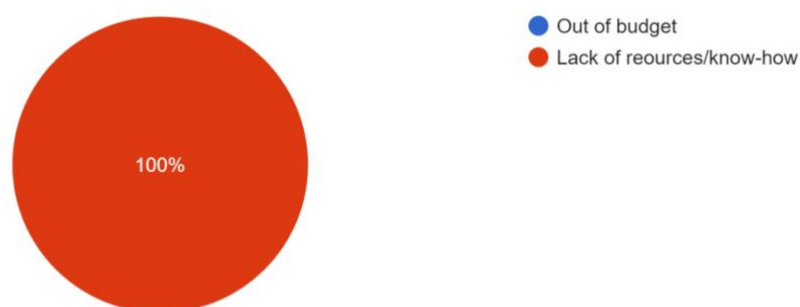


Figure 84: Responses if “Out-of-scope” is selected for Q44.

As shown in Figure 83, 33.3% indicate that they use container Vulnerability Scanning to detect insecure containers, 46.7% are planning to use such tools and 13.3% indicate that the use of such tools is out of scope for their security goals.

According to Figure 84, 100% of the responders who indicate that this is out of scope of their security goals have mentioned that there is a lack of resources/know-how. It is important to raise awareness and stress the importance of using such tools to identify insecure containers, mitigate risks and provide organizations with continuous visibility into their security posture, allowing them to monitor for new vulnerabilities and emerging threats over time.

Q45: Do you use/plan to use automated measures to ensure data privacy in your applications?

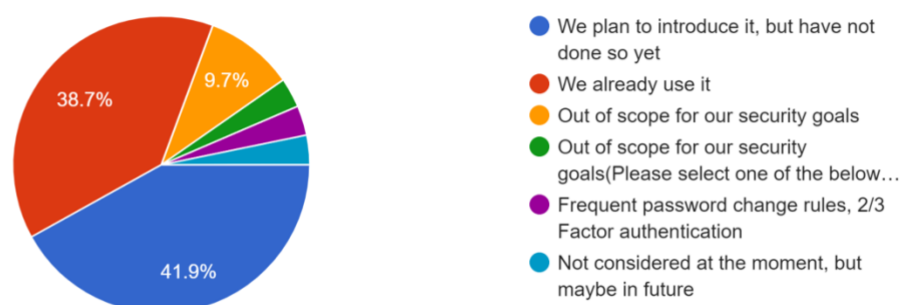


Figure 85: Responses to Q45.

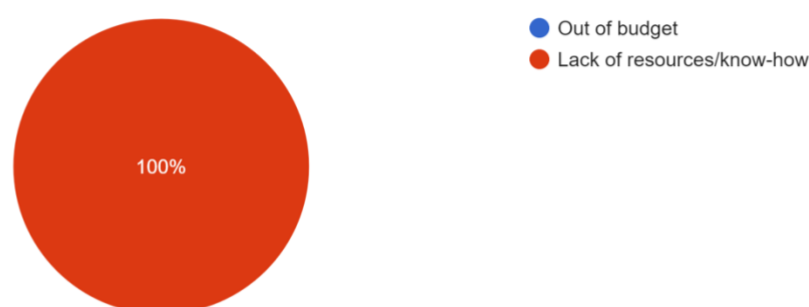


Figure 86: Responses if “Out-of-scope” is selected for Q45.

As shown in Figure 85, 38.7% of the responders indicated that they already use automated measures to ensure data privacy and 41.9% plan to use automated measures. 9.7% indicate that this out of their security goals. It is important to raise awareness and stress the importance of using automated measures to ensure data privacy and to effectively manage data privacy risks, comply with regulations, and protect sensitive information from unauthorized access or disclosure.

According to Figure 86, 100% of the responders have indicated lack of know. It is important to raise awareness that automated measures can efficiently help to handle large volumes of data, making it easier to enforce data privacy policies across an organisation's entire data ecosystem and by continuously monitoring data access, usage, and sharing activities helps identifying potential privacy violations in real-time and taking appropriate actions to mitigate risks.

3.2.3 Questionnaire Responses Analysis Summary

Based on the collected questionnaires and the corresponding responses, some key insights are summarised below, aiming at evaluating the cybersecurity awareness level and posture within the participating SMEs.

It is evident that most SMEs apply measures to protect their organization from cybersecurity risks, which include access control, authentication, use of strong password, and backing up data. However, less attention is given to protecting the organisation in a holistic approach, since database encryption and automated measures for ensuring data privacy were not so popular. Moreover, cybersecurity training of employees was adopted among the half of the participants. This result highlights the importance of giving greater emphasis on cybersecurity training and raising awareness.

End-user Requirements Analysis

In terms of participants' comprehension of contemporary cybersecurity threats, there's room for enhancement, given that approximately 40% of SMEs involved conduct risk assessments for third-party vendors. Moreover, almost the half of the SME's test their intranet network for vulnerabilities, implying that a significant portion of the participants are not identifying and recording potential threats and vulnerabilities. Even SME's operating within the IT sector neglect to scan their codebase for vulnerabilities.

Concerning the ability of participating organisations in finding and analysing potential cybersecurity attacks, slightly over half of the participants consistently monitor their devices. Therefore, enhancing the ability of SME's to continuously monitor their assets and promptly detect potential attacks is crucial. IDS should become widely adopted by SMEs.

Regarding the incident response plan on cyber attacks, the results of the questionnaire indicated that the majority of SMEs overlook this aspect. Although more than the half of the participants clarified that the employees are being informed for cybersecurity incidents, only about one-third of SMEs have corresponding strategies in place to respond to such attacks. Moreover, only a minor portion of the SMES, approximately the 20%, have dedicated teams that are responsible to manage such incidents. Finally, a satisfactory percentage of the participants, about 70%, claimed that they employ data recovery plans.

3.3 NERO Stakeholders

To successfully identify the NERO services and their characteristics, the project had at first to try to identify its different user-types and characters. This endeavour involved a comprehensive approach encompassing the following steps: a) Initially, an exercise to understand the various user needs, experiences, behaviours and goals, recognising that different people have different needs and expectations, was conducted. Our stakeholders span across the following categories:

- SMEs within the financial, transport, medical/health sectors each representing a distinct use case
- Any other SME type not falling in the aforementioned categories
- EU Security organisations e.g., ENISA
- Country specific Security organisation e.g., DSA/National CSIRT

Therefore, within NERO, we identify the following different main user category types, that will be detailed and updated as the project progresses:

- The **Customer**, who represents the end-users of NERO and generally users of the NERO platform – product - and requests access to the NERO set of features and services,
- The **NERO administrator**, who represents one or more users that administer the NERO platform and guarantee the proper operation of its services,
- The **Vendor / Supplier**, since NERO will also be provided as a set of cloud services and tools.

Focusing on the Customer side, we can recognize the following different roles:

- The **Software Engineer**, who is key role that makes full use of the DevOps/DevSecOps pipelines and actually develops the tested software product/service.
- The **Quality Assurance Professional**, who is responsible for thoroughly testing the deployed software so as to identify, categorise, and report in detail possible bugs, security flaws and other functionality and design issues.
- The **Security Analyst**, who, most of the time plays a vital role in keeping an organisation's proprietary and sensitive information secure. Usually, he/she is responsible to identify and

End-user Requirements Analysis

correct flaws in the organization's security systems, solutions, and programs while recommending specific measures that can improve its overall security posture.

- The **Security Professional and Expert**, who searches for vulnerabilities across the organisation's systems, inspects for any attacks and intrusions, recognises potential threats, and designs various strategies and defensive systems against intruders.
- The **Manager and/or Administrator**, who manages things in the IT department, develops the strategy for how to run the department, designs the best policies, and gives direction to the department.

By delineating these multifaceted user categories and their respective roles, NERO is poised to cater to a diverse spectrum of user needs while upholding the highest standards of functionality, security, and user experience.

3.4 End-user Interviews Methodological Framework

Interviews/Surveys will be conducted with scientific partners and end-users of the use cases, in order to understand the expectations and needs of the people who will use the tools and it is essential to communicate with them directly to collect inputs. This step involves conducting interviews or surveys with end-users and key stakeholders to gather information about their preferences, concerns, and any specific requirements they may have and identify any gaps related to cybersecurity.

The following methodological framework for conducting end-user interviews will be followed in order to conduct effective end-user interviews that provide valuable insights to inform decision-making and enhance the user experience of products or services:

1. **Define Objectives.** Clearly articulate the goals and objectives of the interviews. What specific information you are seeking to gather from end-users.
2. **Identify Participants.** Determine the target audience for the interviews based on the characteristics of the end-users you want to understand. Consider demographics, roles, expertise, and other relevant factors.
3. **Develop Interview Protocol.** Create a structured interview protocol that outlines the topics, questions, and prompts to be covered during the interviews. Ensure that questions are open-ended to encourage detailed responses.
4. **Plan Logistics.** Decide on the logistics of the interviews, including the location (in-person or remote), duration, and scheduling. Make arrangements to ensure a comfortable and conducive environment for the interviews.
5. **Recruit Participants.** Identify and recruit participants who match the target audience criteria. Use various recruitment methods such as email invitations, social media, or professional networks.
6. **Gain Informed Consent.** Prior to the interviews, obtain informed consent from participants, explaining the purpose of the interviews, how the data will be used, and any confidentiality measures in place.
7. **Conduct Interviews.** Conduct the interviews according to the structured protocol. Start by building rapport with participants and then gradually delve into the topics outlined in the protocol. Encourage participants to share their experiences, perspectives, and insights freely.

End-user Requirements Analysis

8. **Active Listening and Probing.** Practice active listening during the interviews, paying attention to both verbal and non-verbal cues. Ask probing questions to clarify responses, explore specific areas in more detail, or uncover underlying motivations.
9. **Record Data.** Record the interviews using audio or video recording equipment, with participants' consent. Take detailed notes during the interviews to capture key points, quotes, and observations.
10. **Transcribe and Analyse Data.** Transcribe the interview recordings and organise the data for analysis. Use qualitative analysis techniques such as thematic analysis, coding, and categorisation to identify patterns, themes, and insights across interviews.
11. **Extract Key Findings.** Extract key findings from the data analysis, highlighting common themes, trends, and variations in end-users' perspectives. Use direct quotes and examples to illustrate key points.
12. **Report Results.** Prepare a comprehensive report summarising the findings from the interviews. Include actionable recommendations for product development, design improvements, or other relevant areas based on the insights gained.
13. **Iterate and Follow-Up.** Use the findings to iterate on product or service development processes. Consider conducting follow-up interviews or surveys to gather additional insights or validate findings as needed.

By following these discrete steps and taking into consideration the findings of the literature review and responses of the questionnaire, the interviews have the potential to reveal important both functional and non-functional requirements, aiming to better define the overall NERO ecosystem and construct the demonstrations in order to validate NERO as a solution for enhancing cybersecurity awareness for SMEs.

3.5 Initial List of Requirements

Driven by the analysis in Section 2, regarding the SMEs cybersecurity landscape and common threats, and the responses, along with the insights derived from the questionnaire, the current subsection aims to provide a set of initial requirements that are aligned with the abovementioned aspects and will serve as the basis for designing the NERO ecosystem. This will, then, serve as the input to clearly define, prioritize, and categorise the NERO system requirements in D2.2.

Both the analysis on the SMEs cybersecurity landscape and recommendations, as well as the feedback from the questionnaire, converged into some common indicators, regarding the security gaps of SMEs, aspects that they are aware of or neglect, and potential best practices to enhance their cybersecurity posture. It is evident that certain measures should definitely be employed to facilitate the creation of a cybersecurity culture within SMEs, while the requirements that NERO ecosystem will rely on, should be aligned with the considered strategies. Specifically, practices such as vulnerability discovery, securing endpoints, identifying the SMEs' assets, detecting potential intrusions and anomalies within the network, are essential for enabling SMEs to identify the current cybersecurity risks, protect their systems, and detect potential abnormal incidents. Moreover, strategies for managing and responding to such incidents should be in place. In addition to this, it is imperative to ensure that SMEs' employees receive the appropriate cybersecurity training, even if their role does not lie in the security domain. Employees should undergo consistent training sessions to be equipped with the ability to identify and address various cybersecurity threats. These training programs should be customised to fit the needs of SMEs. Additionally, specialized training should be delivered for individuals that are tasked with cybersecurity roles within their organisation. The considered training should foster a culture of cybersecurity awareness within SMEs, towards safeguarding assets, maintain customer trust, and mitigate detrimental financial and reputational consequences due to cyber incidents.

End-user Requirements Analysis

Finally, it's important to ensure that SMEs can easily access cybersecurity services, while minimising any barriers that they may encounter when seeking these resources. Additionally, users should understand the purpose and functionalities of these services, promoting their seamless utilisation, with the corresponding guidelines. To this end, these cybersecurity services should fall under a consolidated platform, enabling SMEs to access a wide range of security tools according to their requirements and eliminating the need of resorting to multiple third-party vendors. The latter, constitutes a major barrier for SMEs, as it seems challenging to be aligned with various heterogeneous solutions. Finally, it is crucial to provide cybersecurity services given any financial constraints, as affordability is a critical factor that affects the decisions of SMEs, in terms of embracing such services.

Taking the above into consideration, Table 2 summarizes the initial user requirements upon that NERO ecosystem will be constructed.

Table 2 : List of requirements.

Requirement ID	Requirement Title	Description
R01	Vulnerability detection	Identify and suggest mitigation action for the vulnerabilities existing in the source code of software.
R02	Endpoint protection	Implement security measures to safeguard endpoints, such as computers, laptops, smartphones, and tablets, from cyber threats.
R03	Intrusion detection	Identify potential threats and anomalies in the network infrastructure.
R04	Network monitoring	Monitor the internal network and identify potential malicious activities inside the network.
R05	Asset identification	Inventories of hardware, software, services, and systems that are managed by the organisation are recorded and maintained.
R06	Confidentiality	Organisation's data must be protected and be accessed only by privileged users.
R07	Incident response	In case of a cybersecurity incident, a plan should be in place to respond timely, mitigate their impact, and restore normal operation.
R08	Cybersecurity training and awareness	Provide cybersecurity training to the company's employees based on their expertise levels. Personnel should receive awareness to equip them with the necessary skills and knowledge to carry out everyday tasks while considering cybersecurity risks.
R09	Easy access to cybersecurity services	Interested users should easily access the provided cybersecurity services and understand their purpose and functionalities.

End-user Requirements Analysis

R10	Unified cybersecurity platform	All cybersecurity services should be centralised under a common platform, allowing users to choose the most suitable tool for their needs and objectives.
R11	Flexible Cybersecurity Solutions	The cybersecurity solutions should be flexible and easily adaptable to the requirements of the end-user.
R12	Affordable cybersecurity solutions	Cybersecurity products and services should be affordable for end-users, considering that they operate within SMEs. Also, the provision of open-source solutions could be considered.
R13	Usability	The user interface of the cybersecurity platform should be intuitive and user-friendly, enabling users to easily navigate through the provided features and functionalities.

4 NERO Ecosystem

4.1 High-Level Architecture Description

The depth and intricacy of NERO's architectural blueprint is shown in Figure 87, defining an ecosystem characterised by five distinct frameworks: ARCANA, VICTORIOUS, AUDACIOUS, CYBIT, and ASTRAS. Each framework assumes a unique role within the architecture, thereby enriching the overall functionality of the ecosystem.

In this section, we aim to provide an overview of NERO's ecosystem, shedding light on the pivotal roles of the various frameworks planned for development in the project. Furthermore, we will initiate a preliminary discussion on the inter-framework communication, laying the groundwork for a more comprehensive discussion to be expounded upon in D2.2.

This initial exploration serves as a precursor to dive deeper into the intricate interplay between the frameworks, enlighten how they synergistically collaborate to propel NERO towards its objectives. Through meticulous examination and analysis, we endeavour to unravel the intricate tapestry of NERO's ecosystem, paving the way for enhanced understanding and strategic decision-making in the project's trajectory.

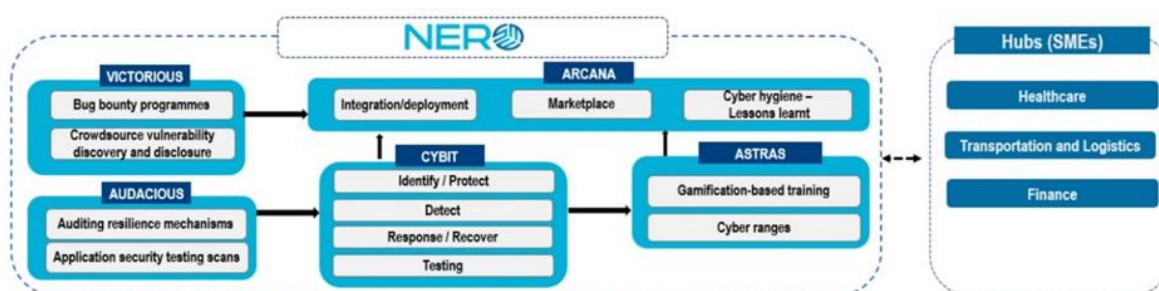


Figure 87: NERO high-level ecosystem

4.1.1 Market Oriented Cybersecurity Awareness Training (ARCANA)

The ARCANA framework serves as the primary interface within the ecosystem, housing NERO's marketplace. This marketplace serves as a centralised hub for all cybersecurity tools and training materials. The integration and deployment of cybersecurity tools within such a marketplace are pivotal for cultivating cyber hygiene practices among SMEs. NERO is committed to seamlessly integrating its cybersecurity tools into the NERO marketplace platform, accompanied by comprehensive training sessions for SMEs on their usage and benefits.

Furthermore, extensive technical assistance will be provided to SMEs following the deployment of these tools. Continuous monitoring and analysis of tool effectiveness will be conducted to pinpoint areas for improvement. The promotion of cybersecurity tool availability within the marketplace will be facilitated through well-orchestrated awareness campaigns and workshops designed to educate SMEs on cyber hygiene practices.

Additionally, collaborative endeavours with cybersecurity experts will amplify the dissemination of best practices in this field. Such collaborative efforts are essential for fostering a robust cybersecurity

NERO Ecosystem

ecosystem and ensuring SMEs are equipped with the knowledge and tools necessary to safeguard their digital assets effectively.

4.1.2 Vulnerability Discovery TO Secure ICT Solutions (VICTORIOUS)

The VICTORIOUS framework will house the Bug Bounty Programs and Crowdsourced Vulnerability Discovery and Disclosure (CSVDD) initiatives, which are strategies aimed at enhancing software security by incentivising the detection and reporting of vulnerabilities in software. Their primary objective is to pinpoint and rectify potential security flaws before they can be exploited by malicious actors. Through NERO's Bug Bounty Programs, rewards will be provided to security researchers for identifying and reporting vulnerabilities, thus aiding companies in efficiently and economically addressing security issues.

CSVDD guidelines establish a structured framework for the responsible identification, reporting, and management of security vulnerabilities. These guidelines enable organisations to consistently and reliably receive and respond to security reports from the public. Leveraging bug bounty programs and CSVDD, NERO aims to reap several benefits, including reduced risks of security breaches, enhanced security for users and customers, and the proactive identification and resolution of security issues.

NERO is prepared to address the challenges associated with these initiatives, such as the risk of false positive 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 recognition of security researchers. NERO's Bug Bounty Programs and CSVDD implementation offer an effective means of bolstering software security, ensuring maximal benefits while minimising potential risks.

4.1.3 Audit-Based Certification For Cybersecurity Preparedness (AUDACIOUS)

The AUDACIOUS framework assumes responsibility for auditing resilience mechanisms and conducting application security testing scans, both of which are indispensable for safeguarding an organisation's digital assets. Within NERO, these activities will be meticulously executed to assess and fortify security controls, identifying any vulnerabilities or deficiencies. Auditing resilience mechanisms seeks to verify the effectiveness of systems and processes in detecting, responding to, and recovering from potential security threats. Conversely, application security testing scans focus on uncovering vulnerabilities inherent in software application code, encompassing concerns such as cross-site scripting and SQL injection.

NERO will systematically undertake 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, complemented by regular employee training sessions emphasising the criticality of application security. This holistic approach ensures that NERO remains proactive in fortifying its security posture, thereby safeguarding its digital infrastructure against potential threats.

4.1.4 Cyber Immunity Toolkit Repository (CYBIT)

The CYBIT framework takes on the crucial role of testing, detecting, identifying, protecting, responding, and recovering using a plethora of tools provided by NERO's partners. Cybersecurity encompasses the vital task of safeguarding information systems, networks, and data from unauthorised access, theft, and

NERO Ecosystem

harm. Within this realm, the processes of identification, protection, detection, response, recovery, and testing of cybersecurity tools stand as pivotal pillars of a robust cybersecurity program.

NERO initiates its cybersecurity defence strategy by meticulously identifying potential vulnerabilities, which may stem from outdated software, weak passwords, or unsecured networks. Subsequently, protective measures, such as firewalls and encryption, are implemented to thwart unauthorised access attempts. Detection tools, including IDS, are leveraged by NERO to vigilantly monitor network activity and swiftly identify potential threats.

In the unfortunate event of a security breach, NERO adopts a proactive stance, swiftly responding to minimise damage and avert further losses. Furthermore, comprehensive testing and validation of cybersecurity tools and processes are conducted to ensure their efficacy. This involves rigorous penetration testing, vulnerability scans, and various security assessments to pinpoint and rectify any weaknesses in the cybersecurity posture.

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

4.1.5 Innovative Cybersecurity Awareness Training Mechanisms (ASTRAS)

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

Cybersecurity gamification-based training and cyber ranges represent cutting-edge methodologies designed to bolster the capabilities and knowledge of both individuals and organisations in combating cyber threats. Within NERO, gamification-based training adopts immersive game-like scenarios and simulations to impart foundational knowledge in cyber defence while refining users' decision-making prowess in identifying and responding to cyber attacks.

On the other hand, NERO's cyber ranges offer a dynamic simulated environment tailored for testing and honing defensive strategies against simulated cyber attacks. This enables organisations to assess and fortify their response mechanisms effectively. Both approaches, whether through gamification or cyber ranges, excel in engaging users, 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 fortifying organisations' overall resilience against cyber threats. By leveraging these innovative training methodologies, NERO aims to empower individuals and organisations with the requisite skills and knowledge to navigate the complex landscape of cybersecurity effectively.

4.1.6 Tools and Frameworks Communications Methodology

4.1.6.1 CYBIT – ASTRAS communication

The inter-framework communication within the NERO ecosystem plays a pivotal role in ensuring robust cybersecurity management. The CYBIT framework, entrusted with testing and detection duties, collaborates closely with ASTRAS, which specialises in updating training materials and staying abreast

of current cybersecurity threats. This symbiotic relationship enables seamless coordination between proactive testing insights and targeted training initiatives. CYBIT's real-time assessments offer invaluable insights into emerging vulnerabilities and potential attack vectors, empowering organisations with a proactive risk management approach. By sharing this critical information with ASTRAS, organisations gain access to timely and relevant training resources tailored to address the latest cybersecurity challenges effectively. Moreover, this collaboration fosters a culture of continuous learning and improvement, encouraging proactive engagement with cybersecurity best practices across the board. As CYBIT and ASTRAS work hand in hand, they not only bolster organisations' resilience against cyber threats but also equip them to navigate the evolving digital landscape with confidence. Through ongoing communication and collaboration, CYBIT and ASTRAS contribute significantly to the adaptability and effectiveness of the NERO ecosystem in safeguarding vital assets and data against cyber threats.

4.1.6.2 CYBIT – ARCANA communication

The communication between CYBIT and ARCANA within the NERO ecosystem serves a fundamental purpose in ensuring comprehensive cybersecurity management. CYBIT, responsible for testing and detection, generates crucial insights into emerging vulnerabilities and potential cyber threats. By communicating these findings to ARCANA, which serves as the central hub for the ecosystem and houses the marketplace for cybersecurity tools and resources, organisations gain immediate access to actionable information. This enables ARCANA to disseminate relevant updates, alerts, and recommendations to users, ensuring they are equipped to address identified vulnerabilities effectively. Additionally, ARCANA can provide CYBIT with valuable feedback from users, such as their experiences with deployed tools or areas where additional support is needed. This feedback loop facilitates continuous improvement and refinement of cybersecurity strategies and toolsets, ultimately enhancing the overall resilience of organisations against cyber threats. Through ongoing communication and collaboration, CYBIT and ARCANA contribute significantly to the efficacy and adaptability of the NERO ecosystem in safeguarding critical assets and data from potential security breaches.

4.1.6.3 CYBIT – AUDACIOUS communication

The communication between AUDACIOUS and CYBIT within the NERO ecosystem is integral to ensuring a robust cybersecurity posture. AUDACIOUS, with its focus on auditing and resilience mechanisms, conducts thorough assessments to identify vulnerabilities and weaknesses in an organisation's digital infrastructure. By sharing these audit findings with CYBIT, which specialises in testing and detection, organisations can gain a comprehensive understanding of their cybersecurity landscape. CYBIT then utilises this information to conduct targeted testing and detection activities, validating and refining the audit insights. Moreover, CYBIT may provide real-time feedback to AUDACIOUS regarding detected vulnerabilities, enabling AUDACIOUS to prioritise and address critical issues promptly. This collaboration fosters 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, empowers organisations to mitigate potential threats effectively, and strengthens their overall resilience against cyber attacks. Through continuous collaboration and information exchange, AUDACIOUS and CYBIT contribute significantly to the effectiveness and adaptability of the NERO ecosystem in safeguarding against evolving cybersecurity threats.

4.1.6.4 ASTRAS – ARCANA communication

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

4.1.6.5 VICTORIOUS – ARCANA communication

The communication between VICTORIOUS and ARCANA within the NERO ecosystem is crucial for orchestrating the Bug Bounty Program effectively. VICTORIOUS, responsible for overseeing the Bug Bounty Program, plays a central role in detecting, assessing, and responding to cybersecurity vulnerabilities identified by security researchers. By communicating bug reports, assessments, and remediation actions to ARCANA, which serves as the central hub and marketplace for cybersecurity solutions, VICTORIOUS ensures that organisations within the ecosystem are promptly informed about potential security threats and vulnerabilities. ARCANA, in turn, disseminates this information to users, providing them with insights into emerging vulnerabilities and facilitating the procurement of necessary tools and resources for remediation. Additionally, ARCANA may provide feedback to VICTORIOUS based on user experiences and bug bounty program needs, enabling VICTORIOUS to refine and optimise its bug bounty program continuously. This collaborative communication streamlines vulnerability management efforts strengthens the overall resilience of organisations within the NERO ecosystem and helps safeguard critical assets and data from potential security risks. Through ongoing collaboration, VICTORIOUS and ARCANA contribute significantly to the cybersecurity posture of organisations, ensuring proactive protection against emerging threats.

4.1.6.6 Tool communication

Each framework within the NERO ecosystem comprises various tools provided by partners specifically for project purposes. These tools function independently, with limited communication restricted to those within the same framework. Inter-tool communication is kept minimal, facilitating the exchange of necessary information on an as-needed basis. Given that the majority of these tools boast high Technology Readiness Levels (TRLs) and weren't initially designed for interoperability, achieving tight integration among them at this stage is unfeasible. Instead, relevant information will flow between tools through straightforward communication channels. Priority is given to framework-to-framework communication over cross-framework tool communication. The design of communication channels, protocols, and the precise information to be shared are currently in the planning stages and are slated for presentation in D2.2.

NERO Ecosystem

A departure from this approach lies in the integration of all tools with the marketplace. The marketplace will serve as a centralised repository for all tools, necessitating a direct linkage between the marketplace and each tool. This linkage will manifest in the form of hyperlinks connecting the marketplace to the central site of each tool. Through the marketplace, users will have seamless access to the required tools via redirection. Moreover, where feasible, a single sign-in option will be incorporated, enabling users to access all tools simply by logging into the marketplace. However, this integration will be limited to tools with endpoints available for such integration, primarily due to their high TRL.

4.1.7 NERO's external communication

External users, such as SMEs, will interface with the NERO ecosystem primarily through the marketplace, which serves as the central hub for accessing cybersecurity tools and resources. SMEs will first access the marketplace through a web-based interface, where they will be presented with a curated selection of tools and solutions tailored to their needs. Upon entering the marketplace, SMEs will have the option to browse through various categories of tools, each categorised according to its specific function and purpose. They can then explore detailed descriptions and features of each tool to make informed decisions.

Once SMEs identify the tools they require, they can initiate the procurement process directly within the marketplace interface. This process may involve a simple click-through procedure to acquire licenses or subscriptions. Additionally, SMEs will have access to support resources within the marketplace, such as user guides, tutorials, and customer support channels, to assist them in implementing and utilising the selected tools effectively.

Furthermore, the marketplace will provide SMEs with access to training materials and educational resources hosted within the ASTRAS framework. These resources aim to enhance the cybersecurity knowledge and skills of SME users, empowering them to better protect their digital assets and mitigate cyber threats.

Overall, the interface between SMEs and the NERO ecosystem prioritises accessibility, user-friendliness, and comprehensive support to ensure that SMEs can easily discover, procure, and utilise cybersecurity tools and resources tailored to their specific needs and requirements.

The remainder of this chapter is devoted to presenting the initial suite of tools to be offered by the NERO project. Each tool will be thoroughly examined, highlighting its functionality, readiness level, and designated placement within the framework. Through this comprehensive analysis, stakeholders will gain insight into the diverse range of tools available within the ecosystem and their respective roles in bolstering cybersecurity measures. Additionally, the chapter will present how each tool aligns with the objectives and focus areas of the ARCANA, VICTORIOUS, AUDACIOUS, CYBIT, and ASTRAS frameworks. By providing a detailed overview of these initial offerings, the chapter aims to lay the foundation for understanding the breadth and depth of the NERO project's capabilities in addressing cybersecurity challenges.

4.2 Partner's Tools

4.2.1 ONE Holistic Security and Privacy Framework (HSPF)

4.2.1.1 Description, Architecture and Subcomponents

HSPF presents a practical approach to developing a robust threat detection model while upholding data privacy and security for all involved clients. This is achieved by leveraging Federated Learning alongside privacy-preserving techniques like Multi-Party Computation, Secure Aggregation, Differential Privacy, and Homomorphic Encryption.

The Federated Anomaly Detection model is designed to be trained by any node within 5G networks, spanning from cloud to edge. Through network flow analysis and Unsupervised Learning techniques, we can assess the likelihood of threats in received communications and respond by promptly blocking and flagging threats for immediate or future mitigation. To implement this, the protected services are augmented with a monitoring tool responsible for monitoring and facilitating the Federated Implementation. This Federated Implementation is supported by a Central Server acting as an Aggregator, responsible for aggregating received information. This information solely consists of Training Weights from the involved clients, ensuring the privacy and security of participants.

With this amalgamation of information, the Aggregator computes gradients using a specified method and returns resulting weight values to clients for further training. The following architectural schema (Figure 88) provides an overview of the process of handling and training network information, beginning with network flows as input, passing through a categorisation process distinguishing anomaly from normal communications. A defined logic identifies attacks based on preset conditions, with these attack identifications forwarded to the policy enforcer for predefined action implementation. The entire analysis can be visualised through the dashboard.

NERO Ecosystem

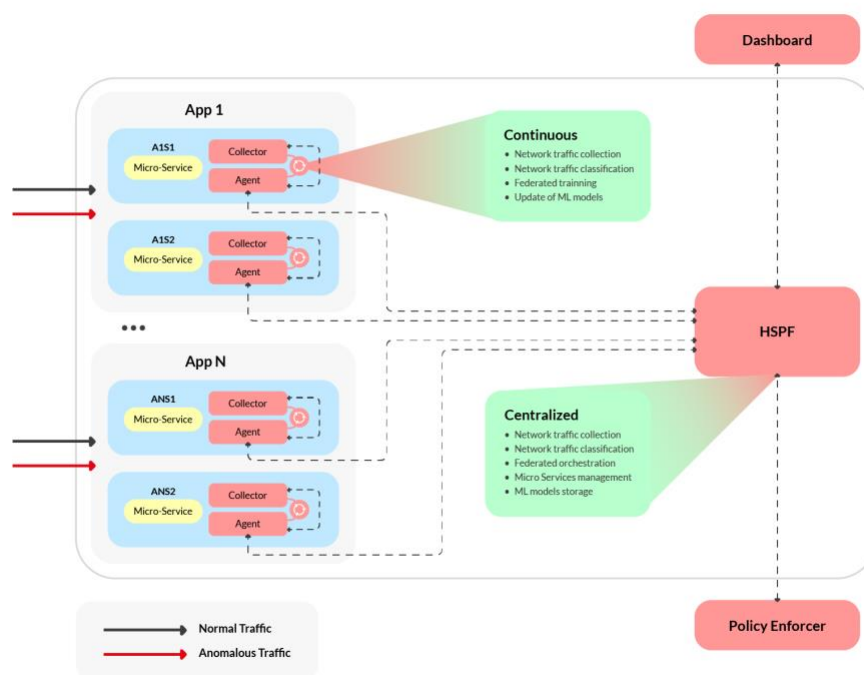


Figure 88: HSPF Architecture.

4.2.1.2 Background Assets

Table 3 includes information about existing assets that have been identified to be modified or extended, and ultimately integrated during the development of the specific NERO tool.

Table 3: Background assets used within HSPF.

Asset name	Description	Owner	Current TRL	License	Target TRL
Collector	Network Information Retriever	ONE	7	Proprietary	8
Agent	Federated Training Client	ONE	7	Proprietary	8
Aggregator/HSPF	Federated Training Server	ONE	7	Proprietary	8

4.2.2 MINDS HoneyPot as a Service (M-HaaS)

4.2.2.1 Description, Architecture, and Subcomponents

MINDS HoneyPot as a Service (M-HaaS) integrates AI and Software-Defined Networking (SDN) to manage and deploy industrial honeypots. These honeypots are crucial for capturing and analysing

malicious network activities. The platform leverages Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs), and stands out by offering robust data storage, normalization and visualisation capabilities for security data. M-HaaS two solutions: Game Theory Intelligence (GTI) and NeuralPot.

GTI utilises mathematical and logical modelling to enhance cybersecurity defences within industrial networks, as shown in Figure 89. It calculates the optimal number of honeypots to deploy by analysing the number of real devices currently connected, the maximum capacity of the network, and the strategic value each connected device. GTI then determines the precise number of honeypots that can be feasibly integrated, while maximising the potential for trapping malicious actors. This calculated deployment not only conserves computing resources but also creates a deceptive landscape, making it difficult to distinguish real assets and traps. The output from GTI guides the distribution of honeypots in a way that keeps a balance between operational efficiency and the enhanced security of network infrastructures.

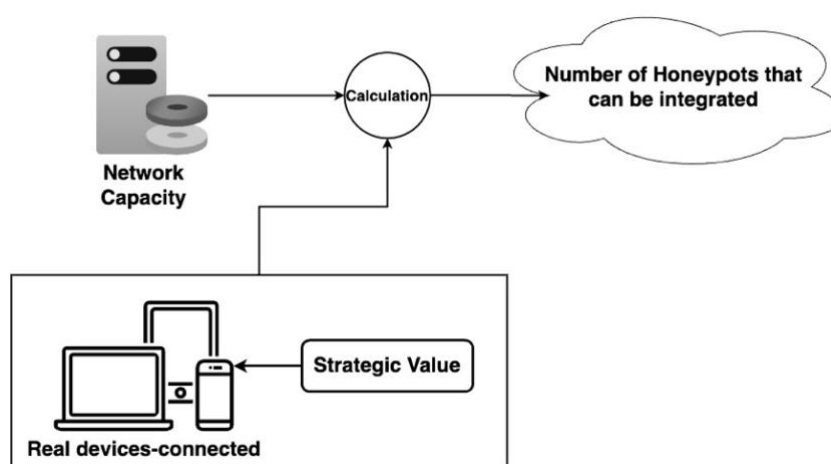


Figure 89: Game Theory Intelligence (GTI) Architecture.

NeuralPot is introduced as a novel method for adapting honeypot technologies to meet the demands of industrial networks. It represents a highly interactive iteration of the Conpot honeypot, capable of generating network traffic based on the patterns of an existing network entity. This innovative approach leverages two distinct DNN implementations, each evaluated for their efficiency in real-time network traffic generation and their capability to mimic actual network communications closely. The architectures employed, as shown in Figure 90, include the Generative Adversarial Network (GAN) and the Autoencoder, with both being assessed against actual Modbus network traffic.

The Generator module is a critical part of the GAN, composed of several layers, including dense layers where the number of neurons increases. Its goal is to output data that closely resembles the real data captured from network traffic. This module operates by receiving a random noise input and transforming it through its network layers to generate simulated data. The Discriminator then assesses this data, comparing it to real traffic data to classify it as either real or fake. This process allows the GAN to adapt and generate traffic data that is not statically defined but dynamically mimics the behaviour of actual network devices.

NERO Ecosystem

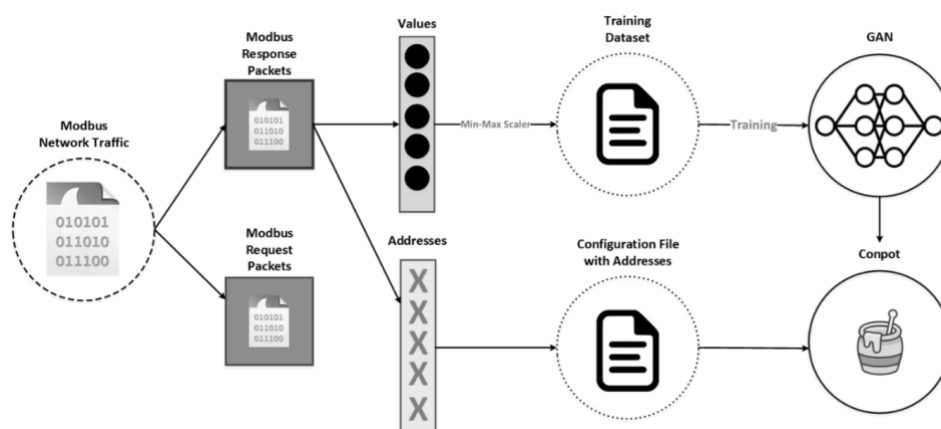


Figure 90: M-HaaS - NeuralPot Architecture.

4.2.2.2 Background Assets

Table 4 includes information about existing assets used within M-HaaS that have been identified to be modified or extended, and ultimately integrated during the development of the specific NERO tool.

Table 4: List of background assets used within M-HaaS.

Asset name	Description	Owner	Current TRL	License	Target TRL
Data-Preprocessing	Tools and techniques for cleaning and organizing raw data for analysis.	Not Specific	N/A	Open Source	N/A
Generative Adversarial Networks	AI models used for generating synthetic data that mimics real data.	Not Specific	N/A	Open Source	N/A
Conpot	An ICS/SCADA honeypot for simulating industrial control systems.	Not Specific	N/A	Open Source	N/A

4.2.3 MINDS RADAR (M-RADAR)

4.2.3.1 Description, Architecture, and Subcomponents

M-RADAR is a human-interactive and visual-based anomaly detection system, which is capable of monitoring and detecting various types of security attacks. For this purpose, it leverages the power both of signature-based methods and AI algorithms. The tool's prominent characteristic is the provision of visualisation graphs that offer a reliable overview of the network in a timely manner.

NERO Ecosystem

M-RADAR employs a wide range of data visualisation techniques aimed at providing an anomaly detection system to the network administrator, including both traditional visualisations (graph lines, tables, etc.) and more advanced ones (activity gauge, dependency wheels, etc.). Finally, tables containing specific details about the network status enable a comprehensive overview of the system's current state.

M-RADAR also utilises a series of ML algorithms, both supervised and unsupervised, to generate security events and inform the network operator for security attacks. The considered ML algorithms are periodically updated with new type of attacks, providing with a continuously expanding layer of protection.

In a nutshell, M-RADAR constantly monitors the network, capturing and analysing packets, while seeking inconsistencies and anomalies. As shown in Figure 91 the key components of M-RADAR are summarized as:

- **M-RADAR Sensors:** Open-source tools for network discovery, network capturing, security auditing, and IDS (e.g., Nmap, Suricata, Wireshark, tcpdump). This component continuously monitors the network packets through the provided sensors and scans the network periodically to discover new assets.
- **M-RADAR Core:** Responsible for gathering sensors' logs, analysing and storing them. For instance, flows and statistics are generated from the observed network traffic, that will eventually constitute a dataset for training the AI-based IDS. The latter will be used for recognising potential anomalies and attacks. Prior to the training of the AI-based IDS, the input data undergoes pre-processing into a predetermined format, while upon training, the model is ready for inference and anomaly detection. As a matter of fact, in contrast to the suricata sensor, which applies static rules that will trigger a security event, the AI-based IDS generates its own rules through training.
- **M-RADAR Dashboard:** Responsible for the demonstration and provision of visual analytics with real-time statistics. M-RADAR offers a user-friendly dashboard, providing useful information to the end-user, including real-time or historical data visualisation, network flow data types, number and type of security events, along with an asset inventory, where information related to the registered network devices is provided.

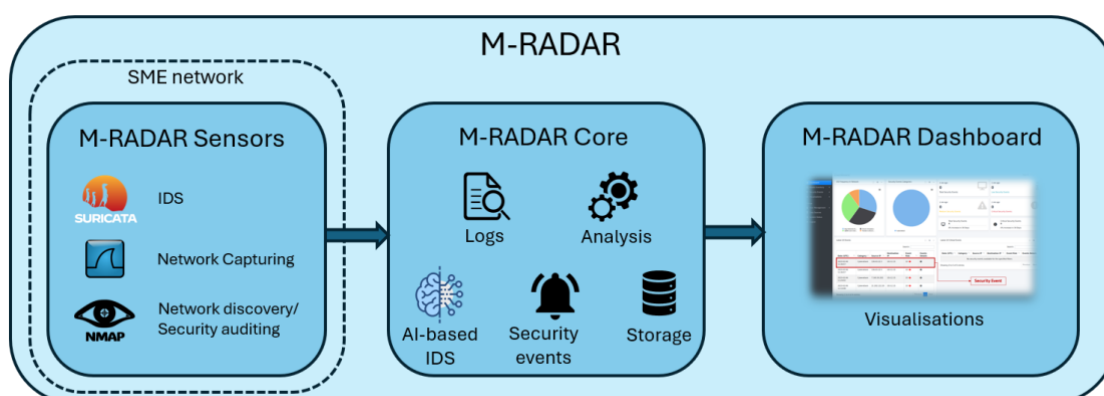


Figure 91: M-RADAR Architecture.

4.2.3.2 Background Assets

Table 5 includes information about existing assets used within M-HaaS that have been identified to be modified or extended, and ultimately integrated during the development of the specific NERO tool.

Table 5: List of background assets used in M-RADAR.

Asset name	Description	Owner	Current TRL	License	Target TRL
Suricata	Suricata is a high performance, open-source network analysis and threat detection software used by most private and public organisations and embedded by major vendors to protect their assets.	Open-source project	N/A	Open-source	N/A
NMAP	A security tool that can provide scans, attack simulation and more advanced attacks using specific plugins.	Open-source project	N/A	Open-source	N/A
Deep IDS	A DNN which is designed to detect intrusions, i.e., classify network traffic as benign or malicious, as well as the type of malicious activity and/or cyber attack.	MINDS	7	Dual license	7

4.2.4 Montimage Monitoring Tool (MMT)

4.2.4.1 Description, Architecture, and Subcomponents

In today's interconnected digital landscape, ensuring the security, performance, and integrity of systems is paramount. As organisations strive to safeguard their assets and maintain operational efficiency, the need for robust monitoring and analysis solutions becomes increasingly critical.

NERO Ecosystem

MMT, the Montimage Monitoring Tool, a versatile and powerful monitoring software suite is designed to address the complex challenges of modern IT environments monitoring. MMT offers organisations a holistic platform for analysing application, system, and network traces both offline and in real-time. MMT's open-source version available on GitHub offers SMEs a cost-effective alternative to proprietary monitoring tools. By leveraging the power of open collaboration, SMEs can harness the capabilities of MMT while minimising licensing costs and vendor lock-in. Furthermore, MMT's containerised deployment option ensures scalability and flexibility, allowing SMEs to adapt the tool to their evolving needs without a big learning curve.

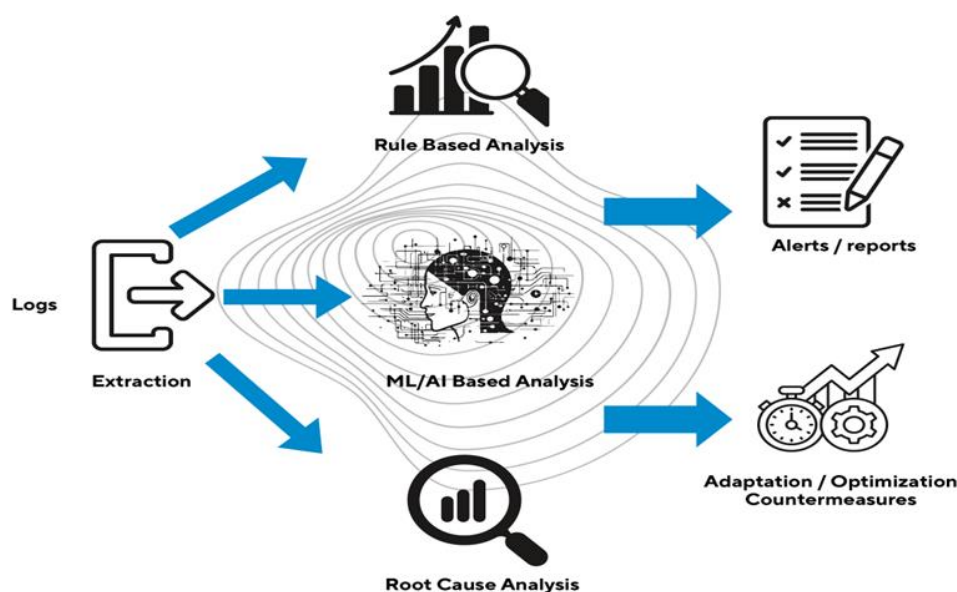


Figure 92: MMT Architecture.

At the heart of MMT lie six distinct components (Figure 92), each contributing to its robust functionality:

- **Extraction Engine:** The foundation of MMT, the Extraction Engine efficiently gathers traces from diverse sources. Whether capturing information from applications, systems, or networks, this component serves as the initial point of extraction of attributes and features for further analysis. This engine relies on a plugin architecture to extend to new data formats and protocols.
- **Rule-Based Analyzer:** Leveraging established rules and guidelines, the Rule-Based Analyzer swiftly identifies known patterns of attacks and anomalies within collected traces. Drawing upon the expertise of security professionals, this component offers a proactive approach to threat detection, enabling organizations to stay ahead of evolving cybersecurity threats.
- **AI/ML-Based Analyzer:** Embracing the power of ML and AI, the AI/ML-Based Analyzer enhances MMT's analytical capabilities. By adapting to new data patterns and identifying emerging threats, this component provides a dynamic and responsive defence against sophisticated attack vectors, elevating the tool's effectiveness in safeguarding systems.
- **Root Cause Analysis Engine:** The Root Cause Analysis Engine uncovers the underlying reasons behind system disruptions. Armed with this knowledge, administrators can pinpoint the root causes of security breaches or performance issues, paving the way for targeted remediation efforts and long-term resilience.

- **Adaptation/Countermeasure Recommendation Engine:** Transforming insights into actionable recommendations, the Adaptation/Countermeasure Recommendation Engine empowers organisations to mitigate risks effectively. By proposing tailored responses to identified incidents and vulnerabilities, this component enables proactive risk management and strengthens the overall security posture.

Dashboard: MMT traffic reports and charts are 100% configurable. The user can edit preconfigured reports and create new ones. Different chart types and graphs can be used including (pie, bars, XY charts, stacked area charts, sequence charts, tables, hierarchical tables, etc.).

4.2.4.2 Background Assets

Table 6 includes information about existing assets used within M-HaaS that have been identified to be modified or extended, and ultimately integrated during the development of the specific NERO tool.

Table 6: List of background assets used in MMT.

Asset name	Description	Owner	Current TRL	License	Target TRL
MMT-DPI (libpcap, dpdk)	Extraction engine with plugins	MONT	8	Apache v2.0	9
MMT-Security	Security analysis	MONT	7	Apache v2.0	9
MMT-RCA (similarity lib)	Root Cause analysis	MONT	4	Apache v2.0	7

4.2.5 MDS Digital Education platform for cybersecurity training (KIOKU AI)

4.2.5.1 Description, Architecture, and Subcomponents

The KIOKU AI tool represents a training component of the NERO platform, specifically designed to enhance the scenario-based training experience. This tool introduces advanced ML algorithms and natural language processing (NLP) techniques to dynamically generate and adapt training scenarios for cybersecurity awareness, tailored to the needs and infrastructure of SMEs.

The architecture of the KIOKU AI tool (Figure 93) is conceptualised in this architecture overview to operate within the NERO ecosystem, consisting of several interconnected subcomponents: Scenario Generation Engine, Adaptation and Learning Module, Feedback Loop, Integration Layer and Analytics and Reporting

Scenario Generation Engine (SGE): KIOKU AI is based on the Scenario Generation Engine, which utilises NLP to illustrate realistic and engaging cybersecurity scenarios. This engine is connected with sources that of cybersecurity incidents, best practices, and SME-specific considerations to generate content that is both relevant and educational. The technical specifications of SGE are:

- **Data Source Integration (under development):** This engine will integrate with multiple data sources to gather up-to-date information on cybersecurity threats, vulnerabilities, and incident reports. Using Application Programming Interfaces (APIs), it will pull data from reputable

NERO Ecosystem

cybersecurity databases, threat intelligence feeds, and industry-specific news sources to ensure the content's relevance and accuracy.

- **NLP Model:** The engine will employ a sophisticated NLP model trained on cybersecurity literature, white papers, real-world incident reports, and best practices. This model will be capable of understanding the context of cybersecurity content, enabling it to generate scenarios that aligned with current industry standards and threats.
- **Content Generation Algorithm:** The algorithm for content generation uses a combination of rule-based and ML techniques. Rule-based systems ensure that generated scenarios adhere to logical structures and learning objectives, while ML algorithms allow for the creative assembly of scenarios that mimic real-life cybersecurity challenges. This hybrid approach facilitates the generation of highly engaging and educational content.
- **Adaptation Mechanism:** This module adapts content based on specific SME parameters, such as company size, industry sector, and existing IT infrastructure. This customisation is achieved through a dynamic template system, which adjusts scenario variables (e.g., the complexity of threats, technical details) according to the learner's profile and organizational context.
- **Scenario Validation Layer:** Before scenarios are deployed, they are validated using a combination of automated checks and expert review. This layer ensures that all generated content is technically accurate, pedagogically sound, and free of unintended biases or errors.

Adaptation and Learning Module (ALM): This module employs ML algorithms to create scenarios based on the user's interaction, learning progress, and the specific vulnerabilities of the SME's IT infrastructure. The technical specifications of ALM:

- **User Interaction Tracking:** This module incorporates advanced tracking mechanisms to monitor user interactions with the training scenarios. It logs actions such as choices made, time spent on each scenario, and responses to quiz questions, using this data to assess user understanding and engagement.
- **Machine Learning Algorithms:**
 - **Predictive Models:** To forecast user performance and identify potential learning gaps.
 - **Recommendation Systems:** To suggest additional scenarios or resources tailored to the user's learning path.
 - **Adaptive Learning Algorithms:** To adjust the difficulty and complexity of scenarios based on the user's progress and performance metrics.
- **Dynamic Content Adjustment:** The module dynamically adjusts scenario parameters such as difficulty levels, thematic focus, and scenario complexity.
- **Learning Progression Engine:** An engine within the module maps out personalised learning paths for users, guiding them through progressively challenging scenarios. This is based on an underlying competency framework that aligns scenario objectives with specific cybersecurity skills and knowledge areas.

Feedback Loop: An integral part of KIOKU AI, the Feedback Loop captures user responses and engagement levels, facilitating continuous improvement of the scenario generation engine. This

NERO Ecosystem

mechanism ensures the training content is not only up-to-date with the latest cybersecurity threats but also resonates with the users' learning preferences. The technical specifications of Feedback Loop

- **Feedback Integration:** A feedback loop allows users to provide direct feedback on scenarios, which is used to refine and adjust future content. NLP techniques analyse qualitative feedback for insights, while quantitative feedback is assessed through engagement metrics and performance scores.

Integration Layer: The Integration Layer will serve as the “connector” between KIOKU AI and NERO platform's user interfaces (web and mobile). It ensures seamless delivery of scenarios to the tutor and student sides, enabling a coherent and interactive learning experience. The technical specifications of the integration layer:

- **API Design and Management:** The Integration Layer is built around a set of, RESTful APIs that facilitate the secure and efficient exchange of data across the platform. These APIs are designed to support various operations, including fetching personalized scenarios, submitting user feedback, and retrieving performance analytics.
- **Interoperability Standards:** To ensure seamless interoperability with external systems and data sources, the layer included interoperability standards and protocols such as:
 - **OAuth 2.0** for secure, token-based user authentication and authorization.
 - **JSON:** For lightweight data interchange, enhancing compatibility with web and mobile platforms.
 - **SCORM (Sharable Content Object Reference Model) and xAPI (Experience API):** To ensure compatibility with existing learning management systems (LMS) and to track and report users' learning experiences in a standardized format.
 - **HTTPS:** For secure data transmission over the Internet, ensuring that all data exchanges are encrypted.
- **Data Synchronization and Caching:** To optimise performance and ensure a smooth user experience, the Integration Layer implements advanced data synchronisation and caching strategies. This allows data retrieval and minimizes latency, especially critical for mobile users who may have varying internet connection speeds.

Analytics and Reporting: This subcomponent provides comprehensive analytics on user performance, scenario engagement, and learning outcomes. It offers tutors actionable insights to further customise the training program and address any identified learning gaps. The technical specifications of Analytics and Reporting:

- **Data Collection and Aggregation:** This module systematically collects data from various interactions KIOKU AI platform, including scenario completions, quiz scores, time spent on each scenario, and user feedback.
- **Advanced Data Analytics:** The module analyses collected data to uncover patterns, and insights. It uses a combination of descriptive analytics to provide a historical view of learning activities and predictive analytics to forecast future learning outcomes and identify potential areas for improvement.

NERO Ecosystem

- **Customizable Dashboards:** Tutors and administrators are provided with customisable dashboards that offer a detailed view of learner progress, engagement levels, and overall training effectiveness. These dashboards allow for the filtering of data based on various criteria, such as individual learner, learner group, specific scenarios, or time periods.
- **Learning Insights and Recommendations:** Based on the analysis, the module generates actionable insights and recommendations for both learners and tutors. For learners, it provides personalised feedback and suggestions for further learning opportunities.
- **Interoperability with Learning Management Systems (LMS):** To ensure integration with existing educational infrastructure, the module supports interoperability standards as the ones mentioned before. This allows for the easy export of learning data to external LMS platforms, enabling a view of learner progress and achievements across different training programs.

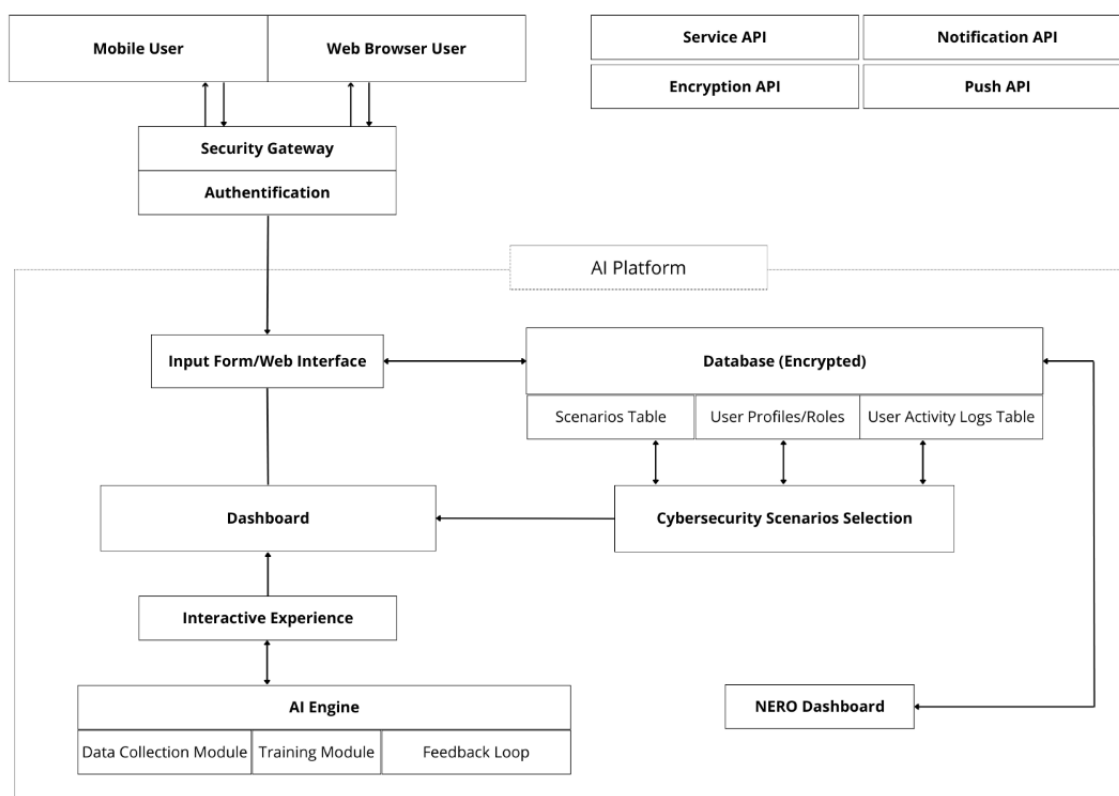


Figure 93: KIOKU AI architecture.

4.2.5.2 Background Assets

Table 7 includes information about existing assets used within KIOKU AI that have been identified to be modified or extended, and ultimately integrated during the development of the specific NERO tool.

Table 7: List of background assets used within KIOKU AI.

Asset name	Description	Owner	Current TRL	License	Target TRL
------------	-------------	-------	-------------	---------	------------

KIOKU AI	Scenario Based Training Platform for cybersecurity awareness training	Massive Dynamic Sweden (MDS)	5	Currently Open Source/License planned	8
----------	---	------------------------------	---	---------------------------------------	---

4.2.6 SNYK

4.2.6.1 Description, Architecture, and Subcomponents

Snyk is a holistic security toolset that help to implement security by design principle in software and application security. Snyk is a developer-first security platform that helps developers find and fix vulnerabilities in their code, open-source dependencies, containers, and infrastructure as code.

Development Lifecycle & DevSecOps Integration: Snyk integrates with various development tools, workflows, and automation pipelines, making it easy for developers to incorporate security throughout the development lifecycle including smoothly integrated into DevSecOps. Snyk (Figure 94) integrates seamlessly with DevSecOps practices by enabling “Shift Left” security. This means prioritizing security throughout the development lifecycle and not only afterthought.

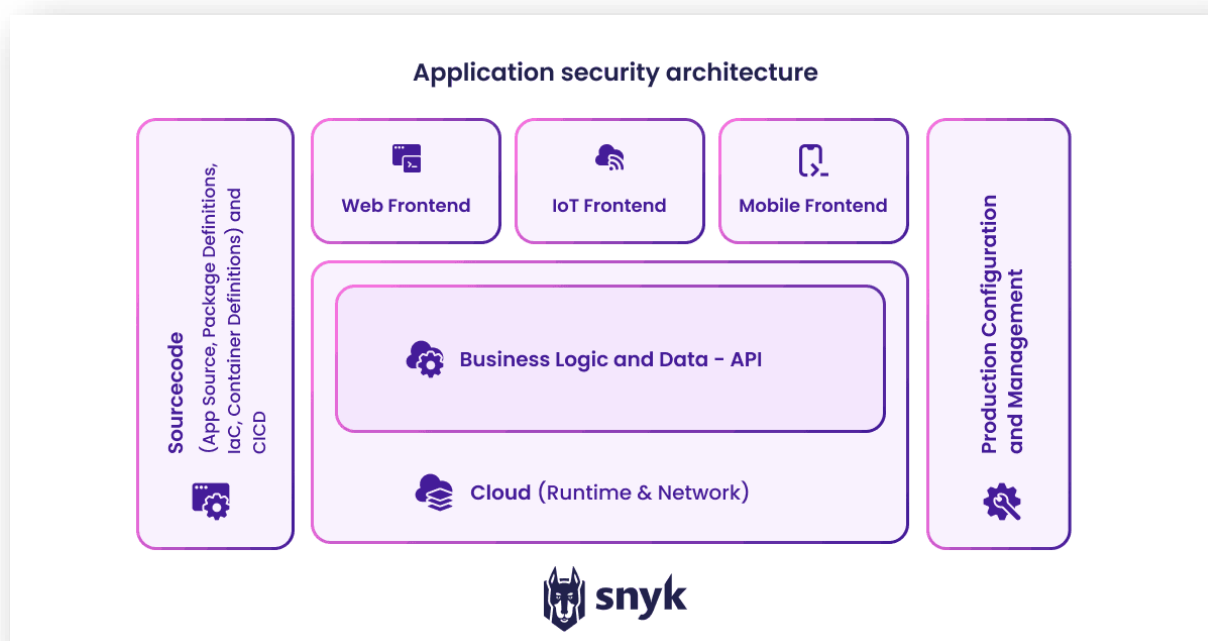


Figure 94: Application Security architecture.

Some of the key benefits of the tool are:

1. **Vulnerability scanning:** Snyk can scan your code, dependencies, containers, and infrastructure code for security vulnerabilities across a vast database of open-source libraries.
2. **Automatic fixing:** Snyk can sometimes automatically fix vulnerabilities or provide recommendations on how to fix them.
3. **Monitoring:** Snyk can continuously monitor your projects for newly discovered vulnerabilities and alert you when a fix becomes available.

NERO Ecosystem

4. **Developer-friendly integrations:** Snyk integrates with various IDEs, code repositories, and CI/CD pipelines, making it easy for developers to use within their existing workflows (as explain above for DevSecOps).

Furthermore, Snyk offers various features and functionalities through other methods besides the API, such as:

1. **Integrations:** Snyk integrates with various development tools and platforms like IDEs, CI/CD pipelines, and cloud source code management platforms. These integrations allow you to leverage Snyk functionality within your existing workflow without needing the API.
2. **Command-Line Interface (CLI):** You can use the Snyk CLI to interact with Snyk and perform various tasks like scanning projects, managing vulnerabilities, and integrating with other tools.
3. **User Interface (UI):** The Snyk web interface provides access to most features available through the API, including vulnerability information, project management, and remediation advice.

Therefore, while the Snyk API itself is not available in the free version, you can still access the core functionality through alternative methods. The Snyk enterprise version offers API key, but we need API if our main application package does not offer the above solutions of the integration. Snyk is open source and the code is available on GitHub.

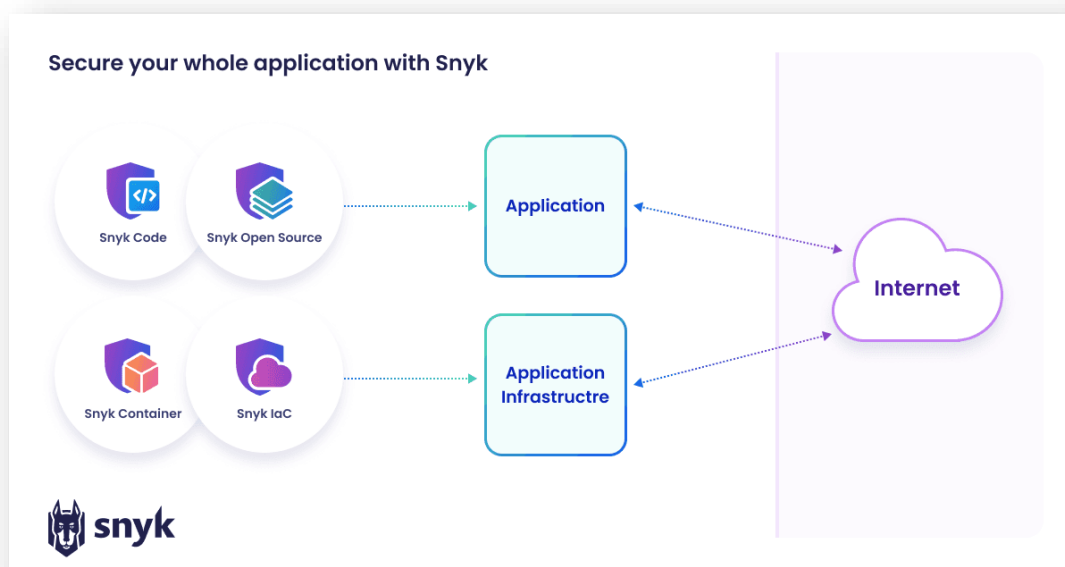


Figure 95: Visual of how Snyk's Toolkit Fits into Application Security.

Snyk Code as shown in Figure 95 utilizes source code analysis to scan for security vulnerabilities, powered by a semantic, AI-based engine. It analyses aspects such as API usage, coding issues, control flow, data flow, and hardcoded secrets. Leveraging vast open-source repositories, Snyk Code transforms code into intermediate representations like abstract syntax trees and event graphs for deep, content-aware analysis. It employs a logic solver with advanced algorithms for efficient runtime and semantic fact generation, aiding in identifying security vulnerabilities. With the support of ML algorithms and insights from Snyk's security experts, a robust knowledge base is created. Additionally, Snyk Open Source helps identify and fix vulnerabilities in the open-source libraries used by applications. It builds a dependency graph, utilising a comprehensive vulnerability database to detect issues in any packages within that tree, providing essential security information to address code vulnerabilities effectively.

NERO Ecosystem

Finally, Snyk reads the information from the file system, the container does not need to be run. This means that for a successful scan, no container or foreign code must be run. After Snyk has the list of installed software, Snyk looks that up against the Snyk Vulnerability Database, which combines public sources with proprietary research.

4.2.6.2 Background Assets

Table 8 includes information about existing assets used within SNYK that have been identified to be modified or extended, and ultimately integrated during the development of the specific NERO tool.

Table 8: List of background assets used within SNYK.

Asset name	Description	Owner	Current TRL	License	Target TRL
Snyk Code	Snyk Code uses an AI-based engine and ML to deeply analyze and identify security vulnerabilities in code through advanced source code analysis and data interpretation.	Snyk	-	Currently Open Source / Free and Paid License.	-
Snyk Open Source	Snyk Open Source identifies and resolves vulnerabilities in application libraries by constructing a dependency graph and utilising a comprehensive database to detect security flaws throughout the library structure.	Snyk	-	Currently Open Source / Free and Paid License.	-
Snyk Container	Snyk scans for vulnerabilities without running containers or foreign code by reading file system information and comparing installed software against its Vulnerability Database, which	Snyk	-	Currently Open Source / Free and Paid License.	-

	includes both public and proprietary data.				
--	--	--	--	--	--

4.2.7 TRUSTILIO Practical Human Centric Risk Management (HRM) methodology

4.2.7.1 Description, Architecture, and Subcomponents

Human threats pose significant risks to the security of Information and Communication Technology (ICT) systems, yet they are often overlooked in traditional risk management approaches. They include malicious or unintentional actions by users within an SME that compromise its security, non-authorised access to data, theft of intellectual property, sabotage of systems and networks, and errors. The human threats are exposed by exploiting human vulnerabilities which include lack of awareness, lack of security culture, lack of practical skills and capabilities, non-secure behaviours, lack of cyber hygiene, low morals, low cyber maturity of the users (e.g., defenders/administrators/third parties) of the ICT system. Human errors, a common serious human threat, are due (among others) to lack of training, stress, nervousness, anxiety, inability to pay attention/concentrate, cognitive malfunction, overconfidence, multitasking, and physical limitations of the users.

The attackers use social engineering attacks to exploit human vulnerabilities to manipulate SME users into divulging confidential information or performing unauthorised actions. These attacks often involve techniques such as phishing emails, pretexting, baiting, and disinformation.

Human Centric Risk Management (HRM) is a methodology that builds upon existing technical risk management methodologies to estimate technical risks and uses cyber socio-psychology techniques to identify human threats and estimate human vulnerabilities and risks. HRM is easy to implement since it uses open-source risk management tools (e.g. ENISA [48], OWASP [49]) for the estimation of technical risks and co-creation workshops for the estimation of human-related risks and the effective management of the risks. The HRM is a risk management methodology that integrates human factor considerations into the framework of ISO 27001, so that SMEs can enhance their ability to manage their security risks effectively. HRM adopts a proactive approach in identifying and addressing human threats and implementing best practices for security management, so the SMEs can strengthen their overall security posture and protect their valuable assets from evolving cyber threats transforming their employees as their strongest allies.

HRM is compliant with ISO27001 that requires organisations to conduct regular risk assessments to identify potential threats and vulnerabilities and estimate the risks of the ICT system to these threats. In addition to technical risks, human element threats should be thoroughly evaluated, considering factors such as SME security culture level, employee behaviour, psychological profiles, personality traits, and cognitive characteristics. Risk treatment measures should be tailored to address human element threats effectively, including the implementation of appropriate controls which are technical but also social measures e.g., awareness raising, training programs, behavioural change interventions, and co-creation workshops towards advancing security behaviours and attitudes. SMEs shall start by identifying the human vulnerabilities of their employees that interact with their ICT. Their risk treatment plan needs to include targeted social controls that will decrease the human vulnerabilities of their employees and their human-related risks striving SMEs to maintain robust security practices.

Evaluating cybersecurity risks of ICT assets against threats involves assessing the vulnerabilities (weaknesses) of the assets for these threats (which depend upon the controls that have been implemented), the impact (consequences of these threats if will be exploited) and the frequency and probability of the threats to occur. While numerous standards, e.g., ISO27000x, ISO 31000:2018 and methodologies (e.g., NIST (SP 800-53), NISR (SP 800-37), NIST SP-800-161, ETSI TS 102 165-1, NISIR 8286) exist for risk assessment, they overlook the human threats and human traits that enable their exploitation (human vulnerabilities), despite the recognition of humans as a weak link in cybersecurity). Also, the existing standards and methodologies undertake technical controls to treat the risks ignoring the necessary social mitigation measures (e.g., awareness raising, training, social interventions, and co-creation workshops) that will help ICT users to strengthen their personal security hygiene and resilience to cyber attacks, decreasing the human vulnerabilities, the occurrence of human threats and in return decrease the risks. HRM examines deeper the human element of the users that defend/ interact with the SME's ICT in order to identify human threats and vulnerabilities and propose targeted technical and social controls that can be easily embraced by the employees.

The human threats and risks are being identified and estimated using socio-psychology principles. In HRM extended psychological profiles of the users are used and analysed besides motivations, abilities and triggers personality traits and social characteristics. Cyber profiling is the instrument used to identify human threats and vulnerabilities of the ICT users as a proactive measure to select targeted social controls that will lower the employees' vulnerabilities to human threats. HRM methodology uses a multi-dimensional cyber psychological profile for the users to evaluate the factors that determine secure behaviours.

Co-creation workshops are also used to develop a comprehensive and effective risk treatment plan. These workshops are participatory events where ICT users collaborate. The adoption of security measures is streamlined through these workshops, as they are designed to directly engage users in the development process, thereby enhancing the likelihood of triggering secure behaviour. The fundamental goal of HRM co-creation workshops is to leverage the collective intelligence and diverse psychological profiles of ICT users, a strategy that has been shown to foster a wider engagement in cybersecurity practices.

Key features of HRM co-creation workshops include:

- **Diversity of Participants:** These workshops prioritise the inclusion of a diverse range of ICT system users, such as organisational insiders (e.g., CISOs, risk managers, incident handlers, defenders, administrators, and general employees), suppliers or supply chain partners, and third parties (e.g., auditors, external penetration testers). This diversity is crucial for capturing a wide array of perspectives and experiences, which enriches the security discourse [50].
- **Collaboration:** Participants are encouraged to collaborate in a structured setting, facilitated by experienced leaders. This approach mirrors effective teamwork strategies that are essential for problem-solving and innovation in cybersecurity [51].
- **Interactive Activities:** Employing methods such as brainstorming sessions, design thinking exercises, and prototyping fosters a creative and engaging environment. These activities are foundational to generating practical and innovative solutions [52].
- **Risk Treatment Generation and Refinement:** The workshops focus on developing a comprehensive set of social and technical measures, which are refined through collaboration into viable security controls. This process aligns with best practices in risk management [53].

NERO Ecosystem

Any available open-source risk assessment tools can be used to assess cyber risks for example the ENISA and OWASP tools:

- ENISA Risk Management (RM) Toolbox:** a set of resources and tools that are designed in order to assist organizations in the effective management of cybersecurity risks. It provides guidance, templates, and best practices for various aspects of cybersecurity risk management, including risk assessment, risk treatment, and risk communication. The aim is to help organisations identify, assess, and mitigate cybersecurity risks in line with industry standards and best practices. Additionally, the ENISA Risk Management (RM) Toolbox includes risk assessment methodologies, risk treatment options, incident response procedures, and guidelines for developing cybersecurity policies and procedures. The ENISA RM toolbox provides stakeholders with a standardised framework for risk management (RM) to facilitate a common understanding of risks and associated levels, accommodating various RM approaches and tools without altering organisations' established practices. This toolbox enables interoperability, allowing comparison of results across different organisations and RM methods. Regulatory bodies can employ it to gain a thorough understanding of risk levels and security posture within particular sectors or jurisdictions, thereby providing guidance to organisations as needed. By aligning RM endeavours and standardising results using common metrics, the toolbox enhances comparison and offers actionable insights for subsequent actions [48] More specifically, the toolbox interprets risk scenarios utilising its own terminology, asset classifications, and threat taxonomies within different risk assessment methodologies, and standardises the assessment results to a common risk matrix, enabling comparable outcomes. It uses the ITSRM [48] as a reference framework for the RM activities and facilitates the alignment of RM activities in four RM functions, depicted in Figure 96.

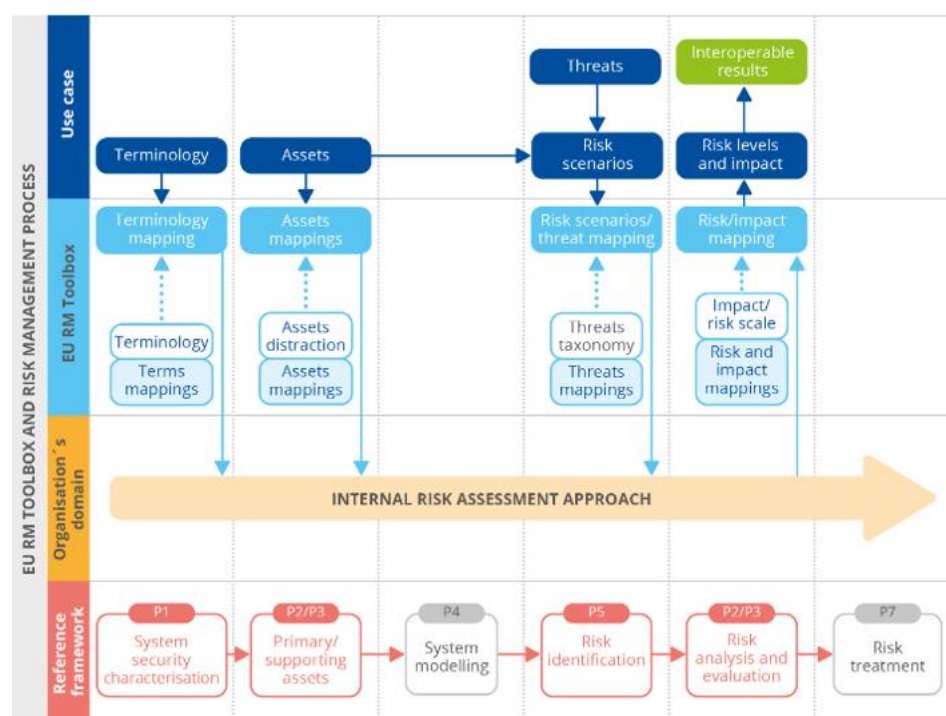


Figure 96: ENISA RM Toolbox and RM process.

- OWASP Risk Assessment Calculator:** is a tool designed to assist organisations in conducting risk assessments specifically focused on web application security. It helps organisations identify and prioritise risks associated with their web applications based on factors such as impact, likelihood, and risk exposure. Some of its key features may include Risk Identification, Risk Analysis, Risk Prioritisation, Documentation and Reporting, Customization and Flexibility. Overall, the OWASP Risk Assessment Calculator can support organizations seeking to assess and manage risks associated with their web applications, by enhancing the security posture of their web applications and mitigate cybersecurity risks proactively. More specifically, it follows the OWASP Risk Rating Methodology [54] which approaches the standard risk model of “Risk = Likelihood*Impact”. After identifying the risk, the OWASP Risk Assessment Calculator can be exploited in order to determine the severity of the risk (Figure 97) by setting specific factors for estimating likelihood and estimating impact. Those steps are crucial for the classification of the risks to determine which should be addressed first.

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Figure 97: Determining a risk's severity [54].

The HRM developed an extended profile based on with traits that identify the users with secure behaviour. As shown in Table 1 these factors include: personality, social traits, technical skills and capabilities according to their relationship (business role) of the users in the SME e.g. the security professionals (e.g. CISO, Risk Managers, auditors) will need to have the skills as defined in European Cybersecurity Skills Framework (ECSF) [55] where the general employees will need to have the skills for practicing personal hygiene. Personal cyber hygiene practices include the use strong passwords, conduct regular software updates, use reputable antivirus software; avoid using public Wi-Fi for sensitive transactions; learn to recognise and avoid phishing emails, messages, and calls; conduct regularly back up; review and adjust the privacy settings, secure file sharing; don't overlook physical security. Factors in Table 9 include the motivations that will stimulate the secure behaviour of the users, and the triggers (opportunities/ measures) that the organization adopts.

Table 9: HRM-multi dimensional profile of users with secure behaviour.

HRM Secure Behaviour Profile of users	
Personality Traits	
Vigilance	Consistently remains alert and attentive to potential security threats, and is proactive in identifying and addressing suspicious activities.

NERO Ecosystem

Responsibility, Curiosity	Takes full ownership of their role, with an innate curiosity that drives them to deepen their understanding of cybersecurity threats and vulnerabilities.
Adaptable-Openness to experiences	Displays flexibility and openness to new security technologies, strategies, and approaches that enhance their security posture. Possesses a blend of intellect and creativity, demonstrates originality, and shows a keen scientific interest alongside a spirit of adventurousness.
Resilient	Has the capacity to cope with stress, setbacks, and failures, demonstrating resilience by quickly bouncing back and steadfastly maintaining a strong focus on achieving security objectives.
Social Traits	
Social exposure	Adapts to conventional social norms with ease, excelling in forging strong bonds with each co-worker. Collaborates effectively with colleagues, security teams, and external partners to tackle security challenges, sharing information and insights for collective benefit.
Conventional relationships	Effortlessly establishes professional virtual relationships, fostering collaborations and creating synergies.
Ethical	Individuals with integrity prioritize honesty, transparency, and respect, steadfastly adhering to ethical principles and professional codes of conduct.
Technical skills & Resources	
Networking skills	Proficient in network security, including protocols, firewalls, routers, and switches; knowledgeable about encryption techniques, cryptographic protocols, and secure communication methods.
IT skills	Cyber hygiene practices, Proficient in a variety of Operating Systems, programming languages, and emerging technologies, with a comprehensive understanding of web application security principles and the ability to identify common vulnerabilities, such as SQL injection and cross-site scripting (XSS).
Soft skills	Efficient problem-solver and team player with strong analytical and communication skills, adept at working with cross-functional teams to achieve security goals. Proficient in creating concise security documentation. Committed to continuous learning and adaptability, quickly grasping new security trends, tools, and practices to address evolving challenges.
Available Resources	Possesses or has access to high computer processing power, such as advanced machines, multiple Virtual Machines, or High-Performance Computing systems (HPCs), and is involved with security communities, including CERT and ISACs.
Relationship with the organization	
Roles include insiders, such as security professionals (as described in the ECSF [10]) and general employees engaging with ICT systems; suppliers or supply chain partners contributing to the	

organisation's value chain; and third parties like auditors, external penetration testers, and authorities interacting with ICT systems.
Motivations (for the employees to adopt a secure behaviour)
To protect ICT systems, prevent harm, and adhere to professional ethics and conduct, while respecting privacy, confidentiality, and legal standards. Aims to foster trust in digital technologies through commitment to security best practices, contribute to public safety, enhance their organisation's security posture, and combat cybercrime, thereby making a global impact. Also focuses on continuous skill and knowledge advancement, with incentives like financial bonuses and rewards.
Triggers /Social Measures (that the SMEs provide to employees in order to adopt secure behaviour)
Implement targeted training and behaviour change interventions to improve cyber hygiene, alongside fostering ethical awareness. Establish clear security policies, procedures, and reporting guidelines, supported by leadership and regular updates. Encourage compliance through user-friendly security solutions, positive reinforcement, and recognition. Offer constructive feedback, coaching, and training on security performance. Cultivate a security-aware culture through positive peer influence.

The HRM profile traits significantly influence the secure behaviour of ICT system users. The assessment of secure behaviour levels among ICT users is facilitated through the use of anonymised questionnaires, a method supported by research indicating its effectiveness in gathering sensitive data [56].

To select appropriate social measures for improving security behaviour, co-creation workshops are employed. The HRM methodology is structured into three main phases according to standards.

- **Phase A**, Cartography, involves setting boundaries and includes developing an asset model to describe and understand interdependencies of all ICT system assets under assessment. This can be accomplished using any Business Process Modelling (BPM) tool such as VISIO, ADONIS, Bizagi Modeler, or TIBCO. Additionally, a user model is developed to identify all users that own or use these assets, along with their relationships with the SME, typically through interviews with the governing body. Furthermore, anonymous HRM profiles of users are created to estimate their levels of secure behaviour, using provided profiles and anonymously distributed and collected questionnaires.
- **Phase B**, Risk Assessment, comprises identifying and estimating the levels of physical, cyber, and human threats, assessing vulnerability and impact levels, and proposing both technical and social countermeasures based on the profiles captured in Phase A. The ENISA Risk Management Toolbox or OWASP guidelines are recommended for the implementation of these strategies, with co-creation workshops utilised to develop and refine pragmatic security measures [56], [57].
- Finally, **Phase C**, Risk Management, involves the implementation of the selected technical and social measures, with SME governance members leveraging business intelligence and cost-benefit analyses in co-creation workshops to ensure effective implementation and testing of these measures.

Given the above, the Human Centric Risk Management (HRM) methodology's architecture can be summarized to the following Figure 98.

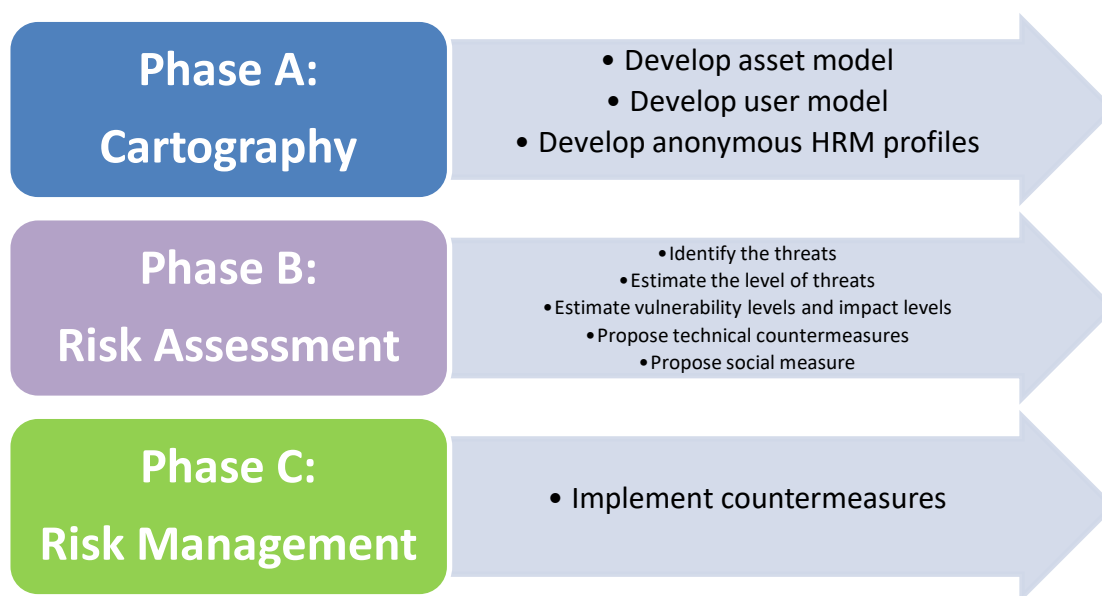


Figure 98: HRM architecture.

4.2.7.2 Background Assets

Table 10 includes information about existing assets used within HRM that have been identified to be modified or extended, and ultimately integrated during the development of the specific NERO tool.

Table 10: List of background assets used within HRM.

Asset name	Description	Owner	Current TRL	License	Target TRL
HRM	Human Centric Risk Management (HRM) Practical Methodology	TRUSTILIO	-	Open Source	-

4.2.8 PLUR Seer Box

4.2.8.1 Description, Architecture, and Subcomponents

Seer Box is a product for the monitoring and protection of Web applications and APIs that, when compared against traditional Web Application Firewalls (WAF), aims to offer a broader perspective on the security of the monitored services. Whilst it enables "Web Application Firewall - like" functionalities, it is as a Web Application Security Manager since it is designed to be the cornerstone of a defensive end-to-end strategy for protecting Web Applications and Services. Seer Box can complement DAST scanners extending the verification surface and providing virtual patches to ensure end-to-end vulnerability management. All of this makes Seer Box able to operate as a primary Web Application Firewall but also to complement WAFs already in the infrastructure representing the last line of security in the protection of Web Applications and APIs. Unlike traditional WAFs Seer Box is designed to be non-invasive during deployment, integrating natively with the devices/solutions already present (both in the cloud and on-premise) both for the observation of traffic in transit and the application of traffic

NERO Ecosystem

blocking policies. Any WAF solutions already present can however be exploited and enhanced by Seer Box, through the construction of traffic-blocking policies built with wizards for the monitored services. Seer Box is natively integrated with the most widely used solutions on the market, such as Web Server/Reverse Proxy/Load Balancer, Application Delivery Controller, Firewall and WAF, and SIEM, both commercial and open-source among the most widely used on the market. It has also been certified by NGINX1 as a fully compatible dynamic NGINX+ module. The solution is deployable indifferently within on-premise and public cloud environments, thus enabling high visibility into web services and applications security with a single point to control them all. Differently from public cloud providers, it aims to be cloud provider-independent, offering the possibility to deploy it anywhere and to monitor their services independently from where they are located. The deployment features make it possible to monitor even heterogeneous environments with a single installation where applications and services are spread across several different locations, both on premise and in the cloud. This provides a much greater level of flexibility than both traditional physical appliances and WAF SaaS solutions, which cannot, however, be used to monitor non-publicly exposed applications. SEER BOX also features an extended set of APIs, to enable and support Security Orchestration, Automation, and Response.

Seer Box relies on a highly concurrent and scalable architecture implemented in Elixir in order to orchestrate its management components, running on the trusted and well-known BEAM/OTP platform and empowered by its robust set of dedicated frameworks, resulting in an extremely resilient and fail-safe system. At the core of its data processing components, Rust is employed to ensure security and efficiency, taking full advantage of the language's ground breaking strengths in terms of speed, memory safety and reliability. The functional approach and the innovative character derived from these leading-edge technologies with the support of their thriving, and modern ecosystem, allowed the PLURIBUS ONE engineering team to build a system providing first-class protection of web services and secure handling of sensitive data, all while guaranteeing efficiency, availability and ease of use.

Seer Box can communicate with external entities and is interoperable with the main security architectures available on the market.

It has even been certified by NGINX, the world's most widely used web server and reverse proxy. (<https://www.nginx.com/products/nginx/modules/seerbox-pluribus-one>). The following Figure 99, represent the Seer Box architecture and, Figure 100 and Figure 101 represent the Seer Boxx Installation architecture.

NERO Ecosystem



Figure 99: Seer Box architecture.

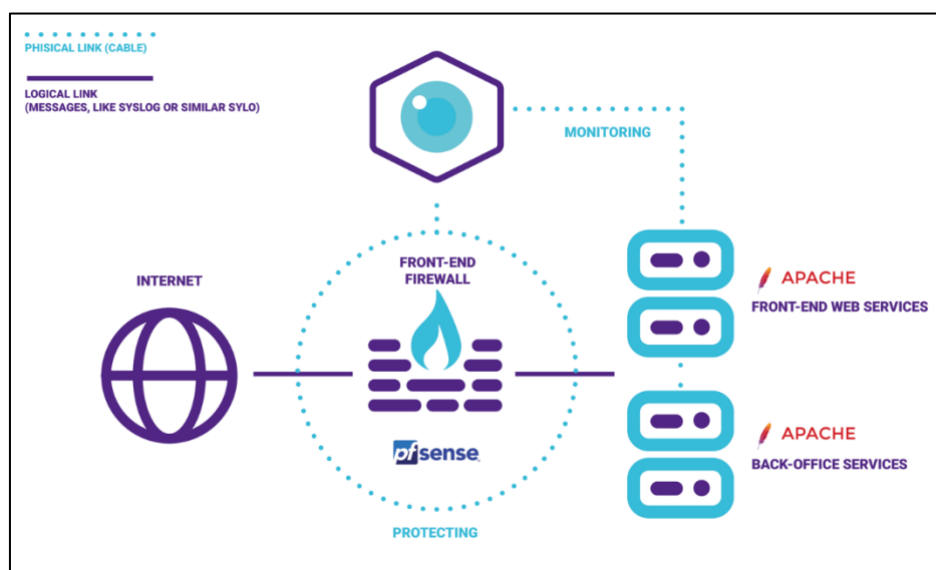


Figure 100: Example of Installation architecture_01.

NERO Ecosystem

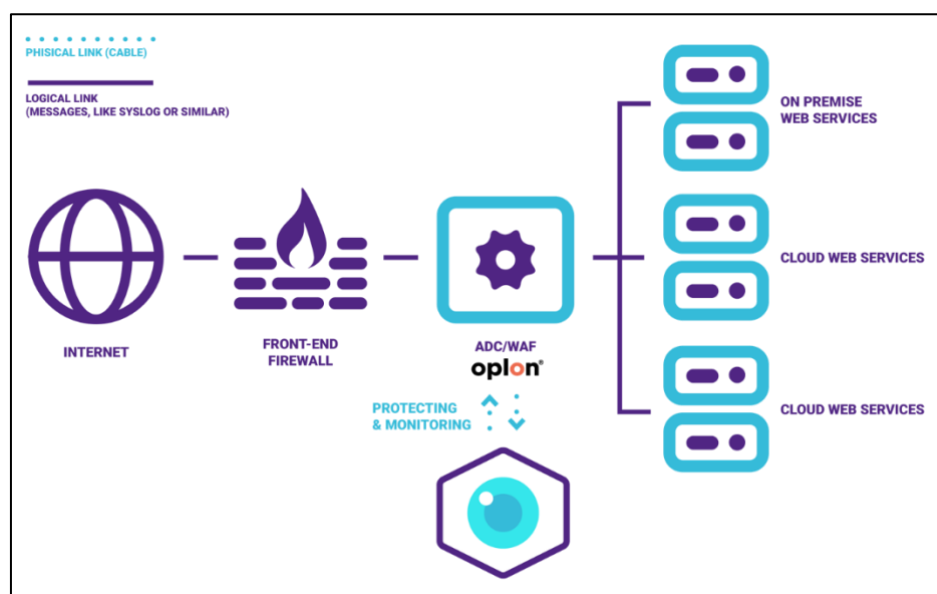


Figure 101: Example of Installation architecture_02.

4.2.8.2 Background Assets

Table 11 includes information about existing assets used within SeerBox that have been identified to be modified or extended, and ultimately integrated during the development of the specific NERO tool.

Table 11: List of background assets used within Seer Box.

Asset name	Description	Owner	Current TRL	License	Target TRL
Seer Box	"Web Application Protection Manager" based on AI and ML techniques, it can be fully integrated into the SecDevOps cycle. Within the CYBIT framework, it will be used to identify/protect, detect and respond/recover. Within the AUDACIOUS framework, it will be used for security testing scans for applications.	PLUR	8	Proprietary-Free trial available	9

4.2.9 Montimage Attack Detect React (ADR)

4.2.9.1 Description, Architecture, and Subcomponents

The Attack Detect React (ADR) Cyber Range represents a cutting-edge virtualised platform designed to bolster cybersecurity preparedness and awareness among individuals and organisations. With a focus on experiential learning, this innovative tool aims to provide hands-on experience in understanding cyber threats, detecting malicious activities, and implementing effective countermeasures. Through simulated attack scenarios and real-time monitoring, participants gain valuable insights into the tactics, techniques, and procedures employed by cyber adversaries (Figure 102). The primary objectives of the Attack Detect React Cyber Range are:

- **Raising Awareness:** By immersing participants in realistic cyber attack scenarios, the Cyber Range aims to raise awareness about the evolving threat landscape. Through first hand experience, participants gain a deeper understanding of the potential risks and vulnerabilities facing their digital assets.
- **Understanding Attack Generation:** The Cyber Range provides participants with insights into the methods used by attackers to infiltrate systems and compromise data. By simulating various attack techniques, participants learn to recognise common indicators of compromise and understand the strategies employed by adversaries.
- **Getting familiar with Detection Techniques:** Participants are equipped with the knowledge and skills needed to detect malicious activities within their network environment. Through the use of advanced monitoring tools and techniques (using the Montimage Monitoring Tool), they learn to identify anomalous behaviour, unusual network traffic, and other indicators of a potential security breach.
- **Learn about mitigation actions:** In addition to detection, participants learn how to respond effectively to cyber threats. By exploring various response strategies and implementing countermeasures, they gain practical experience in mitigating the impact of attacks and safeguarding their systems against future incidents.

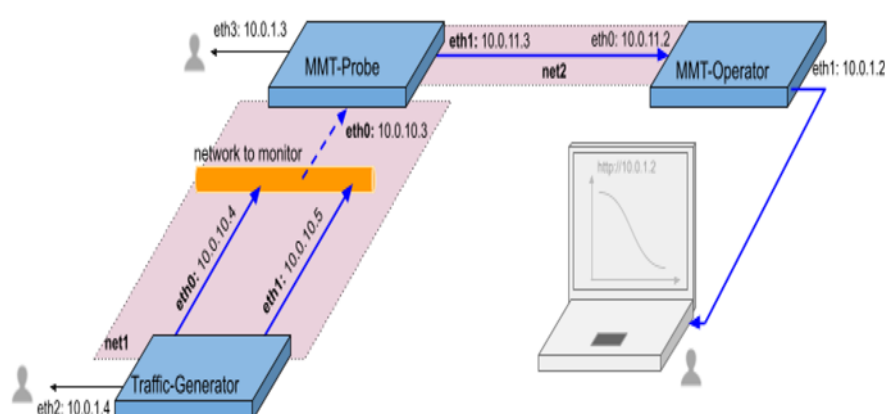


Figure 102: ADR architecture.

The Attack Detect React Cyber Range consists of three virtual machines (VMs), each serving a specific role:

- **Attacker VM:** This VM is responsible for generating simulated cyber attacks against the target environment. Participants have the opportunity to act as attackers, utilising a range of offensive tactics to infiltrate systems and compromise data.
- **Target and Monitoring VM:** The Target VM represents the simulated environment that participants are tasked with defending. It hosts critical assets and services that may be targeted by cyber adversaries. Additionally, this VM includes monitoring tools that enable participants to observe and analyse network traffic for signs of malicious activity.
- **Operator Dashboard VM:** The Operator Dashboard provides participants with a centralised interface for managing and monitoring the Cyber Range environment. From this dashboard, operators can configure attacks scenarios, monitor alerts, and trigger countermeasures.

The Attack Detect React Cyber Range represents a powerful tool for enhancing cybersecurity awareness and readiness. By providing participants with hands-on experience in understanding, detecting, and responding to cyber threats, the Cyber Range equips individuals and SMEs with the knowledge and skills needed to safeguard their digital assets effectively. Through immersive training scenarios and real-time feedback, participants emerge better prepared to defend against the ever-evolving landscape of cyber threats.

4.2.9.2 Background Assets

Table 12 includes information about existing assets used within ADR that have been identified to be modified or extended, and ultimately integrated during the development of the specific NERO tool.

Table 12: List of background assets used in ADR.

Asset name	Description	Owner	Current TRL	License	Target TRL
Attack generator	A set of scripts and pcap files to generate attacks	MONT	9	Dual licence	9
MMT	Montimage monitoring solution	MONT	7	Dual licence	9

4.2.10 TRUST-IT, COMMpla Cyber Range & Capacity Building in Cybersecurity (CyberWiser)

4.2.10.1 Description, Architecture, and Subcomponents

The web portal will offer a unique single point of access to both trainers and trainees to the Cross-Learning Facilities that will host dedicated Workspace areas for specific users/teams.

The web portal, as shown in Figure 103, will guarantee the integration of the Cross-Learning facilities, and therefore the integration of the other CYBERWISER.eu components, through a Single Sign On (SSO) mechanism based on OpenID Connect module that provides a pluggable client implementation for the OpenID Connect protocol.

By accessing the web portal, the user will be able to reach the Cross-Learning Facilities by means of a Workspace organized in different in areas which can be defined by the matching of the user's own

profile and skills. Each area will be based upon a Learning Content Management System (LCMS) which will offer the possibility to enable tailor-made training courses to specific users/teams. For each of the training courses, the LCMS will support the performance of theoretical validation of the competencies acquired by the trainees with the awarding of a certification on competencies acquired.

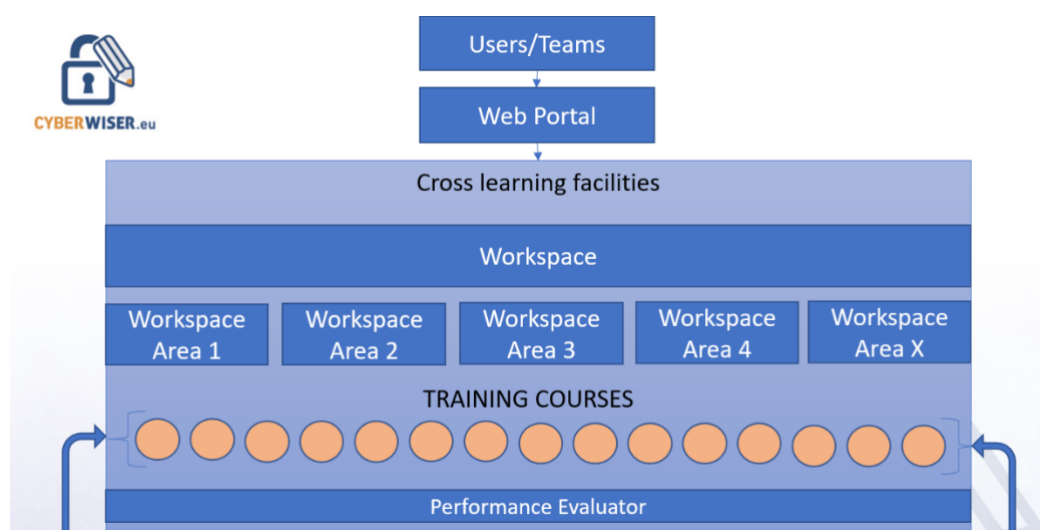


Figure 103: CYBERWISER.eu training platform architecture.

4.2.10.2 Background Assets

Table 13 includes information about existing assets used within CyberWiser.eu that have been identified to be modified or extended, and ultimately integrated during the development of the specific NERO tool.

Table 13: List of background assets used within CyberWiser.eu.

Asset name	Description	Owner	Current TRL	License	Target TRL
Web Portal	The web portal guarantees the integration of the Trust Workspace through a SSO mechanism based on OpenID Connect module that provides a pluggable client implementation for the OpenID Connect protocol.	Trust-IT	7	Proprietary Trust-IT	8
Trust Workspace	A set of Workspace areas and a Learning Content Management	Trust-IT	7	Proprietary Trust-IT	8

NERO Ecosystem

	System which are used by the users to access the courses, the training material and other components				
--	--	--	--	--	--

4.2.11 TRUST-IT, COMMpla CyberSecurity & Privacy Marketplace

4.2.11.1 Description, Architecture, and Subcomponents

The Marketplace (Figure 104) contains curated content sourced from completed EU-funded research projects, as well as products and services offered by providers across Europe. It is based on Drupal 7 CMS to organise and manage this content effectively.

The Marketplace features a user-friendly frontend interface accessible through web browsers. This interface allows users to browse, search, and interact with the content and functionalities of the platform. The Marketplace incorporates a user authentication system that allows users to create accounts and log in securely. Upon registration, users can manage their profiles, including personal information and preferences.

Users have the ability to create their own "Provider minisite" within the Marketplace. This feature enables providers to showcase their offerings, including products and services related to cybersecurity and privacy. The minisite creation process likely involves customizable templates or forms for adding information about the provider, its offerings, contact details, etc.

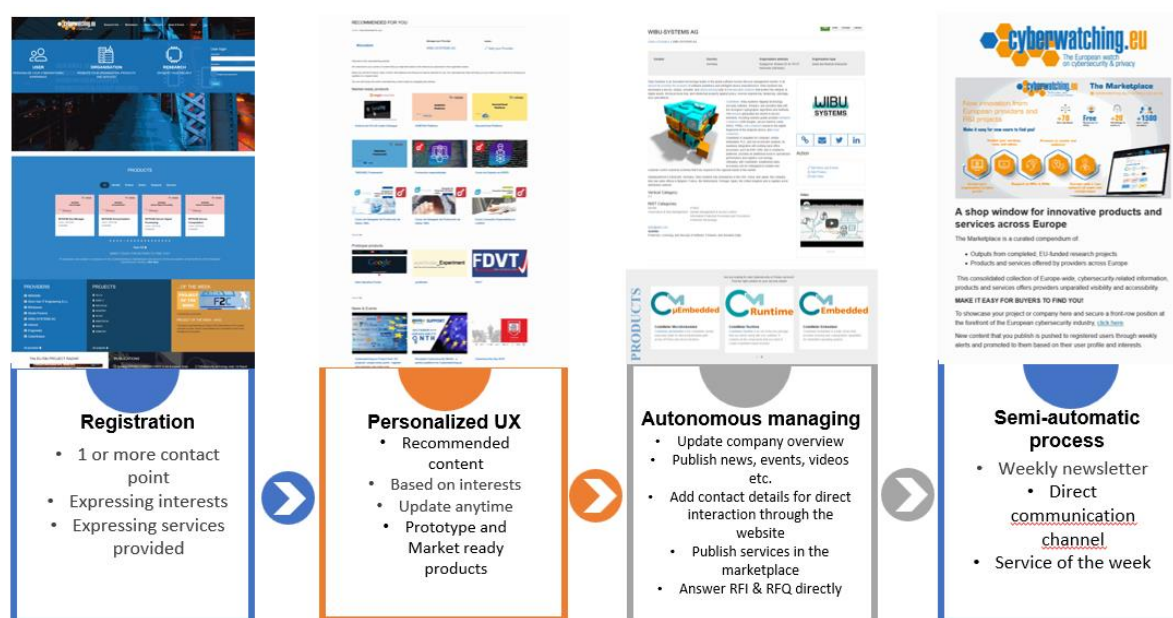


Figure 104: Cyberwatching Marketplace architecture.

4.2.11.2 Background Assets

Table 14 includes information about existing assets used within Cyberwatching Marketplace that have been identified to be modified or extended, and ultimately integrated during the development of the specific NERO tool.

Table 14: List of background assets used in Cyberwatching Marketplace.

Asset name	Description	Owner	Current TRL	License	Target TRL
Web Portal	Drupal based CMS with custom functionalities for R&I projects to autonomously manage and update their dedicated area.	Trust-IT	7	Proprietary Trust-IT	8

4.2.12 Montimage Anti-phishing Cyber Range

4.2.12.1 Description, Architecture, and Subcomponents

The Anti-Phishing Cyber Range Mobile Application is a pioneering educational tool designed to empower users with the knowledge and skills needed to combat phishing attacks effectively. With a focus on experiential learning, this innovative app provides users with a hands-on experience in identifying, analysing, and mitigating phishing threats directly from their mobile devices. By simulating real-world email scenarios, users gain practical insights into the tactics employed by cyber criminals and learn how to safeguard themselves against malicious activities. The Anti-Phishing Cyber Range Mobile Application offers a range of features aimed at enhancing users' digital resilience:

- **Email Simulation:** Users receive simulated emails, both legitimate and malicious, directly within the mobile app. These emails mirror real-world scenarios, providing users with a realistic experience in identifying potential phishing attempts.
- **Phishing Classification:** Users are tasked with classifying incoming emails as either legitimate or phishing attempts. By analysing the content, structure, and sender information, users learn to recognise common indicators of phishing and distinguish between genuine and malicious communications.
- **Explanation of Phishing:** For emails identified as phishing attempts, users are prompted to explain why they believe the email is fraudulent. This feature encourages critical thinking and helps users articulate the specific red flags and deceptive tactics present in the email.
- **Phishing Attack Classification:** Upon identifying a phishing email, users are prompted to classify the type of phishing attack it represents. Whether it's a traditional phishing scam, spear phishing, or a more sophisticated form of social engineering, users learn to categorise different types of phishing attacks based on their characteristics and objectives.

NERO Ecosystem

The app (Figure 105) provides access to educational resources, including tips, best practices, and real-world examples of phishing attacks. Through interactive tutorials and informative content, users deepen their understanding of phishing threats and learn how to protect themselves and their organisations effectively.

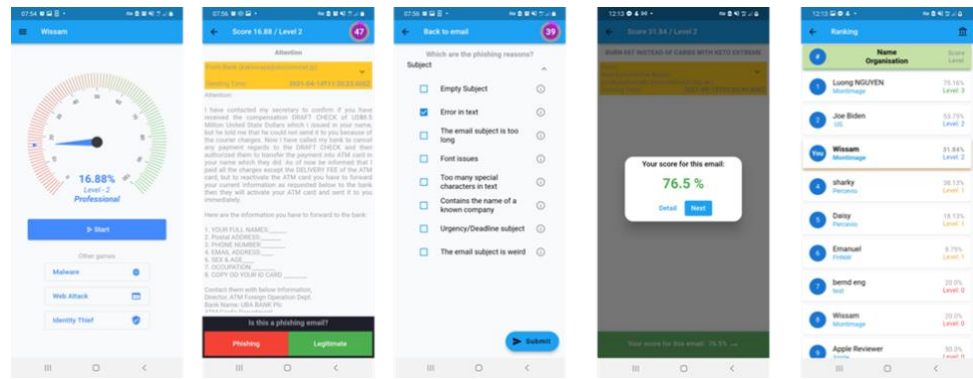


Figure 105: Anti-phishing cyber range screens.

The Anti-Phishing Cyber Range Mobile Application serves as a powerful tool for empowering users with the knowledge and skills needed to defend against phishing attacks. By offering a hands-on learning experience, users develop a heightened awareness of the tactics used by cyber criminals and learn how to respond appropriately to suspicious emails. Whether for individuals seeking to protect their personal information or organisations aiming to enhance their cybersecurity posture, this app provides a valuable resource for building digital resilience and mitigating the risks posed by phishing threats.

4.2.12.2 Background Assets

Table 15 includes information about existing assets used within Anti-phishing Cyber Range that have been identified to be modified or extended, and ultimately integrated during the development of the specific NERO tool.

Table 15: List of background used in Anti-phishing cyber range.

Asset name	Description	Owner	Current TRL	License	Target TRL
DART language	Google multi-platform language for mobile application	DART	9	Free	9

4.2.13 Montimage Cartimia Cyber Threat Intelligence (CTI)

4.2.13.1 Description, Architecture, and Subcomponents

CARTIMIA CTI is an innovative CTI service designed to provide organisations with unparalleled insights into network communications on the internet. By leveraging advanced analysis techniques and integrating data from various sources, CARTIMIA CTI offers a holistic view of communication routes, detects anomalies, and identifies newly malicious IPs in real-time. With its web-based interface and

intuitive functionality, CARTIMIA CTI equips organisations with the tools they need to enhance their cybersecurity posture and mitigate emerging threats effectively. Its key functionalities are:

- **Route Mapping Analysis:** CARTIMIA CTI specializes in analysing BGP (Border Gateway Protocol) announcements, traceroute data, and OSINT (Open Source Intelligence) to map the routes of communication on the web. By tracing the paths taken by data packets between source and destination, organizations gain valuable insights into the underlying infrastructure and potential vulnerabilities in their network communications.
- **Global Network View:** CARTIMIA CTI provides users with a comprehensive, global view of network communications on the internet. Through its intuitive interface, organisations can visualise the flow of data across different regions and understand the interconnected nature of the digital landscape. This global perspective enables organisations to identify potential points of compromise and proactively address security concerns.
- **Communication Analysis:** CARTIMIA CTI enables users to understand how communication is performed between a single source and destination. By analysing the flow of data packets, identifying intermediary nodes, and assessing the reliability of communication paths, organisations gain a deeper understanding of their network infrastructure and potential points of weakness.
- **Anomaly Detection:** Leveraging advanced algorithms and ML techniques, CARTIMIA CTI detects anomalies/breakdown in network communications in real-time. Whether it's unexpected deviations in communication routes or unusual patterns of data transmission, CARTIMIA CTI alerts users to potential security threats and enables prompt mitigation measures.
- **Malicious IP Detection:** CARTIMIA CTI actively monitors internet traffic to detect newly malicious IPs as they emerge. By analysing indicators of compromise and cross-referencing against threat intelligence feeds, CARTIMIA CTI identifies IPs associated with malicious activities such as malware distribution, phishing, or Distributed Denial of Service (DDoS) attacks. This proactive approach helps organizations stay ahead of evolving threats and protect their network infrastructure effectively.

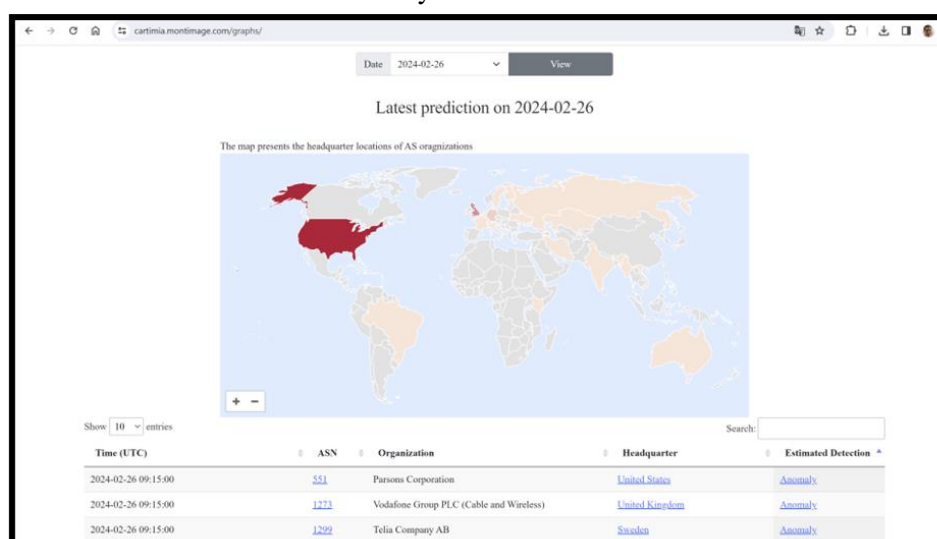


Figure 106: CARTIMIA CTI service Web site.

CARTIMIA CTI (Figure 106) is accessible through a user-friendly, web-based interface available at <https://cartimia.montimage.com/>. This platform offers seamless access to CARTIMIA CTI's powerful

analytical capabilities, allowing organisations to monitor network communications, detect anomalies, and respond to emerging threats from any device with internet connectivity. With its intuitive design and robust functionality, the web-based solution ensures organisations can leverage CARTIMIA CTI to enhance their cybersecurity posture with ease.

4.2.13.2 Background Assets

Table 16 includes information about existing assets used within CARTIMIA CTI that have been identified to be modified or extended, and ultimately integrated during the development of the specific NERO tool.

Table 16: List of background assets used in CARTIMIA CTI.

Asset name	Description	Owner	Current TRL	License	Target TRL
DART language	Google multi-platform language for mobile application	DART	9	Free	9

4.2.14 Montimage Network Fuzzer

4.2.14.1 Description, Architecture, and Subcomponents

The Montimage Network Fuzzer represents an innovative tool in the context of security testing, designed to identify vulnerabilities and assess the resilience of networked systems against malicious traffic. Built upon the foundation of the open-source software 5Greplay, this innovative solution empowers organisations to proactively defend against cyber threats by generating and mutating traffic to simulate potential attack scenarios (Figure 107). With its versatile capabilities and plugin architecture, the Montimage Network Fuzzer offers a comprehensive approach to fuzz testing that adapts to evolving network protocols and security requirements. It has the following features and functionalities.

- **Traffic Mutation:** At the core of the Montimage Network Fuzzer lies the ability to generate malicious traffic by mutating nominal traffic. Leveraging a combination of mutation functions, the Fuzzer alters the characteristics of benign network packets to simulate various attack vectors. This capability allows organizations to test the robustness of their network infrastructure and applications against potential threats in a controlled environment.
- **Fuzzing Techniques:** The Montimage Network Fuzzer offers flexibility in fuzzing techniques, enabling both random fuzzing and smart fuzzing using GANs that is still under development. Random fuzzing introduces randomness into the traffic generation process, while smart fuzzing leverages ML algorithms to intelligently manipulate packet payloads and structure. This combination of techniques enhances the effectiveness and efficiency of security testing, enabling organizations to uncover vulnerabilities with greater accuracy.
- **Protocol Support:** Building upon the foundation of 5Greplay, the Montimage Network Fuzzer already supports a wide range of protocols, including those specific to 5G networks. This comprehensive protocol support ensures that organizations can assess the security of their network infrastructure across diverse environments and technologies. Additionally, the Fuzzer's

NERO Ecosystem

plugin architecture allows for the seamless integration of additional protocols and fuzzing rules, ensuring compatibility with emerging standards and custom network configurations.

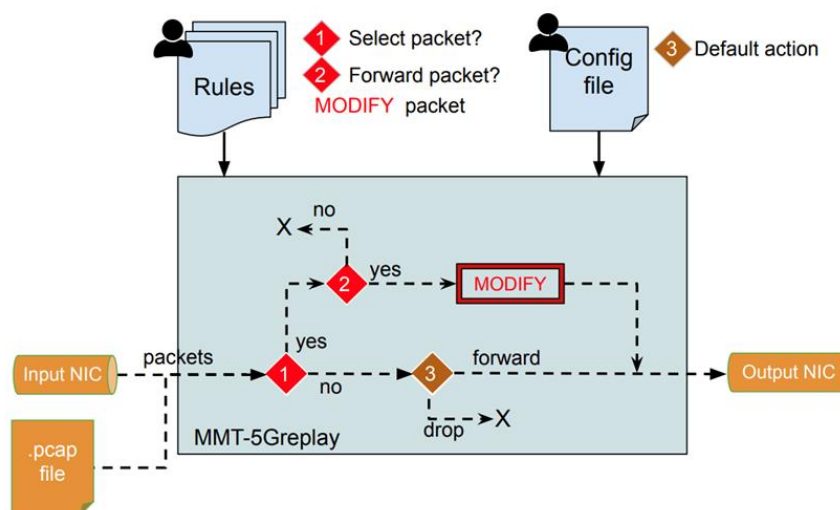


Figure 107: Montimage Network Fuzzer architecture.

In a context marked by ever-evolving cyber threats and complex network infrastructures, the Montimage Network Fuzzer emerges as a vital tool for organisations seeking to enhance their security posture. By leveraging advanced fuzzing techniques and protocol support, the Fuzzer enables organizations to simulate realistic attack scenarios and identify vulnerabilities proactively. With its plugin architecture and support for emerging technologies, the Montimage Network Fuzzer offers a future-proof solution for comprehensive security testing, empowering organizations to defend against cyber threats with confidence and resilience.

4.2.14.2 Background Assets

Table 17 includes information about existing assets used within Montimage Network Fuzzer that have been identified to be modified or extended, and ultimately integrated during the development of the specific NERO tool.

Table 17: List of background assets used in Montimage Network Fuzzer.

Asset name	Description	Owner	Current TRL	License	Target TRL
MMT-DPI	Engine to decode a protocol	MONT	7	Apache 2.0	9
5Greplay	5G network fuzzer	MONT	6	Apache 2.0	7

4.2.15 Sphynx Incident Response (SPH-IR)

4.2.15.1 Description, Architecture, and Subcomponents

The Sphynx Incident Response (IR) platform (Figure 108) is a system that enables the manual or automated execution of Collaborative Automated Course of Action Operations (CACAO) security

NERO Ecosystem

playbooks. The platform can be set up either as a standalone system or as a module (tool) integrated with the SPHYNX Security and Privacy Assurance Suite (SPA). As a standalone solution, the IR platform can import, export, and execute CACAO security playbooks triggered by a variety of third-party tools utilizing each playbook's REST API.

As a module of the SPA Suite, the IR platform can be used to execute security playbooks triggered by the SPA Suite's components, such as EVEREST and utilise information obtained by the Asset Model and the CTI component. Also, the IR platform can be used to orchestrate SPA Suite's components. The system offers a graphical drag-n-drop interface for creating and editing CACAO security playbooks, that can later be executed or exported as CACAO JSON files following the CACAO specification.

Finally, the IR platform offers an interactive dashboard that provides real-time views of the system's status and the execution of security playbooks along with high- and low-level logs, KPIs, user notification and other information.

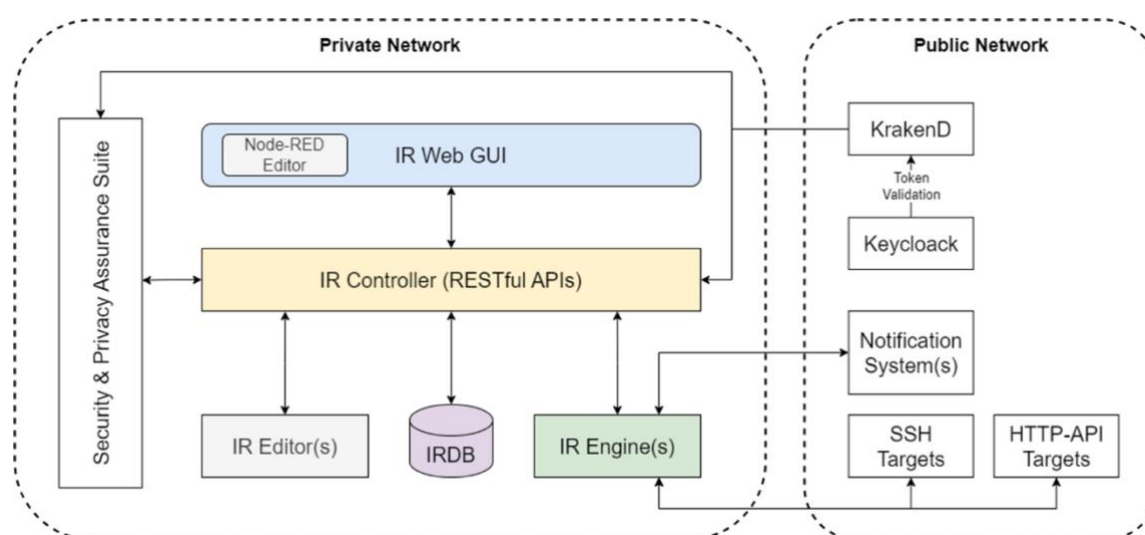


Figure 108: Sphynx Incident Response (IR) platform architecture.

Some of the IR key points are the following:

- Sphynx Incident Response (IR) platform is an organized approach to addressing and managing the aftermath of a security breach or cyber attack.
- The entire process is documented with files, usually using free text, called “playbooks” which can be shared across organizations.
- Playbooks provide graphs containing nodes that roughly map to executable actions.
- Incident response playbooks provided by most security agencies and organisations are not executable workflows.
- Industry solutions provide executable playbooks that are not free, opensource or interoperable between incident response tools.

CACAO (Figure 109) is a standard from OASIS Open that provides a comprehensive structure for implementing incident response playbooks. These playbooks are created as structured JSON objects, allowing for detailed and executable workflows that are essential for effective cybersecurity incident management. With the inclusion of various logic elements, such as loops, conditional statements, and

NERO Ecosystem

parallel execution, CACAO playbooks are versatile and powerful tools in responding to security incidents. They also come with metadata and relevant information about the incident they are designed to tackle, aiding in situational awareness and decision-making. As each incident response engine is tasked with parsing these playbooks, it ensures the smooth execution of the defined workflow. One of the key benefits of CACAO playbooks is their ability to address challenges related to the sharing and interoperability of incident response strategies, promoting a more unified and efficient approach to cybersecurity threats.

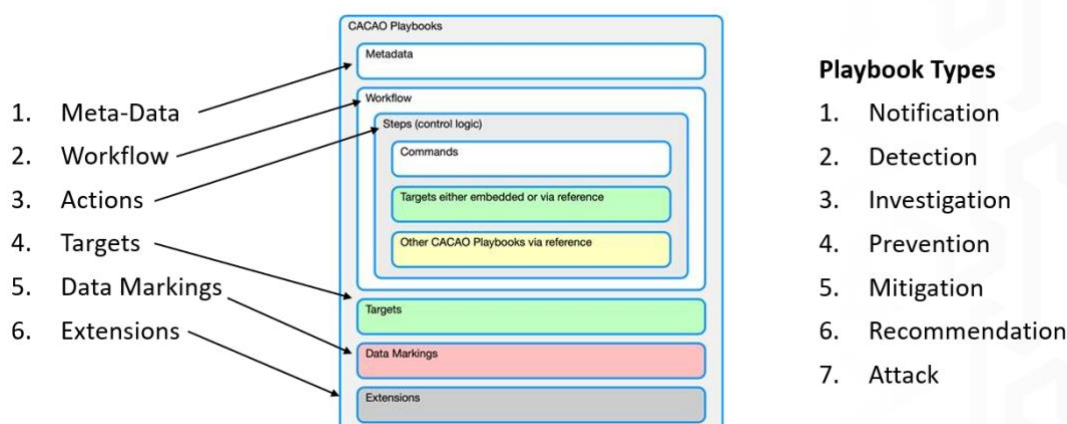


Figure 109: CACAO Playbooks.

Sphinx IR (Figure 110) stands out with its array of key features designed to streamline and empower the incident response process. It provides an intuitive graphical interface for the creation of CACAO playbooks through a drag-and-drop method, simplifying the development of complex workflows. Users can import, modify, and execute CACAO playbooks from third-party sources, like CTI feeds, enhancing collaboration and knowledge sharing. With its strict adherence to the OASIS-Open CACAO playbook specification, Sphinx IR ensures compliance and standardization in incident response activities. The system's integration with STS's SAP Suite, along with popular third-party applications such as The Hive and Slack, enables a seamless workflow within and across organisational tools. The flexibility of manual and automated playbook execution allows teams to respond to threats with the required immediacy. Command execution capabilities on both local and remote hosts provide comprehensive control over incident management tasks, and real-time monitoring of playbook executions offers immediate insights into the operational effectiveness of the incident response.

NERO Ecosystem

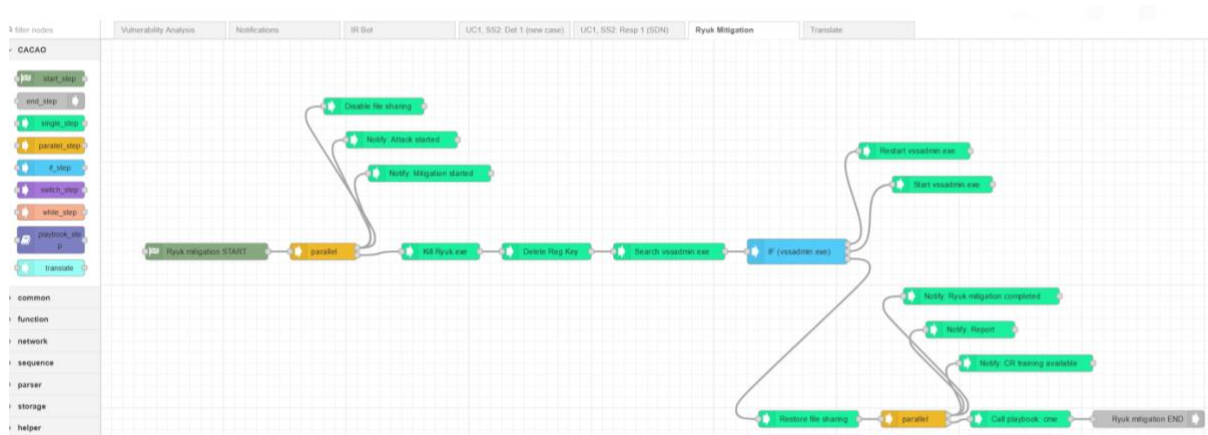


Figure 110: Sphynx IR key features.

4.2.15.2 Background Assets

Table 18 includes information about existing assets used within SPH-IR that have been identified to be modified or extended, and ultimately integrated during the development of the specific NERO tool.

Table 18: List of background assets used in SPH IR.

Asset name	Description	Owner	Current TRL	License	Target TRL
SPH-IR	Sphynx Incident Response (IR) platform	SPH	6	Proprietary	8

4.2.16 Sphynx Security and Privacy Assurance (SPH-SPA)

4.2.16.1 Description, Architecture, and Subcomponents

SPHYNX's Security and Privacy Assurance (SPA) suite is responsible for monitoring, testing, and assessing the security (& privacy, if needed) posture of the protected organisation(s) and their assets, in a real-time, continuous manner. Several built-in security assessments addressing the Confidentiality – Integrity – Availability (CIA) principles (via custom metrics that can be tailored concerning the platform's components) can be utilised, leveraging an evidence-based approach, to provide security assurance assessments with certifiable results. A high-level view of SPA's internal architecture is provided below in Figure 111:

NERO Ecosystem

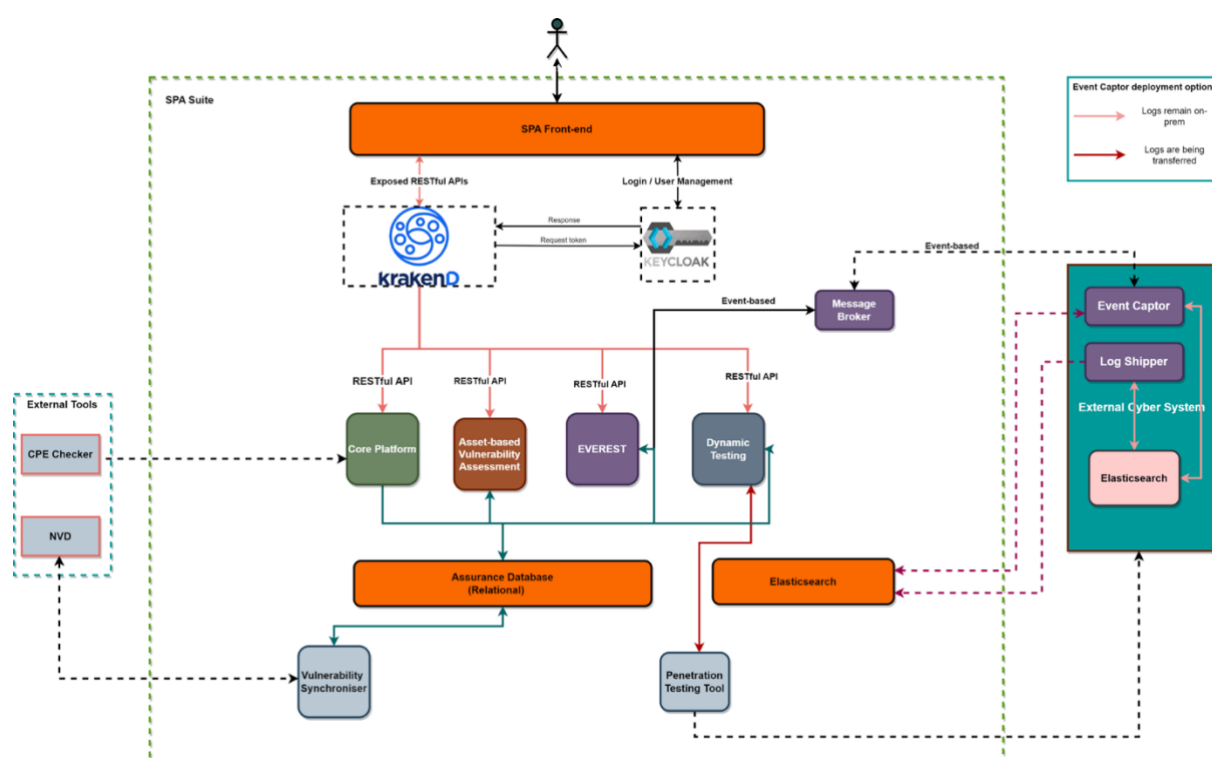


Figure 111: Security & Privacy Assurance platform (SPA) Architecture.

The SPA architecture is composed of six components: Core Platform, Asset-based vulnerability assessment, Dynamic Tester, Event REaSonIng Toolkit (EVEREST), Event Captors, and Security Component.

The Core Platform component is responsible for managing the asset and assessment model of an organisation. This component includes (a) the Asset Loader, and (b) the Assessment Loader. The former is responsible for maintaining the cyber system's asset model for the target organization. This model includes the organisation's assets, security properties for these assets, relations between assets in the model, and the security controls that protect the assets. This component provides the following ways to insert one or more assets. First, the user can utilise the SPA Suites' front end to insert one or more assets, through wizards. Secondly, the user can fill out a pre-structured Excel, and either utilise the front end to upload it or the exposed API. Lastly, the user can provide an SBOM (either in CycloneDX or SPDX format) and, again, make sure of the platform's front end or the corresponding REST API to insert the assets defined within it, in the system.

As for the Assessment Loader, it is the component responsible for handling the available assessments that the SPA Suite offers. More specifically, it provides means to manage the assessment (a) criteria, (b) profiles, (c) results, and (d) model executions.

The asset-based vulnerability assessment component is responsible for performing a passive vulnerability assessment to identify known vulnerabilities of assets defined within an organisation's asset model. This component supports two different kinds of vulnerability assessments. The former communicates with the core platform, receives the Common Platform Enumeration (CPE) of the assets within the assessment execution and then retrieves the relevant Common Vulnerabilities and Exposures entries, by searching in a local copy of the National Vulnerability Database (NVD, a U.S. government repository of standards-based vulnerability management data, maintained by the National Institute of Standards and Technology). This copy is continuously updated using an in-house component fetching the latest known CVEs. Following the execution of a vulnerability assessment, the tool will report

known vulnerabilities for those assets that have a valid CPE. The latter, communicates with the core platform, but instead of CPEs, it expects the pURLs per asset. Following, it makes use of Sonatype's [OSS index](#) to identify vulnerabilities on open-source systems.

The Dynabac Tester component is responsible for performing a passive vulnerability assessment to identify known vulnerabilities of assets defined within an organisation's asset model. This component supports two different kinds of vulnerability assessments. The former communicates with the core platform, receives the [CPE](#) of the assets within the assessment execution and then retrieves the relevant Common Vulnerabilities and Exposures entries, by searching in a local copy of the [NVD](#), a U.S. government repository of standards-based vulnerability management data, maintained by the National Institute of Standards and Technology. This copy is continuously updated using an in-house component fetching the latest known CVEs. Following the execution of a vulnerability assessment, the tool will report known vulnerabilities for those assets that have a valid CPE. The latter, communicates with the core platform, but instead of CPEs, it expects the pURLs per asset. Following, it makes use of Sonatype's [OSS index](#) to identify vulnerabilities on open-source systems.

The EVEREST component responsible for monitoring the target organisation, for potential issues within its cyber system. In its monitoring capacity, EVEREST possesses a multifaceted approach. It surveils the cyber system across a spectrum of crucial aspects, such as network traffic, potential threats from both internal and external sources, misconfiguration, and not properly installed security controls. By continuously evaluating events against defined rules expressed in Event Calculus and Drools, EVEREST can detect anomalies, deviations, and potential risks within the system. EVEREST works with the Event Captors to fetch the raw events from the cyber system.

An Event Captor is a tool that, based on a specification set by EVEREST, aggregates log and event information from the targeted infrastructure, and encapsulates it in a specific format that can be consumed by the EVEREST model. Logs and events can be collected in two modes. The former mode is based on the ELK solution. More specifically, [Elasticsearch](#) and some lightweight shippers (namely [Beat](#)) are utilised to forward and centralise log data. The latter makes use of SPHYNX's Native Event Captors, i.e., captors that cannot utilise the logging capabilities of the ELK stack. The needed Event Captors are initiated through EVEREST.

The Security component that provides Identity and Access Management capabilities, as well as, an API Gateway for exposing RESTful APIs (when needed). This component is comprised of two main components:

- Keycloak, which is used for identity and access management, and
- KrakenD, the API Gateway that handles authorization in conjunction with Keycloak.

More specifically, [Keycloak](#) is an open-source identity and access management platform that provides a single point of access for modern applications, APIs, and microservices. It offers features such as single sign-on, identity brokering, and social login, as well as robust user management and authentication capabilities. Following, [KrakenD](#) is a lightweight, high-performance API Gateway that helps expose internal and external microservices to the world, while keeping the complexity and routing logic out of core services. It allows one to easily build and deploy API Gateway configurations using a simple, declarative configuration file, and provides features such as rate limiting, circuit breaking, and caching to help manage the performance and reliability of your APIs.

4.2.16.2 Background Assets

Table 19 includes information about existing assets used within SPH-SPA that have been identified to be modified or extended, and ultimately integrated during the development of the specific NERO tool.

Table 19: List of background assets used in SPH SPA.

Asset name	Description	Owner	Current TRL	License	Target TRL
SPH-SPA	Security & Privacy Assurance platform	SPH	7	Proprietary	8

4.3 Tools Relation to NERO Ecosystem

Table 20 provides the NERO tools, their related task and deliverable, and partnering within which they correlate with the functions of the NERO framework. It also provides a mapping diagram with details showing the interrelationships among NERO functions, enhancing the project capability regarding identification, protection, detection, and response to cyber threats, and finally maps the partners involved in each tool.

Table 20: Tools Relation to NERO Ecosystem.

Tool Name	Owner	Related tasks	Related deliverables	Related NERO framework	Related framework function
HSPF	ONE	T2.4, T6.3, T6.4	D2.1, D2.2, D6.2, D6.3	CYBIT	Protect, Detect
M-HaaS	MINDS	T3.1, T3.2, T3.3, T6.1, T6.2, T6.3, T6.4	D3.1, D3.2, D6.1, D6.2, D6.3	CYBIT	Identify, Protect
M-RADAR	MINDS	T3.1, T3.2, T3.3, T6.1, T6.2, T6.3, T6.4	D3.1, D3.2, D6.1, D6.2, D6.3	CYBIT	Detect
MMT	MONT	T3.1, T3.2, T3.3, T6.1, T6.2, T6.3, T6.4	D3.1, D3.2, D6.1, D6.2, D6.3	CYBIT	Detect
KIOKU AI	MDS	T2.1, T2.2, T2.3, T2.4, T3.1, T3.2, T3.3, T5.1, T5.2, T5.3	D2.1, D2.2, D2.3, D2.4, D3.1, D3.2, D3.3, D5.1, D5.2, D5.3	ASTRAS	Cybersecurity Training, Cyberhygiene

NERO Ecosystem

SNYK	TRUSTILIO	T2.1, T2.2, T3.1, T4.3, T6.1, T6.2, T6.5	D4.1, D2.1, D6.1, D3.1, D3.2	VICTORIOUS, AUDACIOUS	Audit, Crowdsource Vulnerability Discovery and Disclosure
HRM	TRUSTILIO	T2.1, T2.2, T3.1, T4.3, T6.1, T6.2, T6.5	D4.1, D2.1, D6.1, D3.1, D3.2	VICTORIOUS, CYBIT, ARCANA	Audit, Crowdsource Vulnerability Discovery and Disclosure
Seer Box	PLUR	T3.3, T4.3	D3.1, D3.2, D4.1	AUDACIOUS	Application Security Testing Scans
ADR	MONT	T5.3	D5.1, D5.2, D5.3	ASTRAS	Identify, detect, react, protect
Cyberwiser Training Platform	Trust-IT, COMmpla	T5.1, T5.2, T5.3	D5.1, D5.2, D5.3	ASTRAS	Gamification- based Training
Cyberwatching Marketplace	Trust-IT, COMMpla	T3.3	D3.1, D3.2	ARCANA	Marketplace
Anti-phishing Cyber Range	MONT	T5.3	D5.1, D5.2, D5.3	ASTRAS	Identify, detect, react, protect
CARTIMIA CTI service	MONT	T3.1, T3.2, T3.3, T6.1, T6.2, T6.3, T6.4	D3.1, D3.2, D6.1, D6.2, D6.3	CYBIT	Identify
Montimage Network Fuzzer	MONT	T3.1, T3.2, T3.3, T6.1, T6.2, T6.3, T6.4	D3.1, D3.2, D6.1, D6.2, D6.3	CYBIT	Detect
SPH-IR	SPH	T3.1, T3.2, T3.3, T5.1, T5.2, T5.3	D3.1, D3.2, D5.1, D5.2, D5.3	CYBIT	Response, Recover
SPH-SPA	SPH	T3.1, T3.2, T3.3, T5.1, T5.2, T5.3	D3.1, D3.2, D5.1, D5.2, D5.3	CYBIT	Response, Recover, Identify, Protect

5 Use Cases Definitions

This section aims to detail specific use cases where the NERO Ecosystem can significantly benefit SMEs.

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

5.1.1 UC1 Description

UC1 is focused on enhancing patient data security in healthcare through cybersecurity tools, aiming to demonstrate the applicability, flexibility, and value of the NERO ecosystem to healthcare organisations spanning from small hospitals and larger healthcare centers to diagnostic labs and small clinics.

Furthermore, the enhancement of patient data security, through the exploitation of adequate cybersecurity tools, is of great importance. Keeping in mind the increasing digitization of medical records and the reliance on electronic health systems, the protection of sensitive patient information from cyber threats is critical in order to ensure patient privacy, maintain trust in healthcare institutions, and also comply with privacy regulations. By implementing robust cybersecurity measures, healthcare organisations can mitigate the risk of data breaches, prevent unauthorized access to patient records, and uphold the integrity and confidentiality of medical information. Ultimately, prioritising patient data security not only protects individuals' sensitive information but also fosters a safer and more resilient healthcare ecosystem for all stakeholders involved.

Taking all the above under consideration, we argue that the added value of the particular use case extends beyond mere risk mitigation. It embraces leveraged patient trust, compliance with privacy regulations, operational efficiency and finally better health care delivery.

Additionally, in the current landscape of healthcare data management, numerous challenges related to data security exist. Despite advancements in technology, vulnerabilities to sophisticated cyber threats and unauthorised access attempts are frequent. Weaknesses in security protocols and outdated software leave patient data fragile to breaches, posing significant risks to confidentiality and integrity. Furthermore, the systems' reliance on interconnected networks intensifies the complexity of cybersecurity defence measures.

5.1.2 System Architecture and Assets Identification

The diagram in Figure 112 depicts the ecosystem of a healthcare system tailored to a specific use case, highlighting the intricate interactions between the core infrastructure and its associated stakeholders. Within this context, the main core system, comprising 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 comprehensive network illustrates the tailored integration necessary to support the targeted healthcare use case, encompassing patient care, data exchange, research collaboration, and financial transactions within its operational scope.

Use Cases Definitions

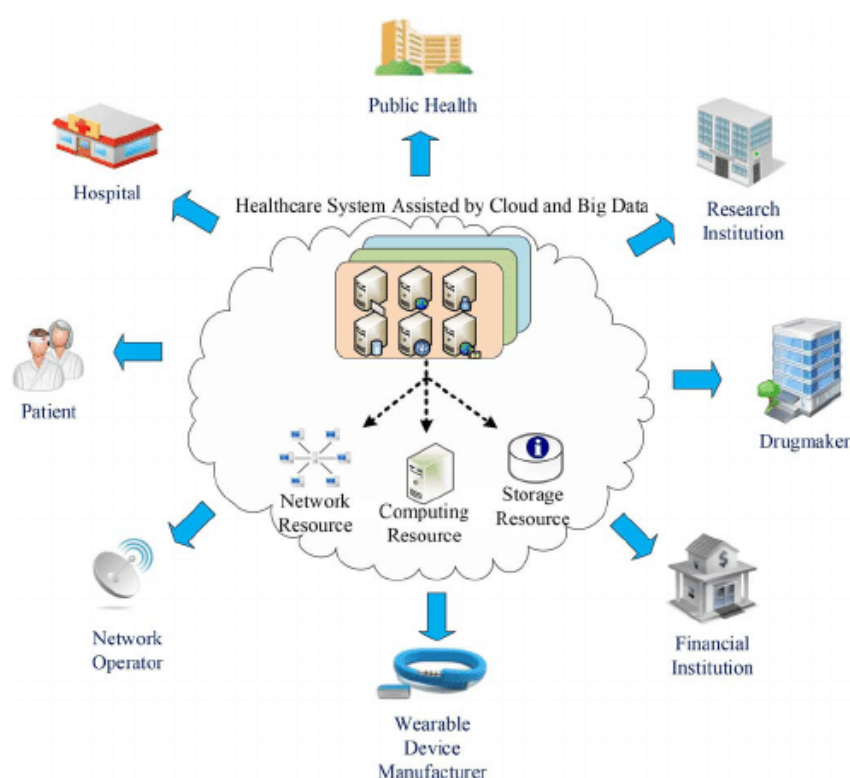


Figure 112: UC1 Healthcare Interactions.

The diagram in Figure 113 presents a comprehensive process for enhancing cybersecurity within healthcare small and medium enterprises (HSMEs), starting with an assessment of an HSME's visions, needs, current capabilities, and existing state. Subsequently, the gathered information or data is carefully and thoroughly assessed encompassing compliance with privacy regulations, threat and risk analysis, and gap analysis. This data is then channelled through the ARCANA and CYBIT frameworks, with the deployment of cybersecurity tools provided by the partners involved. These tools, including network monitoring, code auditing, IDS, risk management, and incidence response plans, collectively fortify the system against potential threats. In the end, the primary goals include safeguarding medical and healthcare personal data, improving operational efficiency, and fostering trust throughout the healthcare ecosystem.

Use Cases Definitions

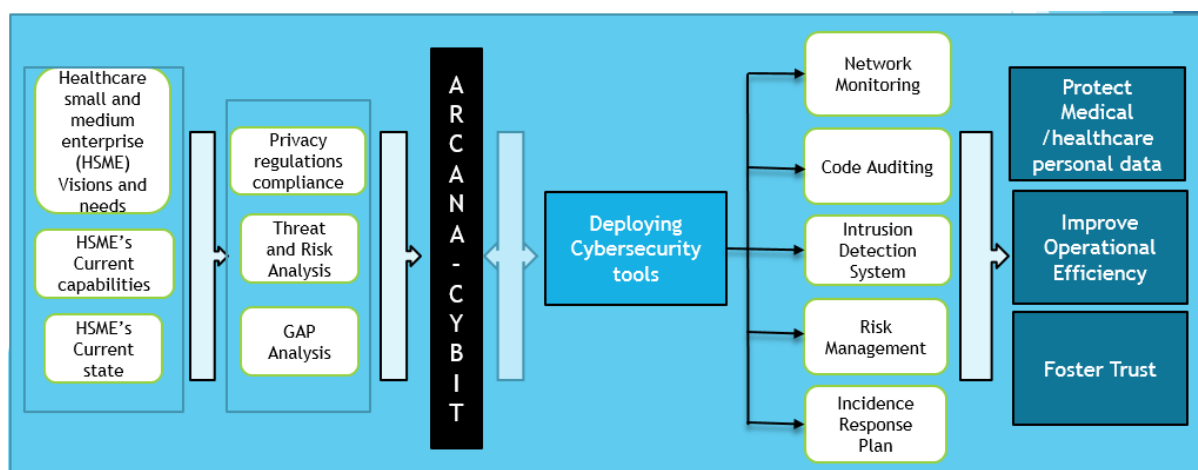


Figure 113: UC1 system architecture diagram 1.

The diagram in Figure 114 illustrates the system architecture of a healthcare HSME facilities, each featuring two distinct networks interconnected with a central database (DB). Within each facility, a server and client computers form individual networks, facilitating internal communication and data exchange. Notably, these networks are interconnected, ensuring seamless connectivity between HSME facilities, even if they are geographically distant. This interconnectedness underscores the importance of efficient communication and data sharing across the HSME network infrastructure, enabling collaborative operations and centralised data management. Additionally, within the current use case robust cybersecurity measures are meant to be implemented to safeguard sensitive medical information and ensure the integrity and confidentiality of data transmitted across the interconnected network.

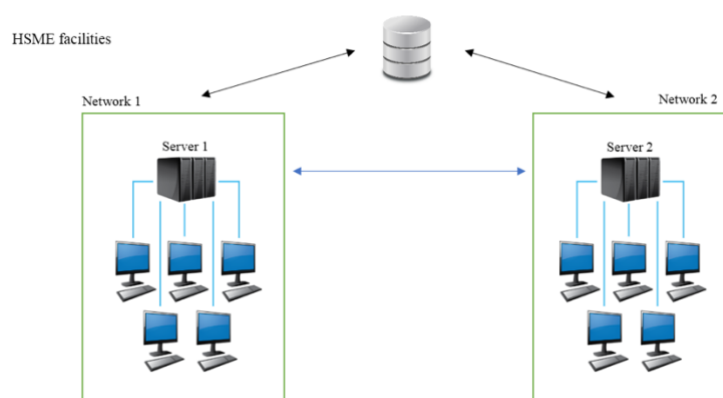


Figure 114: UC1 System Architecture Diagram 2.

The subsequent Table 21 provides a comprehensive breakdown of the assets associated with the first use case. It includes asset names, descriptions, the types of data processed by each asset, and their respective criticality levels.

Table 21: UC1 assets description.

Asset Name	Description	Data processed by the asset	Criticality
End-users	Healthcare personnel (e.g., doctors, nurses,	Patient and healthcare personnel personal	Medium/High

Use Cases Definitions

	administrators) that uses the PC's	data depending on user account	
Server admin	Person that has full access on the Server systems	All the facilities data	High
DB- Database	An electronically stored collection of data	Includes all the healthcare data	High
Server	Computer of system which provides resources, medical data, healthcare services of programs	All the facilities data	High
Network	A system of Interconnected PC's	All the facilities data	High

5.1.3 Scenarios Definition

The following Table 22, Table 23, and Table 24 present the scenarios definition for the first use case. They include a detailed description, assumptions and pre-conditions, the use case goal, involved actors, scenario initiation, main flow of events, and evaluation criteria such as related Key Performance Indicators (KPIs).

Table 22: UC1 - Scenario 1 (SC1.1).

Scenario name	Health data exchange between different healthcare entities
Description	An HSME which has separate facilities, is vulnerable to various types of cyber attacks, namely insider threats, data breaches, phishing attacks etc. The aim is ensuring that all the patient, staff and medical data are secure.
Assumptions & Pre-Conditions	Interoperability, User education, Threat evolution
Goal (Successful End Condition)	Prevent data breaches, minimising the risk, comply with regulations, increase confidence, minimise the financial, legal and reputational risks, secure patient/healthcare stakeholders' information.
Involved Actors	Doctors, patients, nurses, healthcare personnel, admins, systems technicians.
Scenario Initiation	To be defined
Main Flow	<ol style="list-style-type: none"> Utilisation: In this step, system admins and technicians identify the HSME's systems interaction and the involved actors. This is essentially understanding how different components of the system interact with each other and with users or other external entities. Cartography Phase: Here, system admins and technicians develop relevant asset and user models, along with anonymous HRM profiles of the ICT system under assessment. This involves mapping out the assets (such as hardware,

Use Cases Definitions

	<p>software, data) and users (employees, customers, etc.) within the system, as well as creating profiles to understand their potential impact on security.</p> <p>3. Risk Assessment Phase: This phase involves conducting a risk assessment using tools like the ENISA RM Toolbox or the OWASP tool. The steps include:</p> <p>4. Identifying threats: Recognising potential risks and vulnerabilities to the system.</p> <ul style="list-style-type: none"> ○ Estimating threat levels: Assessing the likelihood and severity of these threats. ○ Estimating vulnerability and impact levels: Understanding the weaknesses in the system and the potential consequences of exploitation. ○ Proposing technical and social countermeasures: Suggesting both technical (e.g., software patches, encryption) and social (e.g., training, policies) measures to mitigate risks. <p>5. Risk Management Phase: Finally, system admins prioritise vulnerabilities based on the assessment and implement countermeasures. This involves addressing the most critical risks first and taking steps to reduce their likelihood or impact.</p>
Evaluation Criteria – Related KPIs	<p>1. Enhance Cybersecurity Awareness and Prevention</p> <ul style="list-style-type: none"> • KPI: Security Training Completion Rate > 80% <p>2. Improve Incident Response Efficiency</p> <ul style="list-style-type: none"> • KPI: Reported Incident Response Rate Increase by >20% <p>3. Ensure Employee Training Across Companies</p> <ul style="list-style-type: none"> • KPI: Training of >200 employees from >40 SMEs and >5 large healthcare companies within 2 years post-project completion

Table 23: UC1 - Scenario 2 (SC1.2).

Scenario name	Software code audit for Healthcare Entities
Description	A healthcare entity (hospital, clinic, diagnostic centre, medical IT company) is evaluating a new software for managing patient records. Before purchasing the software, the hospital needs to ensure that its code is secure. This is achieved by conducting a code audit.
Assumptions & Pre-Conditions	The healthcare entity (hospital, clinic, diagnostic centre, medical IT company) has found a software that meets its operational needs and is accessible for a code audit.

Use Cases Definitions

Goal (Successful End Condition)	The goal is to conduct a successful audit of the software's code with Snyk through NERO. At the same time, the healthcare entity needs to confirm that the code meets its security standards and it needs to decide whether to proceed with the purchase.
Involved Actors	<ol style="list-style-type: none"> 1. Software Development Company IT department: Develops the medical services/ applications and is responsible for conducting code audits for vulnerabilities/compliance with standards quality. 2. Software Development Company: It provides the software and any necessary documentation or support for the audit. 3. Healthcare entity IT Department: It is responsible for conducting additional audit in case needed.
Scenario Initiation	At the beginning of the scenario, the healthcare entity distinguishes/ selects a specific software and then proceeds to a potential purchase. Meanwhile, it decides to conduct a code audit to evaluate the software.
Main Flow	<ol style="list-style-type: none"> 1. Integration Setup: Configure Snyk to work with the software's code repository. 2. Audit Execution: Use Snyk to audit the software's code, identifying vulnerabilities or issues. 3. Results Analysis: Analyse audit findings to assess risks, possibly with the assistance of a security consultant. 4. Planning: Prioritise vulnerabilities based on their severity. 5. Remediation Phase: Collaboratively address identified vulnerabilities between the IT department and software developers. 6. Re-Audit Execution: Re-audit the software's code using Snyk to ensure identified vulnerabilities have been resolved.
Evaluation Criteria – Related KPIs	<ol style="list-style-type: none"> 1. Improve Incident Response Efficiency <ul style="list-style-type: none"> • KPI: Reported Incident Response Rate Increase by >20% 2. Ensure Employee Training Across Companies <ul style="list-style-type: none"> • KPI: Training of >200 employees from >40 SMEs and >5 large healthcare companies within 2 years post-project completion

Table 24: UC1 - Scenario 1 (SC1.3).

Scenario name	Vulnerability Detection in Healthcare Software Code
Description	An SME developing software for the healthcare sector aims to proactively identify and address vulnerabilities. Additionally, in the case of the

Use Cases Definitions

	development of medical services/ applications the code must be checked for compliance with standards quality.
Assumptions & Pre-Conditions	The SME has healthcare software projects that require security assessments.
Goal (Successful End Condition)	The goal is to effectively identify all critical and high vulnerabilities in the healthcare software's code.
Involved Actors	<ol style="list-style-type: none"> 1. Development Team: The team is responsible for the software's creation and for fixing any vulnerabilities. 2. Project Managers: Project managers set the project timelines and ensure security auditing is integrated into the development lifecycle without causing any delays.
Scenario Initiation	The scenario begins when the SME decides to integrate Snyk into its software development lifecycle to enhance the security of its healthcare software.
Main Flow	<ol style="list-style-type: none"> 1. Integration Setup: Configure Snyk to work with the development environment and the software's code repository. 2. Initial Scan: Perform the first vulnerability scan on the existing code. 3. Analysis of Findings: Review Snyk's report to identify critical and high vulnerabilities. 4. Planning: Prioritize vulnerabilities based on their severity. 5. Remediation Phase: Developers address the identified vulnerabilities according to the plan. 6. Re-assessment: Conduct scans with Snyk to ensure all vulnerabilities are resolved and verify no new ones have been introduced.
Evaluation Criteria – Related KPIs	<ol style="list-style-type: none"> 1. Enhance Cybersecurity Awareness and Prevention <ul style="list-style-type: none"> • KPI: Security Training Completion Rate > 80% 2. Improve Incident Response Efficiency <ul style="list-style-type: none"> • KPI: Reported Incident Response Rate Increase by >20% 3. Ensure Employee Training Across Companies <ul style="list-style-type: none"> • KPI: Training of >200 employees from >40 SMEs and >5 large healthcare companies within 2 years post-project completion

5.1.4 NERO frameworks and tools to be validated

The following Table 25 presents the list of the NERO frameworks and tools slated for validation. It includes details such as the tool name, collaborating entity, assigned role, and associated NERO framework. This comprehensive compilation ensures a structured approach to the validation process.

Table 25: UC1 Frameworks and Tools to be validated.

Tool	Partner	Role	NERO framework
SNYK	TRUSTILIO	Detect and treat code vulnerabilities	VICTORIOUS, AUDACIOUS
HRM	TRUSTILIO	Risk assessment and security management package	ARCANA, CYBIT
Seer box	PLUR	Web Application Security Manager	AUDACIOUS
HSPF	ONE	Attack identification through anomaly detection	CYBIT
Cyberwiser.eu training platform	TRUST-IT	Contribute to the training planning in WP5	ASTRAS
VitalCheck Urinesensor - Sensor	SHG	Collecting data from various sources (blood sample results, lab test results, etc.) to be used in an algorithm for diagnostic purposes.	CYBIT
MMT	MONT	Intrusion detection and response based on ML behaviour analysis and multi-source data capture.	ASTRAS, CYBIT
MI Cyberrange	MONT	Anti-phishing training game	ASTRAS

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

5.2.1 UC2 Description

UC2 is focused on strengthening supply chain resilience through cybersecurity awareness in the transportation and logistics industry. More precisely, the NERO Ecosystem will be evaluated in maritime logistics domain which involves shipping companies, port authorities, maritime infrastructure,

Use Cases Definitions

supply chain managers, vessel operators and maritime cybersecurity service providers, aiming to validate NERO's adaptability to different domains.

The deployment of the NERO cybersecurity framework within maritime logistics represents a transformative stride towards securing the sector's sprawling and interconnected digital landscape. Amidst escalating cyber threats that perilously hover over global trade's lifelines, NERO emerges not merely as a defensive mechanism but as a strategic bulwark designed to shield, detect, and counteract cybersecurity risks endemic to maritime operations.

At the heart of NERO's deployment in maritime logistics is the seamless integration of its specialised modules: VICTORIOUS, AUDACIOUS, CYBIT, ARCANA, and ASTRAS. Each component, meticulously tailored to address specific security challenges, converges to create a fortified cybersecurity posture that extends across the entire maritime logistics spectrum.

In a bustling port where thousands of containers are moved daily, the Maritime Logistics Company (MLC) faces a critical challenge: protecting sensitive data against cyber threats. Insider threats, data breaches, and phishing attacks threaten to disrupt operations and compromise the safety and confidentiality of cargo and crew information. Recognizing these risks, MLC turns to the NERO cybersecurity framework as its solution.

MLC manages vast amounts of sensitive data critical for day-to-day operations—details about cargo contents, crew schedules, and port operations. This information, if leaked or tampered with due to a cyber attack, could lead to significant financial losses, legal issues, and damage to MLC's reputation. MLC implements NERO, a comprehensive cybersecurity framework, focusing on protecting, detecting, and responding to cyber threats. NERO's approach is threefold, Protecting Sensitive Data, Detecting Threats in Real Time, Responding to Incidents.

Specifically, NERO integrates advanced encryption algorithms and multi-factor authentication to protect the transmission and storage of critical data, including cargo details, crew schedules, and operational logistics. This ensures that sensitive information remains inaccessible to unauthorised users and resilient against manipulation.

Real-time monitoring and threat detection systems, part of NERO's core capabilities, continuously scan for anomalies and signs of cyber intrusion, leveraging AI and ML for enhanced precision. This vigilant oversight permits MLC to identify and neutralise threats promptly, preventing potential disruptions to its operations. Furthermore, the comprehensive incident response strategy empowered by NERO enables MLC to swiftly isolate and address security breaches, minimising impact and facilitating rapid recovery.

This robust cybersecurity framework not only preserves the integrity of MLC's operational processes but also fortifies the trust among its network of partners, customers, and regulatory bodies. By demonstrating a proactive and technologically advanced approach to cybersecurity, MLC highlights its dedication to safeguarding the critical infrastructure that underpins the seamless flow of international trade, thereby reinforcing its reputation as a secure and reliable link in the global supply chain. Through NERO, MLC has not just enhanced its security measures but has also set a new benchmark for cybersecurity excellence in the maritime logistics sector.

Furthermore, the initiative to plan new logistics operations underlines the imperative need for robust cybersecurity measures. NERO's framework ensures interoperability among diverse logistics systems, comprehensive cybersecurity education for all users, and a proactive stance towards evolving maritime

Use Cases Definitions

threats. These elements are crucial for creating a fortified digital environment where operations can proceed unhindered by the spectre of cyber threats.

In essence, the NERO framework sets a new standard for cybersecurity in maritime logistics. Through rigorous system audits, targeted cybersecurity training, advanced authentication mechanisms, and continuous vigilance, NERO encapsulates the maritime sector's commitment to cybersecurity excellence. Its strategic deployment transcends traditional security measures, embodying a holistic and dynamic approach to safeguarding the maritime logistics sector against the turbulent seas of cyber threats, thus ensuring the safe and secure exchange of information vital to the arteries of global trade.

5.2.2 System Architecture and Assets Identification

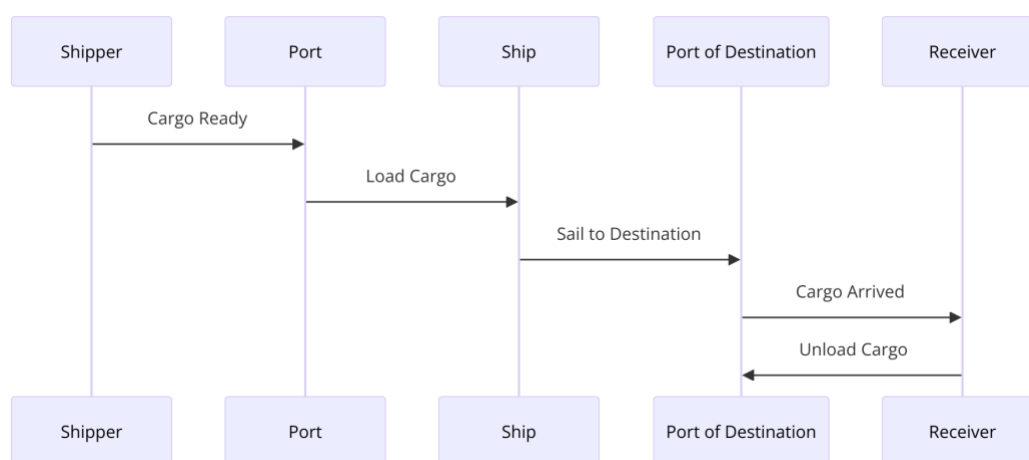


Figure 115: UC2 Maritime logistics interaction.

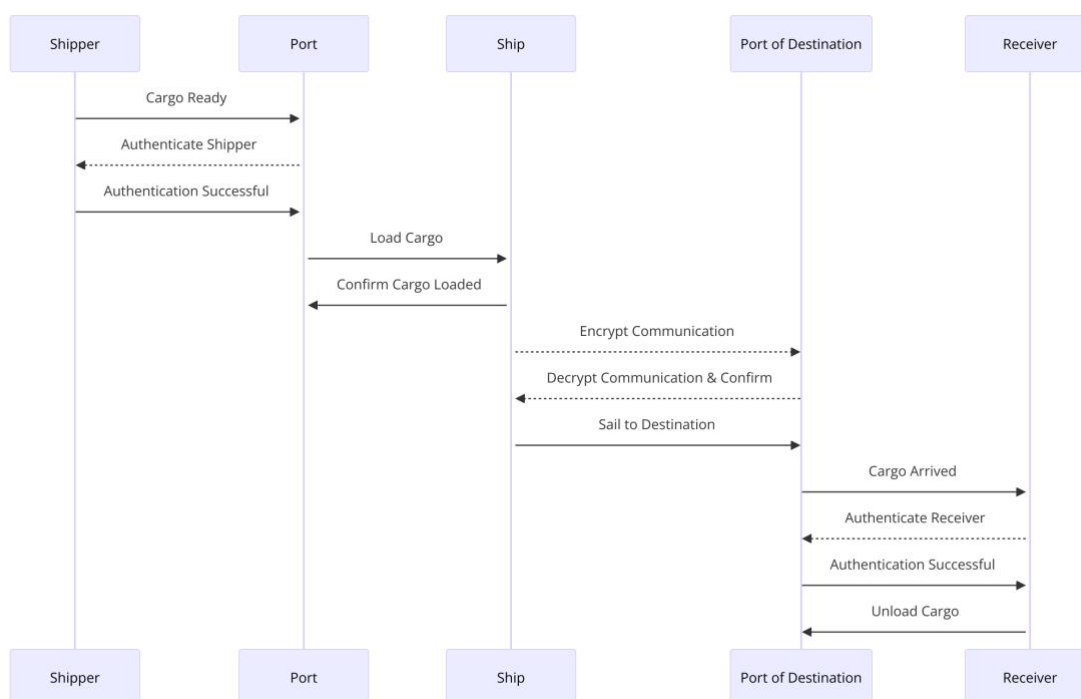


Figure 116: UC2 Maritime logistics interactions with authentication mechanism.

Use Cases Definitions

Maritime logistics (Figure 115, Figure 116) a vital artery for global trade, faces unique cybersecurity challenges due to its diverse and international nature. The NERO Framework, designed to fortify cybersecurity defences in this sector, offers a comprehensive approach through its distinct components: VICTORIOUS, AUDACIOUS, CYBIT, ARCANA, and ASTRAS. Each component targets specific aspects of cybersecurity, from bug bounty programs to gamification-based training, catering to the nuanced needs of maritime logistics stakeholders.

For instance, a shipping company, leveraging the VICTORIOUS module, initiates a Bug Bounty Program to unearth vulnerabilities within its IT infrastructure. This proactive measure not only enhances the security posture but also engages the cybersecurity community in a collaborative effort to safeguard critical maritime operations. Concurrently, port authorities adopt the AUDACIOUS module to audit resilience mechanisms and conduct thorough application security testing scans, ensuring the robustness of their digital and physical assets against evolving cyber threats.

Another scenario can be a comprehensive threat analysis using the CYBIT module, focusing on identifying, protecting, detecting, responding to, and recovering from cybersecurity incidents. This step is crucial for maritime logistics entities that manage sensitive data, including cargo information and shipping schedules, stored in centralized databases and servers. By deploying advanced authentication mechanisms, such as Multi-Factor Authentication and Biometric Verification, alongside robust access control measures, the integrity and confidentiality of this data are preserved.

Furthermore, the integration of ARCANA and ASTRAS modules facilitates the deployment of cybersecurity tools and the enhancement of personnel's cybersecurity awareness through gamified training environments. These measures not only fortify the cybersecurity infrastructure but also cultivate a security-aware culture among individuals who interact daily with logistics systems, from logistics managers to dock workers. The following diagram (Figure 117) represents the overall architecture of the second use case as mentioned above.



Figure 117: UC2 system architecture.

The subsequent Table 26 provides a comprehensive breakdown of the assets associated with the second use case. It includes asset names, descriptions, the types of data processed by each asset, and their respective criticality levels

Use Cases Definitions

Table 26: UC2 Asset Description.

Asset Name	Description	Data Processed by the asset	Criticality
End-users	Individuals who interact with the logistics systems, such as logistics managers, shipping company personnel, and dock workers.	They process information through inputs and queries and may execute tasks based on the information received.	Medium/High
Server admin	Person that has full access on the Server systems	All the facilities data	Very High
DB- Database	An electronically stored collection of data	Stores and retrieves critical data related to cargo, shipping schedules, manifests, and tracking information.	Very High
Server	A computer or computer program that manages access to a centralised resource or service in a network	All the facilities data	Very High
Network	A system of Interconnected PC's	Transmits data and connects various assets within the maritime logistics framework, such as terminals, cargo ships, and ports	High
Security Systems	Comprises both cyber and physical security measures used to protect the assets from threats.	Monitors for threats and unauthorised activity, manages access control, and maintains integrity of the logistics chain.	Very High
Cargo Handling Systems	Mechanical and software systems used for the movement of cargo in ports and on ships.	Manage the physical movement, tracking, and storage of cargo.	Medium

Use Cases Definitions

Communication Systems	Systems used for the exchange of information between ships, ports, and logistics operators.	Handles operational commands, navigational data, and emergency communications.	Medium/High
Supply Chain Management Software	Software tools used to oversee and manage supply chain transactions and processes.	Manages orders, inventory, supply and demand forecasting, and vendor relationships.	Medium/High
Automated Identification Systems (AIS)	An automatic tracking system used on ships and by vessel traffic services for identifying and locating vessels.	Processes vessel information, such as identification, position, course, and speed.	Medium/High

5.2.3 Scenarios Definition

The following Table 27 and Table 28 present the scenarios definition for the first use case. They include a detailed description, assumptions and pre-conditions, the use case goal, involved actors, scenario initiation, main flow of events, and evaluation criteria such as related KPIs.

Table 27: UC2 - Scenario 1 (SC2.1).

Scenario name	Strengthening Cybersecurity Measures in maritime logistics company
Description	In this scenario, the maritime logistics entity undertakes a proactive approach to bolster its cybersecurity defences. Beginning with a thorough assessment of existing measures, vulnerabilities are identified and targeted training sessions are initiated to elevate awareness and establish best practices among personnel. Advanced authentication mechanisms are then deployed to tightly control access to sensitive data, ensuring only authorised individuals can exchange information. Continuous monitoring systems are implemented to detect potential threats in real-time, allowing for prompt response and ongoing improvements based on evolving cybersecurity landscapes. Through these measures, the entity establishes a robust cybersecurity framework, safeguarding critical operations and maintaining confidence in the secure exchange of information within the maritime logistics network.
Assumptions & Pre-Conditions	Personnel Engagement, Resource Availability

Use Cases Definitions

Goal (Successful End Condition)	Prevent data breaches, minimise risks, comply with maritime regulations, increase stakeholder confidence, and minimise financial, legal, and reputational risks while securing sensitive maritime data.
Involved Actors	Shipping company personnel, dock workers, logistics managers, port administrators, systems technicians, customs officers.
Scenario Initiation	The scenario begins with the maritime logistics entity recognising the critical importance of fortifying its cybersecurity measures in light of the sensitive information it manages and the potential consequences of compromised data. Concerns over insider threats, data breaches, and sophisticated phishing attacks prompt the entity to prioritise the secure exchange of information as its primary objective, setting the stage for a proactive approach to enhancing cybersecurity within its operations.
Main Flow	<ol style="list-style-type: none"> 1. Assessment of Current Cybersecurity Measures: Conduct an extensive audit of existing cybersecurity measures and systems interoperability and identify vulnerabilities and areas for enhancement in the current infrastructure. 2. Controlled Attacks Execution. Different cyber attacks will be investigated and will be conducted against certain devices in the network in a controlled environment. 3. Cybersecurity Training Sessions: Roll out targeted cybersecurity training sessions for all personnel involved in the logistics operation and elevate awareness and establish best practices to mitigate insider threats, data breaches, and phishing attacks. 4. Implementation of Advanced Authentication Mechanisms: Deploy advanced authentication mechanisms to strictly control and monitor access to sensitive data and ensure that only authorised personnel can access and exchange sensitive information. 5. Continuous Monitoring and Improvement: Implement robust monitoring systems to continuously assess cybersecurity posture and detect any potential threats or unauthorised access and regularly update and enhance cybersecurity measures based on evolving threats and industry best practices.
Evaluation Criteria – Related KPIs	<ol style="list-style-type: none"> 1. Increased Resilience and Cybersecurity <ul style="list-style-type: none"> KPI: Threat Detection Rate >90% 2. Enhanced Monitoring and Identification of Threats <ul style="list-style-type: none"> KPI: Vulnerability Management >25/year 3. Ensure Employee Training Across Companies

Use Cases Definitions

	<ul style="list-style-type: none"> • KPI: Training of >200 employees from >40 SMEs and >5 large companies in the maritime sector companies within 2 years post-project completion • KPI: Lessons Learnt >10
--	---

Table 28: UC2 - Scenario 2 (SC2.2)

Scenario name	Enhancing Interoperability and Data Exchange
Description	A maritime logistics entity operating across multiple locations and jurisdictions is vulnerable to various types of cyber attacks, including insider threats, data breaches, phishing attacks, and more. The goal is to ensure that all data related to cargo, crew, port operations, and logistics are secure.
Assumptions & Pre-Conditions	Interoperability between different logistics systems, education of all users in cybersecurity best practices, evolution of threats in the maritime sector.
Goal (Successful End Condition)	Prevent data breaches, minimize risks, comply with maritime regulations, increase stakeholder confidence, and minimise financial, legal, and reputational risks while securing sensitive maritime data.
Involved Actors	Shipping company personnel, dock workers, logistics managers, port administrators, systems technicians, customs officers.
Scenario Initiation	Planning of a new logistics operation that necessitates secure data sharing among shipping companies, ports, customs, and logistics providers, highlighting the importance of cybersecurity to guard against threats and unauthorized access.
Main Flow	<ol style="list-style-type: none"> 1. Enhanced Interoperability Among Logistics Systems: Establish interoperability among diverse logistics systems to facilitate seamless data exchange and ensure that data can flow securely between shipping companies, ports, customs, and logistics providers. 2. Secure Data Exchange Protocols: Develop and implement secure data exchange protocols and standards to ensure the confidentiality, integrity, and availability of data and encrypt data transmission channels to prevent unauthorised access and data breaches during exchange. 3. Collaborative Partnerships and Information Sharing: Foster collaborative partnerships among stakeholders to promote information sharing and coordination in cybersecurity efforts and establish protocols for sharing threat intelligence and incident

Use Cases Definitions

	<p>response strategies to collectively address cybersecurity challenges.</p> <p>4. Testing and Validation of Data Exchange Systems: Conduct rigorous testing and validation of data exchange systems to ensure their reliability and security and perform simulated cyber attack scenarios to evaluate the resilience of the systems and identify potential vulnerabilities.</p>
Evaluation Criteria – Related KPIs	<p>1. Enhanced Monitoring and Identification of Threats</p> <ul style="list-style-type: none"> KPI: Vulnerability Management >25/year <p>2. Ensure Employee Training Across Companies</p> <ul style="list-style-type: none"> KPI: Training of >200 employees from >40 SMEs and >5 large companies in the maritime sector companies within 2 years post-project completion KPI: Lessons Learnt >10

5.2.4 NERO Frameworks and tools to be Validated

The following Table 29 presents the list of the NERO frameworks and tools slated for validation. It includes details such as the tool name, collaborating entity, assigned role, and associated NERO framework. This comprehensive compilation ensures a structured approach to the validation process.

Table 29: UC2 Frameworks and Tools to be validated.

Tool	Partner	Role	NERO framework
SNYK	TRUSTILIO	Detect and treat code vulnerabilities	VICTORIOUS, AUDACIOUS
HRM	TRUSTILIO	Risk assessment and security management package	ARCANA, CYBIT
Seer box	PLUR	Web Application Security Manager	AUDACIOUS
HSPF	ONE	Attack identification through anomaly detection	CYBIT
Cyberwiser.eu training platform	TRUST-IT	Contribute to the training planning in WP5	ASTRAS

Use Cases Definitions

VitalCheck Urinesensor - Sensor	SHG	Collecting data from various sources (blood sample results, lab test results, etc.) to be used in an algorithm for diagnostic purposes.	CYBIT
MMT	MONT	Intrusion detection and response based on ML behaviour analysis and multi-source data capture.	ASTRAS, CYBIT
MI Cyberrange	MONT	Anti-phishing training game	ASTRAS

5.3 UC3: Boosting Financial Security through Enhanced Cybersecurity Awareness Tools

5.3.1 UC3 Description

The deployment of the NERO cybersecurity framework in the financial sector serves as a proactive measure against the ever-evolving landscape of cyber threats. With the continuous rise in sophisticated cyber attacks targeting financial institutions, NERO offers a comprehensive solution to mitigate risks and fortify defences. By safeguarding sensitive financial data from unauthorised access and manipulation, NERO plays a pivotal role in preserving the confidentiality, integrity, and availability of crucial information. Moreover, its capabilities extend beyond mere protection, encompassing proactive detection and prevention mechanisms to thwart potential cyber threats before they escalate. As financial institutions strive to uphold their commitment to clients' security and trust, the implementation of NERO emerges as a strategic imperative. It not only mitigates financial losses and reputational damage resulting from cyber incidents but also fosters resilience in the face of emerging threats. Furthermore, by ensuring the stability and integrity of financial systems and transactions, NERO contributes to the overall resilience and trustworthiness of the broader financial ecosystem. In essence, NERO represents a cornerstone in the defence against cyber threats in the financial sector, offering unparalleled protection, risk mitigation, and trust reinforcement.

Within the dynamic landscape of the financial sector, the deployment of the NERO cybersecurity framework emerges as a strategic imperative, encompassing a multifaceted approach to fortify defences and safeguard critical assets. At the forefront of this defence strategy lies the IDS, a sophisticated tool meticulously tuned to monitor incoming network traffic in real time. Through continuous analysis, the IDS diligently scrutinises patterns, behaviours, and signatures indicative of potential threats or intrusions. Leveraging the intelligence provided by NERO's training materials and program, the cybersecurity team stands poised to swiftly respond to any alerts triggered by the IDS, employing a proactive stance to mitigate potential damage and prevent unauthorised access.

Furthermore, as financial institutions heavily rely on commercial software to facilitate their operations, the scrutiny of the source code becomes paramount. Here, NERO's vulnerability scanning software

Use Cases Definitions

comes into play, meticulously scrutinising the source code for any vulnerabilities or weaknesses that could be exploited by malicious actors. By subjecting the code to rigorous examination and applying patches or updates as necessary, financial institutions ensure the integrity and resilience of their software systems, bolstering their defences against potential exploits.

Internally, the network infrastructure of financial institutions represents a critical battleground in the ongoing struggle against cyber threats. Through the implementation of NERO's network monitoring tools, the internal network is continuously monitored for signs of compromise, unauthorised access attempts, or suspicious behaviour. By correlating data from various sources and analysing network traffic patterns, the cybersecurity team remains vigilant, and ready to identify and respond to emerging threats in real-time.

Moreover, recognising that the human element constitutes both a vulnerability and a line of defence, NERO places significant emphasis on employee training and awareness. Through immersive training modules, interactive simulations, and real-world scenarios, employees are empowered with the knowledge and skills necessary to recognise, report, and mitigate cybersecurity threats effectively. By fostering a culture of cybersecurity awareness and accountability, financial institutions ensure that their staff remains vigilant guardians of sensitive data, contributing to the overall resilience and security posture of the organisation.

5.3.2 System Architecture and Assets Identification

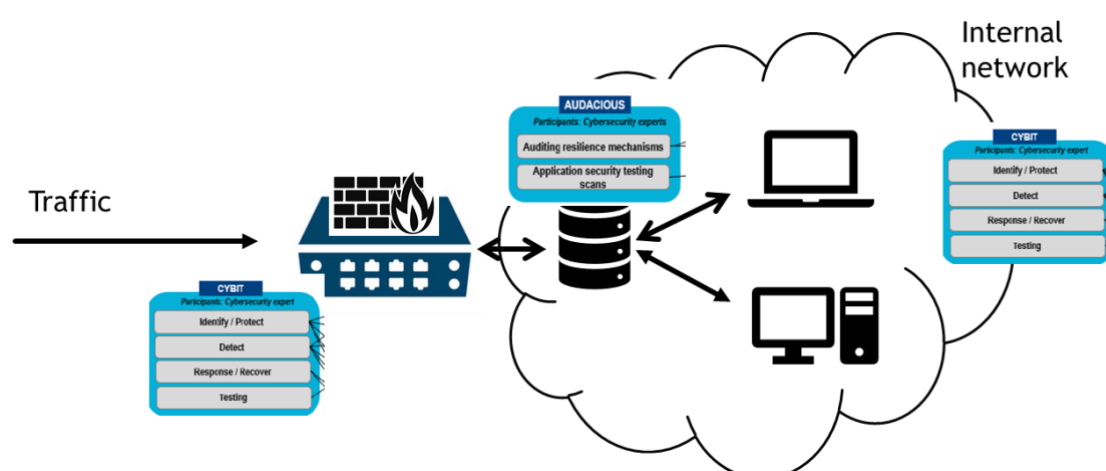


Figure 118: UC3 system architecture.

Within the architecture of an internal network tailored for a financial institution, several pivotal components synergise to uphold an impregnable cybersecurity infrastructure as shown in Figure 118. At the forefront, a meticulously configured firewall stands sentinel, meticulously scrutinising incoming and outgoing traffic, thus erecting a barrier against unauthorised access and potential threats that may seek to infiltrate the network's perimeter. NERO's CYBIT framework will be used alongside the network's firewall to monitor and protect the network from unauthorised access.

Internally, the network consists of servers, hosting indispensable financial applications and services. These servers are the backbone of the company infrastructure, hosting the key software used for the company's activities, as well as the source code of the company's product offered to other financial

Use Cases Definitions

institutions. This software will be examined and the source code will be scanned for vulnerabilities using the AUDACIOUS framework.

Moreover, the workstations entrusted to employees, equipped with robust endpoint security software, serve as the frontline interface, facilitating secure access to network resources and undertaking daily tasks with unwavering reliability. These workstations, alongside the servers and all the network equipment, comprise the internal network. The internal network will be protected against any threats, with a continuous monitoring performed by the CYBIT framework of the NERO project.

The subsequent Table 30 provides a comprehensive breakdown of the assets associated with the second use case. It includes asset names, descriptions, the types of data processed by each asset, and their respective criticality levels.

Table 30: UC3 Asset Description.

Asset Name	Description	Data processed by the asset	Criticality
Servers	Physical hardware used to deploy all systems	The servers host all the data of the company	High
Commercial Software	The offered solution from the company	All the operation data of the company	High
Network Infrastructure	The networking and firewall of the company	All data passes from the infrastructure	High
Individual PCs	The companies own hardware used by the employs	Only data accessible to each employee position are processed at the individual PCs	Medium

5.3.3 Scenarios Definition

The following Table 31, Table 32, and Table 33 present the scenarios definition for the first use case. They include a detailed description, assumptions and pre-conditions, the use case goal, involved actors, scenario initiation, main flow of events, and evaluation criteria such as related KPIs.

Table 31: UC3 - Scenario 1 (SC3.1).

Scenario name	UC3.1 Intrusion detection
Description	The financial organization uses intrusion detection and prevention tools to monitor their networks for unauthorized access attempts and to block malicious traffic.
Assumptions & Pre-Conditions	Authorization mechanism

Use Cases Definitions

Goal (Successful End Condition)	Protect the network against unauthorized access
Involved Actors	Users' employees, network admins
Scenario Initiation	Penetration testing by NERO tools
Main Flow	<ol style="list-style-type: none"> 1. Deployment of Intrusion Detection System (IDS): The financial institution deploys an IDS to monitor incoming network traffic. 2. Real-Time Scanning for Suspicious Patterns: The IDS scans for suspicious patterns, anomalies, or known attack signatures in real-time. 3. Alert Triggering and Response Protocol: Upon detection of potential threats or intrusions, the IDS triggers alerts to the cybersecurity team for further investigation and response.
Evaluation Criteria – Related KPIs	<ol style="list-style-type: none"> 1. Enhance Cybersecurity Awareness and Prevention <ul style="list-style-type: none"> • KPI: Security Training Completion Rate > 80% 2. Improve Incident Response Efficiency <ul style="list-style-type: none"> • KPI: Reported Incident Response Rate Increase by >20% 3. Ensure Employee Training Across Companies <ul style="list-style-type: none"> • KPI: Training of >200 employees from >50 SMEs and >5 fintech companies within 2 years post-project completion

Table 32: UC3 - Scenario 2 (SC3.2)

Scenario name	UC3.2 System vulnerability management
Description	The financial organisation uses vulnerability management tools to identify and remediate security vulnerabilities in its systems and applications.
Assumptions & Pre-Conditions	Access to internal infrastructure is given
Goal (Successful End Condition)	Decrease the number of vulnerabilities in its systems and applications
Involved Actors	Employees, admin, IT
Scenario Initiation	Software vulnerabilities check
Main Flow	<ol style="list-style-type: none"> 1. Source Code Vulnerability Scanning: Before deploying or updating commercial software used within the financial institution, the source code undergoes thorough vulnerability scanning.

Use Cases Definitions

	<ol style="list-style-type: none"> NERO Vulnerability Scan: NERO's vulnerability scanning software is utilized to identify any weaknesses or security flaws within the source code. Vulnerability Resolution: Detected vulnerabilities are addressed either by patching, updating, or finding alternative solutions, ensuring that the software remains secure and resilient against potential exploits.
Evaluation Criteria – Related KPIs	<ol style="list-style-type: none"> Enhanced Monitoring and Identification of Threats <ul style="list-style-type: none"> KPI: Decrease Number of Vulnerabilities >20% Ensure Employee Training Across Companies <ul style="list-style-type: none"> KPI: Training of >200 employees from >50 SMEs and >5 fintech companies within 2 years post-project completion

Table 33: UC3 - Scenario 3 (SC3.3)

Scenario name	UC3.3 Threat identification and mitigation actions
Description	The financial organisation continuously monitors their systems and networks for security incidents and alerts and implements a rapid response plan to quickly contain and mitigate potential incidents.
Assumptions & Pre-Conditions	Ability to integrate to current systems
Goal (Successful End Condition)	Reduce the number of threats to the systems and network.
Involved Actors	Employees, Admin, IT
Scenario Initiation	Continuous process
Main Flow	<ol style="list-style-type: none"> Continuous Internal Network Monitoring: The internal network of the financial institution is continuously monitored for threats and malicious activities." Deployment of NERO's Network Monitoring Tools: NERO's network monitoring tools are deployed to detect unauthorized access attempts, unusual behaviour, or internal security breaches." Threat Identification and Mitigation: By analysing network traffic, log data, and user activities, the cybersecurity team can identify and mitigate potential threats before they escalate.
Evaluation Criteria – Related KPIs	<ol style="list-style-type: none"> Enhance Cybersecurity Awareness and Prevention <ul style="list-style-type: none"> KPI: Security Training Completion Rate > 80%

	<p>2. Improve Incident Response Efficiency</p> <ul style="list-style-type: none"> • KPI: Reported Incident Response Rate Increase by >20% <p>3. Ensure Employee Training Across Companies</p> <ul style="list-style-type: none"> • KPI: Training of >200 employees from >50 SMEs and >5 fintech companies within 2 years post-project completion
--	--

5.3.4 NERO Frameworks and tools to be Validated

The following Table 34 presents the list of the NERO frameworks and tools slated for validation. It includes details such as the tool name, collaborating entity, assigned role, and associated NERO framework. This comprehensive compilation ensures a structured approach to the validation process.

Table 34: UC#3 Frameworks and Tools to be validated.

Tool	Partner	Role	NERO framework
KIOKU AI	MDS	Employee's training	ASTRAS
M-RADAR	MINDS	Intrusion Detection System	CYBIT
MMT	MONT	Threat detection	CYBIT
Advanced cyber range tools	MONT	Employee's training	ASTRAS
MI Cyberrange	MPNT	Employee's training	ASTRAS
SEER Box	PLUR	Vulnerability checks	AUDACIOUS
Cyberwiser.eu	TRUST-IT	Marketplace	ARCANA
HSPF	ONE	Intrusion Detection System	CYBIT

6 Conclusion and Future Work

The document describes the NERO project approach to identify, analyse, and address cybersecurity challenges that SMEs face. This deliverable provides an in-depth cybersecurity landscape threat analysis, the end-user requirements through comprehensive questionnaires, and a high level of the NERO ecosystem. Furthermore, the questionnaire and the literature review provided insight about the cybersecurity awareness and specific challenges to SMEs, paving the way for the development of the NERO ecosystem. Overall, this deliverable is an initial version of the NERO ecosystem where the tools that will be used in this project are described, and the use cases are defined.

The deliverable will be used as the core technical reference document in the project to align the planning, design, and development of the framework components in the rest of the technical work packages. The final version of the architecture (D2.2) will ensure the full alignment of the description with the actual methodology and the implemented NERO ecosystem with its components and subcomponents.

References

References

- [1] ‘Cybersecurity for SMEs - Challenges and Recommendations’, ENISA. Accessed: Apr. 25, 2024. [Online]. Available: <https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes>
- [2] N. Zahoor, O. Al-Tabbaa, Z. Khan, and G. Wood, ‘Collaboration and Internationalization of SMEs: Insights and Recommendations from a Systematic Review’, *Int. J. Manag. Rev.*, vol. 22, no. 4, pp. 427–456, 2020, doi: 10.1111/ijmr.12238.
- [3] PONEMON Institute, ‘2019 Global State of Cybersecurity in Small and Medium-Sized Businesses’, 2019. [Online]. Available: <https://www.cisco.com/c/dam/en/us/products/collateral/security/ponemon-report-smb.pdf>
- [4] ENISA, ‘Threat Landscape 2020’, 2020. [Online]. Available: <https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape/enisa-threat-landscape-2020>
- [5] ANSSI, ‘Cyber Threat Overview 2022’, 2022. [Online]. Available: <https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-002.pdf>
- [6] Verizon, ‘DBIR Data Breach Investigations Report’, 2022. [Online]. Available: <https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf>
- [7] IBM, ‘Cost of a Data Breach Report 2022’, 2022. [Online]. Available: <https://www.ibm.com/downloads/cas/3R8N1DZJ>
- [8] ENISA, ‘Threat Landscape 2023’, 2023. [Online]. Available: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>
- [9] CISCO, ‘Cybersecurity for SMBs: Asia Pacific Businesses Prepare for Digital Defense’, 2021. [Online]. Available: https://www.cisco.com/c/dam/global/en_hk/assets/pdfs/cybersecurity-for-smb-asia-pacific-businesses-prepare-for-digital-defense.pdf
- [10] europol, ‘.’ [Online]. Available: <https://www.europol.europa.eu/>
- [11] cyberwatching.eu, ‘Cybersecurity and Privacy research results for a resilient Europe’. [Online]. Available: <https://cyberwatching.eu/>
- [12] CISCO, ‘Securing Against Rising Threats’, 2022. [Online]. Available: <https://www.cisco.com/c/dam/en/us/solutions/collateral/fy22-smb-dynamo-v4-final.pdf>
- [13] NIST, ‘The NIST Cybersecurity Framework (CSF) 2.0’, 2024. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>
- [14] C. Pugnetti and C. Casián, ‘Cyber risks and Swiss SMEs : an investigation of employee attitudes and behavioral vulnerabilities’, Jan. 2021, doi: 10.21256/zhaw-21478.
- [15] A. Moneva and R. Leukfeldt, ‘Insider threats among Dutch SMEs: Nature and extent of incidents, and cyber security measures’, *J. Criminol.*, vol. 56, no. 4, pp. 416–440, Dec. 2023, doi: 10.1177/26338076231161842.
- [16] D. Javaheri, M. Fahmideh, H. Chizari, P. Lalbakhsh, and J. Hur, ‘Cybersecurity threats in FinTech: A systematic review’, *Expert Syst. Appl.*, vol. 241, p. 122697, May 2024, doi: 10.1016/j.eswa.2023.122697.
- [17] M. Falch, H. Olesen, K. E. Skouby, R. Tadayoni, and I. Williams, ‘Cybersecurity Strategies for SMEs in the Nordic Baltic Region’, *J. Cyber Secur. Mobil.*, pp. 727–754, 2022, doi: 10.13052/jcsm2245-1439.1161.

References

- [18] ‘Determining the Main Causes that Lead to Cybersecurity Risks in SMEs’, *Bus. Excell. Manag.*, vol. 10, no. 4, pp. 38–48, 2020, Accessed: Apr. 26, 2024. [Online]. Available: <https://www.ceeol.com/search/article-detail?id=915191>
- [19] C. Boletsis, R. Halvorsrud, J. Pickering, S. Phillips, and M. Surridge, ‘Cybersecurity for SMEs: Introducing the Human Element into Socio-technical Cybersecurity Risk Assessment’, in *Proceedings of the 16th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications*, Online Streaming, --- Select a Country ---: SCITEPRESS - Science and Technology Publications, 2021, pp. 266–274. doi: 10.5220/0010332902660274.
- [20] C. Ponsard, J. Grandclaoudon, and S. Bal, ‘Survey and Lessons Learned on Raising SME Awareness about Cybersecurity’, in *Proceedings of the 5th International Conference on Information Systems Security and Privacy*, Prague, Czech Republic: SCITEPRESS - Science and Technology Publications, 2019, pp. 558–563. doi: 10.5220/0007574305580563.
- [21] N. Rawindaran, A. Jayal, E. Prakash, and C. Hewage, ‘Cost Benefits of Using Machine Learning Features in NIDS for Cyber Security in UK Small Medium Enterprises (SME)’, *Future Internet*, vol. 13, no. 8, p. 186, Jul. 2021, doi: 10.3390/fi13080186.
- [22] M. Antunes, M. Maximiano, R. Gomes, and D. Pinto, ‘Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal’, *J. Cybersecurity Priv.*, vol. 1, no. 2, pp. 219–238, Apr. 2021, doi: 10.3390/jcp1020012.
- [23] M. Kappe, R.-C. Härting, C. Karg, and D. Deffner, ‘Cybersecurity in SMEs – Drivers of Cybercrime, Insufficient Equipment and Prevention’, *Procedia Comput. Sci.*, vol. 225, pp. 3631–3640, Jan. 2023, doi: 10.1016/j.procs.2023.10.358.
- [24] J. Rajamäki *et al.*, ‘Improving the Cybersecurity Awareness of Finnish Podiatry SMEs’, 89448. Accessed: Apr. 26, 2024. [Online]. Available: <http://www.theseus.fi/handle/10024/809095>
- [25] M. Van Haastrecht *et al.*, ‘A Shared Cyber Threat Intelligence Solution for SMEs’, *Electronics*, vol. 10, no. 23, p. 2913, Nov. 2021, doi: 10.3390/electronics10232913.
- [26] K. A. Ubaidillah, S. I. Hisham, F. Ernawan, G. Badshah, and E. Suharto, ‘using Autoencoder based Deep Neural Network for SME Cybersecurity’, in *2021 5th International Conference on Informatics and Computational Sciences (ICICoS)*, Aug. 2021, pp. 210–215. doi: 10.1109/ICICoS53627.2021.9651851.
- [27] L. F. Ilca, O. P. Lucian, and T. C. Balan, ‘Enhancing Cyber-Resilience for Small and Medium-Sized Organizations with Prescriptive Malware Analysis, Detection and Response’, *Sensors*, vol. 23, no. 15, p. 6757, Jul. 2023, doi: 10.3390/s23156757.
- [28] G. Erdogan, R. Halvorsrud, C. Boletsis, S. Tverdal, and J. B. Pickering, ‘Cybersecurity Awareness and Capacities of SMEs’, *296-304*, 2023, doi: 10.5220/0011609600003405.
- [29] S. Mishra, ‘Exploring the Impact of AI-Based Cyber Security Financial Sector Management’, *Appl. Sci.*, vol. 13, no. 10, p. 5875, May 2023, doi: 10.3390/app13105875.
- [30] F. Damage: The Perspective of Small Enterprises in Saudi Arabia’, *Sensors*, vol. 21, no. 20, p. 6901, Oct. 2021, doi: 10.3390/s21206901.
- [31] C. Boletsis, S. N. Orni, and R. Halvorsrud, ‘The HORM Diagramming Tool: A Domain-Specific Modelling Tool for SME Cybersecurity Awareness’, *VISIGRAPP*, pp. 203–213, 2023, doi: 10.5220/0011786600003417.
- [32] B. Pickering, C. Boletsis, R. Halvorsrud, S. Phillips, and M. Surridge, ‘It’s Not My Problem: How Healthcare Models Relate to SME Cybersecurity Awareness’, in *HCI for Cybersecurity, Privacy*

References

- and Trust*, vol. 12788, A. Moallem, Ed., in Lecture Notes in Computer Science, vol. 12788., Cham: Springer International Publishing, 2021, pp. 337–352. doi: 10.1007/978-3-030-77392-2_22.
- [33] D. Branley-Bell, L. Coventry, and E. Sillence, ‘Promoting Cybersecurity Culture Change in Healthcare’, in *Proceedings of the 14th Pervasive Technologies Related to Assistive Environments Conference*, in PETRA ’21. New York, NY, USA: Association for Computing Machinery, Mar. 2021, pp. 544–549. doi: 10.1145/3453892.3461622.
- [34] F. Rizzoni, S. Magalini, A. Casaroli, P. Mari, M. Dixon, and L. Coventry, ‘Phishing simulation exercise in a large hospital: A case study’, *Digit. Health*, vol. 8, p. 20552076221081716, Jan. 2022, doi: 10.1177/20552076221081716.
- [35] M. Neri, F. Niccolini, and R. Pugliese, ‘Assessing SMEs’ cybersecurity organizational readiness: Findings from an Italian survey’, *Online J. Appl. Knowl. Manag.*, vol. 10, no. 2, pp. 1–22, Sep. 2022, doi: 10.36965/OJAKM.2022.10(2)1-22.
- [36] ‘SMESEC: A lightweight Cybersecurity framework for thorough protection’. [Online]. Available: <https://www.smesec.eu/>
- [37] B. Y. Ozkan and M. Spruit, ‘Assessing and Improving Cybersecurity Maturity for SMEs: Standardization aspects’.
- [38] S. Parker, Z. Wu, and P. D. Christofides, ‘Cybersecurity in process control, operations, and supply chain’, *Comput. Chem. Eng.*, vol. 171, p. 108169, Mar. 2023, doi: 10.1016/j.compchemeng.2023.108169.
- [39] D. Kant and A. Johannsen, ‘Evaluation of AI-based use cases for enhancing the cyber security defense of small and medium-sized companies (SMEs)’, *Electron. Imaging*, vol. 34, no. 3, pp. 387-1-387–8, Jan. 2022, doi: 10.2352/EI.2022.34.3.MOBMU-387.
- [40] N. Rawindaran, A. Jayal, and E. Prakash, ‘Exploration of the Impact of Cybersecurity Awareness on Small and Medium Enterprises (SMEs) in Wales Using Intelligent Software to Combat Cybercrime’, *Computers*, vol. 11, no. 12, p. 174, Dec. 2022, doi: 10.3390/computers11120174.
- [41] A. Sukumar, H. A. Mahdiraji, and V. Jafari-Sadeghi, ‘Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors’, *Risk Anal.*, vol. 43, no. 10, pp. 2082–2098, 2023, doi: 10.1111/risa.14092.
- [42] M. M. A. Mutalib, Z. Zainol, and M. H. M. Halip, ‘Mitigating Malware Threats at Small Medium Enterprise (SME) Organisation: A Review and Framework’, in *2021 6th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE)*, Sep. 2021, pp. 1–6. doi: 10.1109/ICRAIE52900.2021.9703991.
- [43] M. A. J. *Interact. Multimed. Artif. Intell.*, vol. 6, no. 3, p. 55, 2020, doi: 10.9781/ijimai.2020.08.003.
- [44] M. Benz and D. Chatterjee, ‘Calculated risk? A cybersecurity evaluation tool for SMEs’, *Bus. Horiz.*, vol. 63, no. 4, pp. 531–540, Jul. 2020, doi: 10.1016/j.bushor.2020.03.010.
- [45] ENISA, ‘Cybersecurity guide for SMEs - 12 steps to securing your business’, 2021. [Online]. Available: <https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes>
- [46] America’s Cyber Defense Agency, ‘Cyber Guidance for Small Businesses’. [Online]. Available: <https://www.cisa.gov/cyber-guidance-small-businesses>
- [47] Australian Government, ‘.’ [Online]. Available: <https://www.cyber.gov.au/>
- [48] ENISA, ‘Interoperable EU Risk Management Toolbox’, ENISA. Accessed: Apr. 26, 2024. [Online]. Available: <https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-toolbox>
- [49] OWASP, [Online]. Available: <https://www.security-net.biz/files/owaspriskcalc.html>

References

- [50] B. Schneier, *Liars and Outliers: Enabling the Trust that Society Needs to Thrive*. John Wiley & Sons, 2012.
- [51] D. M. West, *Digital Government: Technology and Public Sector Performance*. Princeton University Press, 2005.
- [52] E. Gonen, ‘Tim Brown, Change by Design: How Design Thinking Transforms Organizations and Inspires Innovation (2009)’ , *Mark. Glob. Dev. Rev.*, vol. 4, no. 2, Jan. 2020, doi: 10.23860/MGDR-2019-04-02-08.
- [53] G. Stoneburner, A. Goguen, and A. Feringa, ‘Risk management guide for information technology systems : recommendations of the National Institute of Standards and Technology’, National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-30, 2002. doi: 10.6028/NIST.SP.800-30.
- [54] owasp, ‘OWASP Risk Rating Methodology’. [Online]. Available: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology#
- [55] ENISA, ‘European Cybersecurity Skills Framework (ECSF)’. [Online]. Available: <https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework>
- [56] E. B.-N. Sanders and P. J. Stappers, ‘Co-creation and the new landscapes of design’, *CoDesign*, vol. 4, no. 1, pp. 5–18, Mar. 2008, doi: 10.1080/15710880701875068.
- [57] T. Mattelmäki, K. Vaajakallio, and I. Koskinen, ‘What Happened to Empathic Design?’, *Des. Issues*, vol. 30, no. 1, pp. 67–77, Jan. 2014, doi: 10.1162/DESI_a_00249.