CALL H2020-SU-DS-2018-2019-2020
Digital Security
TOPIC SU-DS05-2018-2019
Digital security, privacy, data protection and accountability in critical sectors

AI4HEALTHSEC

"A Dynamic and Self-Organized Artificial Swarm Intelligence Solution for Security and Privacy Threats in Healthcare ICT Infrastructures"

D1.7 – Public Final Management report

Due date of deliverable: 31.12.2023
Actual submission date: 17.05.2024

Grant agreement number: 883273
Start date of project: 01/10/2020
Revision 3

Lead contractor: CNR
Duration: 39 months

Project funded by the European Commission within the EU Framework Programme for Research and Innovation HORIZON 2020	
Dissemination Level	
PU = Public, fully open, e.g. web	✓
CO = Confidential, restricted under conditions set out in Model Grant Agreement	
CI = Classified, information as referred to in Commission Decision 2001/844/EC.	
Int = Internal Working Document	

D1.7 – Public Final Management report

Editors

Stefano Silvestri, Mario Ciampi, Rita Capasso, Giuseppe De Pietro (CNR)

Contributors

Argyro Chatzopoulou (TUV)

Reviewers

Jihane Najar (AEGIS)

Kitty Kioskly (UoE)

VERSION	*DATE*	*REVISION AUTHOR*	*SUMMARY OF CHANGES*
0.1	28/11/2023	Stefano Silvestri, Mario Ciampi, Rita Capasso, Giuseppe De Pietro	ToC and first draft
0.2	31/11/2023	Stefano Silvestri	Context and Section 2 draft
0.5	12/12/2023	Stefano Silvestri, Mario Ciampi, Argyro Chatzopoulou	Section 2 final draft
0.7	18/12/2023	Stefano Silvestri, Mario Ciampi	Section 3 draft
0.9	28/12/2023	Stefano Silvestri, Mario Ciampi	Final draft version
1.0	16/01/2024	Stefano Silvestri, Mario Ciampi, Rita Capasso, Giuseppe De Pietro	Internal reviews and final version
1.1	17/04/2024	Stefano Silvestri, Mario Ciampi, Rita Capasso, Giuseppe De Pietro	Extension of subsection 3.2 on the impacts of the project, in compliance with reviewers' recommendations
1.2	07/05/2024	Mario Ciampi	Correction of a typo related to the dissemination level

The work described in this document has been conducted within the project AI4HEALTHSEC, started in October 2020. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883273

Executive Summary

This document summarises the project's activities performed during the whole 39 months of duration, with a particular highlight on the management and coordination activities that allowed to successfully accomplish the planned results.

The deliverable, after a preliminary description of the context of the proposal and its main objectives, it briefly describes the activities and the main achievement of the project's WPs. Then, it presents the other management activities related to the pilot and open call, dissemination, and policy and standardisation contributions obtained thorough the AI4HEALTHSEC project's results.

Finally, it shows the main result of the project, namely the AI4HEALTHSEC platform, a software framework that implements the cybersecurity awareness methodology proposed by the project, providing an overview of the planned exploitation and impact of the obtained results.

The detail of the technical and non-technical information provided in this document allows for a general domain understandability, as well as does not contain any confidential information. In this way, it can be used to further disseminate the obtained results to the general public, if required, providing in this way a summarised final report of the project's management activities and results.

Contents

List of acronyms

AEGIS	AEGIS IT Research G.M.B.H.
DB	Data Base
CA	Consortium Agreement
CI	Classified
CNR	Consiglio Nazionale delle Ricerche
CO	Confidential
CTI	Cyber Threat Intelligence
D	Deliverable
DNS	Domain Name Server
DOA	Description Of the Action
DREAD	Damage, Reproducibility, Exploitability, Affected users, and Discoverability
DSAF	Dynamic Situational Awareness Framework
EAB	External Advisory Board
EBIT	EBIT S.R.L.
EC	European Commission
EM	Exploitation Manager
ENoLL	European Network of Living Labs
FHG-IBMT	Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung E.V.
FORTH	Foundation for Research and Technology / Idryma Technologias Kai Erevnas
FP	Focal Point
FVT	Forensics Visualisation Toolkit
GA	Grant Agreement
GAP	Grant Agreement Preparation
GDPR	Global Data Protection Regulation
HCII	Health Care Information Infrastructures
HCSCS	Health Care Supply Chain Services
HIS	Hospital Information System
IOA	Indicators Of Attack
IOC	Indicators Of Compromise
ICCS	Institute of Communication and Computer Systems

IDS	Intrusion Detection System
IM	Innovation ì Manager
IPR	Intellectual Property Rights
IT	Information Technology
KB	Knowledge Base
KER	Key Exploitable Result
KLINIK	Klinikum Nürnberg
KPI	Key Performance Indicator
LL	Living Lab
L/EM	Legal/Ethical Manager
M	Month
MDR	Medical Device Reporting
MS	MileStone
NA	Not Applicable
NER	Named Entity Recognition
NIST	National Institute of Standards
OT	Operational Technology
PC	Project Coordinator
PCs	Personal Computers
PDMFC	Projectos de Desenvolvimento Manutenção Formação e Consultadoria L.D.A.
PEST	Political, Economic, Social and Technological Analysis
PHILIPS	Philips Electronics Nederland B.V.
PIC	Project Implementation Committee
PM	Person/Month
PN	Privanova S.A.S.
PO	Project Officer
PRC	PRivacy Committee
PSC	Project Steering Committee
PSO	Project Security Officer
PTM	Project Technical Manager
PU	Public
QDM	Quality and Dissemination Manager
QMC	Quality Management Committee

R&D	Research and Development
RM	Risk Manager
SAB	Security Advisory Board
SAP IS-H	SAP Industry Solution for Healthcare
SDO	Standards Developing Organization
SME	Small and Medium-sized Enterprise
STS	Sphynx Technology Solutions A.G.
SVM	Support Vector Machine
SWOT	Strengths, Weaknesses, Opportunities & Threats Analysis
T	Task
TRL	Technology Readiness Levels
TUV	TÜV TRUST IT GmbH Unternehmensgruppe TÜV AUSTRIA
UAB	User Advisory Board
UAT	User Acceptance Testing
UEBA	User and Entity Behaviour Analytics
UOB	University of Brighton
UOE	University of Essex
WP	Work Package
WPL	Work Package Leader

List of tables

List of figures

1 Summary of the Context and Overall Project's Objectives

This Section provides the description of the context of the proposal, and the main project's overall objectives. Moreover, it provides a summary of the project's main objectives achieved during its development. Finally, it shows the AI4HEALTHSEC consortium.

1.1 *Context of the proposal*

Over the past decade, the medical field has experienced a massive digitization, as well as the adoption of new medical technologies including IoT, Cloud Computing, and Big Data, improving overall patients' experiences and outcomes. This scenario led to an increasing interconnection of technologies in healthcare both at the physical and cyber levels, transforming these infrastructures into large Health Care Information Infrastructures (HCIIs). This evolving digital interconnectivity of medical devices has also changed the cybersecurity threat landscape, also because the digitalization of patient data is attracting more attention from cybercriminals, producing a wide range of security and privacy challenges, and increasing the danger of potential cybersecurity attacks in HCIIs. Moreover, the integrated nature introduces many additional potential entry points for propagating cyber-attacks and risks in terms, such as obsolete security infrastructure or outdated systems, infected devices, lack of appropriate security protocols across organizations.

Today, the HCIIs are unprotected from complex cyber-attacks because they usually address cybersecurity with individual and isolated products, without defining a high-level security strategy capable of orchestrating multiple security components to identify system vulnerabilities and sophisticated attacks.

In this scenario, AI4HEALTHSEC proposed an innovative state of the art solution capable of improving the detection and the analysis of cyber-attacks and threats on HCIIs, and, at the same time, increasing the knowledge on the current cyber security and privacy risks. AI4HEALTHSEC solution builds risk awareness within the digital Healthcare ecosystem and among the involved Health operators, enhancing their insight into their Healthcare ICT infrastructures, providing them with capability to react in case of security and privacy breaches. Finally, the proposed AI4HEALTHSEC solution supports the exchange of reliable and trusted incident-related information among ICT systems and entities composing the HCIIs without revealing sensitive corporate details. The next Figure 1-1 shows an overview of the current scenario composed of the highly interconnected software and hardware, highlighting the main criticality and cybersecurity needs of the corresponding assets (grouped in circles).

The proposed AI4HEALTHSEC platform enhances the security and resilience of the modern digital healthcare ecosystems and the medical supply chain services through the provision of a novel Dynamic Situational Awareness Framework (DSAF), which supports the HCIIs and the other stakeholders of comprising the Health Care ecosystem to recognize (and not only in the case of Healthcare domain, identify, model, and dynamically analyse cyber risks Moreover, it supports forecasting, treatment and response to advanced persistent threats and handle daily cyber-security and privacy risks, incidents, and data breaches.

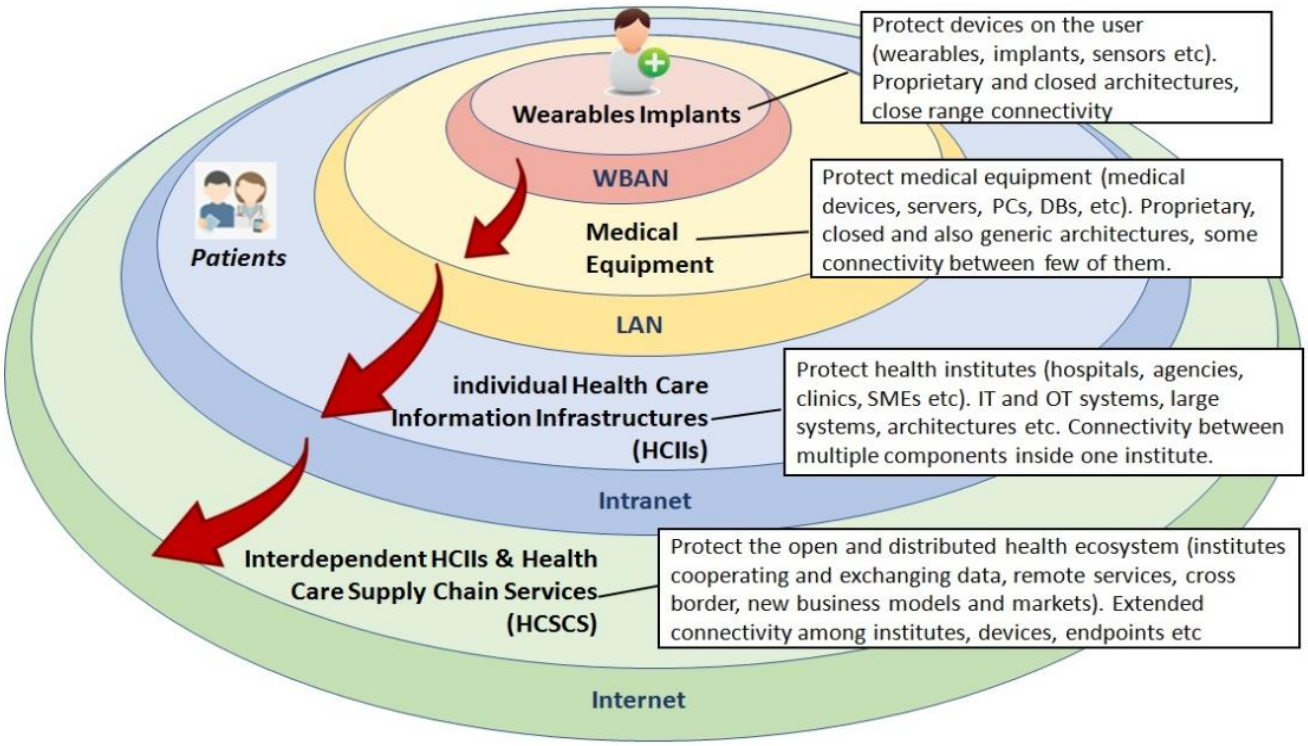

Figure 1-1. Health sector overview and main cybersecurity issues

1.2 *Overall Objectives of the AI4HEALTHSEC project*

Based on the project call and design, seven main objectives have been set and achieved during the 39 months duration of the project. These objectives are listed below:

- *Objective 1: Conceptualize and establish a self-organized Swarm Intelligence (SI) model.*
  - The Swarm intelligent model, based on agents, has been designed and conceptualised, allowing also for the definition of management and coordination schemes and structures.
- *Objective 2: Provide distributed data management and reasoning capabilities for threats, risks and vulnerabilities identification.*
  - The Individualised Autonomous Networking Protocol, the threat intelligence services have been designed, implemented and integrated in the final AI4HEALTHSEC platform.
- *Objective 3: Develop an advanced cyber incident handling approach for the health care ecosystem.*
  - The design and development of data sensing and data fusion functionalities and models, of the anomalies identification functions and of the orchestration functions have been successfully delivered.

- *Objective 4: Develop a novel Dynamic Situational Awareness Approach (AI4HEALTHSEC framework) for HCIIs*.
    - The detailed specification of the AI4HEALTHSEC framework has been provided.
- *Objective 5: To develop the AI4HEALTHSEC system based on the AI4HEALTHSEC framework*.
    - The final implementation of the modules of the AI4HEALTHSEC system has been released and integrated, and also tested in the pilots.
- *Objective 6: To deploy and validate the AI4HEALTHSEC Framework and System in real operational environments.*
    - The pilot scenarios have been defined, also identifying the specific technical needs to deploy the AI4HEALTHSEC system in the corresponding real operational environments. The deployment and implementation of the pilots, leveraging the final release of the AI4HEALTHSEC Framework, have been successfully exploited in the real real-life Health Care scenarios provided.
- *Objective 7: To disseminate knowledge developed during the project to different areas of the health care ecosystem and transfer knowledge to other critical sectors.*
    - Several dissemination activities and actions have been performed by the members of the consortium, through the participation in workshops, events, conferences and seminars, the use of social media, the presentation of scientific papers, the publication of press releases and others, achieving and overcome the related planned specific KPIs.

These objectives have been all achieved by the end of the project, respecting the planned timelines (as demonstrated by the achievement of the corresponding measurable KPIs, also set at the beginning of the project, such as the specification od the functionalities, the implementation of the services, the validation in pilots, the TRL of the platform, and others).

Furthermore, the project also achieved all the others planned KPIs, defined with the purpose of measuring and assessing the performances and operations of the project, assessing the full achievement of all the planned results.

1.3 *AI4HEALTHSEC consortium*

The AI4HEALTHSEC consortium includes 15 Partners from 9 different Countries (Italy, Nederland, Germany, Greece, Belgium, Switzerland, UK, Portugal, France). The consortium includes partners from Universities, Research Bodies, Large Industry, SMEs, Healthcare Organization and from Inspection and Certification Body.

Figure 1-2. Partners of the AI4HEALTHSEC consortium

2 Summary of the Project Activities and tasks

This Section provides a summary of the AI4HEALTHSEC's activities and tasks performed during the 39 months duration of the project, performed with the full support of the management and coordination team of the project. Moreover, it lists the milestones reached during the project's development and implementation. This Section also describes the pilot activities performed to assess and test the proposed solution, including the open call that allowed to make external partners to propose and implement additional pilots, also in different domains with respect to the healthcare, allowing to demonstrate the wider applicability of the AI4HEALTHSEC platform. Finally, it summarises the main dissemination activities of the project and the contributions provided to standardisation and policy activities in the domain of cybersecurity.

2.1 *AI4HEALTHSEC WPs and Tasks*

2.1.1 WP1

The main objective of WP1 was to ensure timely and qualitative achievement of the project results through technical and administrative coordination, to coordinate the Quality and Innovation of the results, and the Pilot activities. Moreover, it established and coordinated the activities of the project's Boards and the Committees for the control, coordination, and assessment of the project. Finally, it provided timely and efficient organizational and financial coordination, meeting the contractual commitments. The management of the project work comprised the following main activities: 1) Decision-making and conflict resolution; 2) Administrative and financial management; 3) Scientific and technological management; 4) Risk and opportunities management and Quality assurance; 5) Innovation management; 6) Ethical, Privacy, GDPR Compliance, Security Coordination. Each one of these activities have been included and developed in a specific Task of the WP1. The WP1 successfully delivered 7 reports deliverables, respecting their planned deadlines.

2.1.2 WP2

The activities of the WP2 aimed at eliciting, collecting, and analysing the requirements associated with security incident management mainly in the HCIIs. Moreover, the WP2 produced the specifications for the real-life scenario pilots. It also performed a preliminary analysis of the legal and ethical framework applicable to AI4HEALTHSEC. From the technical point of view, it provided the specifications of the AI4HEALTHSEC architecture and interfaces and delineated the implementation process. The performed tasks identified the high-level legal and ethical requirements associated with the technological innovation of the project. Finally, it defined the appropriate evaluation methodology and the corresponding metrics for the demonstration of the unique characteristics of AI4HEALTHSEC. The WP2 delivered the obtained results in 4 deliverables, released in time in the first 8 months of the project.

2.1.3 WP3

The WP3 aimed to provide the main theoretical foundation for developing the technical solution of the swarm intelligence model proposed by the AI4HEALTHSEC project. The WP3 intended to transfer the emerging idea of swarm intelligence, enabling the healthcare operators to co-operate in an innovative way. More in details, it defined the proposed model aspects (i.e., swarm -inspired and self-organising) and the entities of abstraction, (i.e., healthcare entities, primary and supervisor agents). These healthcare entities act locally, performing their own actions, which provide an ecosystem with the potential of achieving higher-order intelligence results, which the individual healthcare entities could not reach by themselves. The primary agents perform a set of actions to secure a specific area of the HCII. These actions gradually accumulate by means of the supervisor agents, to form an intelligence of a higher level, for making its optimal decisions. The supervisor agents are swarm-inspired, so that they can correlates the data from the primary agents and analyse the data to identify the pattern for risk and incidents. Finally, the outputs from the task also provided a communication model to capture the communications and flow of knowledge exchange among the agents. The results of the WP3 are included in 4 reports, delivered during the first 24 months of the project.

2.1.4 WP4

WP4 developed the models and specifications for all the horizontal layers of the AI4HEALTHSEC architecture (see next Section 3.1=. In detail, it firstly performed the necessary state-of-the-art analysis of the existing situational awareness trends and approaches. Then, it developed the specifications of all the horizontal layers, as well as the mathematical models and instruments involved in all those layers. Moreover, the activities carried out within the WP4 also allowed to develop all the techniques and methods for the Attack Forecasting & Incident Simulator, which are leveraged by all the horizontal layers of the proposed architecture. The WP4 submitted the 5 planned deliverables respecting their deadlines during the first 24 months of the project.

2.1.5 WP5

The results of the activities of the WP5 allowed to successfully develop and implement the Horizontal Layers 1, 2, 3 and 4 and of the Vertical Layers 1 and 2 of the AI4HEALTHSEC's platform architecture (see next Section 3.1). Moreover, also the Cyber-Attack Forecasting & Security Incident Simulator subsystems have been developed and implemented, finally making available almost all the subsystems and modules of the AI4HEALTHSEC platform, with the exception of the Visualization and Context-Rich/Analytical Exploration subsystems of the VL3 of the architecture (which provides the visualisation and GUI functionalities of the platform, implemented in the WP7). In summary, the WP5 was focused on the implementation of the modules included in the various layers of the AI4HEALTHSEC architecture, as previously specified by the results of the WP4. The work carried on in the WP5 is documented in 18 deliverables (9 reports and 9 demonstrators), submitted in two iterations from M17 to M30 of the project.

2.1.6 WP6

WP6 had the objective of defining and implementing a set of pilots to assess in detail if the technical objectives and KPIs developed on WP2 have been reached, and more in general, the usefulness and the effectivity of the proposed platform. The activities of the WP6 have been developed by FHG-IBMT, EBIT, KLINK, and UoB (partners of the project), who proposed 4 different pilots including 6 different use case scenarios, respectively covering the security aspects of: i) medical implants, ii) medical wearables, iii) biobanks, vi) systems acquiring, gathering, and delivering clinical data, v) real-time patient monitoring and treatment services, and vi) Health Living Labs. Moreover, the activities of the WP6 involved stakeholders from the consortium partners' networks, as well as external pilot users and end-users from standardization bodies and companies (security integrators, hospitals, and Care Centres) outside the consortium, to further assess the project's results, as well as to get their feedback to improve the proposed platform, and, finally, to disseminate the pilots' rand the project's results. The results of the pilot planning and design, exploitation and validation activities performed in the WP6 have been delivered in 3 reports, submitted from M17 to M38.

2.1.7 WP7

WP7 focused on the development of the visualization and analytical exploration sub-system of the AI4HEALTHSEC platform, on the Integration of all the AI4HEALTHSEC sub-components in a single integrated framework, on the definition of an evaluation and benchmarking methodology (including tools, instruments, and techniques for evaluating the project's results from multiple perspectives), evaluating the AI4HEALTHSEC results from different perspective. Moreover, the activities of WP7 performed an evaluation of the usability of the AI4HEALTHSEC incident handling approach and associated system. Finally, they produced a range of best practices and policy development guidelines for the wider use of the AI4HEALTHSEC incident handling approach, taking also into account the feedback from the pilots. The WP7 submitted 11 deliverables (7 reports and 4 demonstrators) until the end of the project.

2.1.8 WP8

The activities of WP8 were mainly related the dissemination and communication activities of the project, the IPR Management and Exploitation Planning, the Standardization and Certification Activities, the Market Analysis and Business Planning and, finally, the organisation of an open call for the selection of external partners for the development and exploitation of further pilots, also in different critical domains different from the Healthcare (assessing in this way a wider usability and applicability of the proposed method and platform). The details of the WP8's activities are included in 7 reports, submitted during the whole project's duration.

2.1.9 WP9

The WP9 aimed at ensuring the respect of the Ethics requirements of the project, overseeing, and addressing any issue related to the participation of humans in the project, to the protection of

personal data as well as any other ethical issue. The WP9's outputs are included in 4 deliverables, submitted from M6 to M24.

2.2 *Milestones*

The project set 23 Milestones (listed in the next Table 1), assessing the various stages of development and implementation of the proposed methodology and software platform, as well as its validation in real-world use cases. All the project's Milestones have been successfully achieved, respecting the corresponding planned deadlines.

Table 1: AI4HEALTHSEC project's milestones

Milestone number	Milestone name	WP number	Description	Achievement Month
M1	User requirements updated & Pilot Scenarios Specified	2	D2.1 and D2.3 available & delivered.	**8**
M2	AI4HEALTHSEC Architecture and Technical Specifications Available	2	D2.4 Available; AI4HEALTHSEC components technical specification available.	**8**
M3	1st AI4HEALTHSEC Self-organized SI Model Specified	3	D3.1 delivered; Specification 1st vertical layer.	**12**
M4	2nd AI4HEALTHSEC Self-organized SI Model Specified	3	D3.2 delivered; Detailed Specification 1st vertical layer.	**24**
M5	1st AI4HEALTHSEC security and privacy sub-systems Specified	3	D3.3 available with specification of the 2nd vertical layer.	**12**
M6	2nd AI4HEALTHSEC security and privacy sub-systems Specified	3	D3.4 available with all the specification of the 2nd vertical layer.	**24**
M7	1st AI4HEALTHSEC's Horizontal layers' specifications completed	4	D4.1 and D4.3 delivered; Specification of all horizontal layers.	**12**
M8	2nd AI4HEALTHSEC's Horizontal layers' specifications completed	4	D4.2 and D4.4 delivered; Detailed Specification of all horizontal layers.	**24**
M9	Simulator Specified	4	D4.5 available & delivered.	**16**
M10	1st All vertical layers implemented	5,7	D5.1, D5.2, D5.5, D5.6, D7.1 and D7.2 available & delivered.	**17**
M11	2nd All vertical layers implemented	5, 7	D5.3, D5.4, D5.7, D5.8, D7.3 and D7.4 available & delivered.	**30**

Milestone number	Milestone name	WP number	Description	Achievement Month
M12	1st All horizontal layers implemented	5	D5.9, D5.10, D5.13 and D5.14 available & delivered.	**17**
M13	2nd All horizontal layers implemented	5	D5.11, D5.12, D5.15 and D5.16 available & delivered.	**30**
M14	Simulator implemented	5	D5.17, D5.18 available & delivered.	**30**
M15	1st Pilot Operations Completed	6	D6.1 and D6.2 (accordingly) delivered.	**21**
M16	2nd Pilot Operations Completed	6	D6.3 delivered. Conclusion of pilot operations.	**38**
M17	1st AI4HEALTHSEC System Integrated	7	D7.5 and D7.6 available.	**20**
M18	2nd AI4HEALTHSEC System Integrated	7	D7.7 and D7.8 available.	**39**
M19	1st AI4HEALTHSEC Framework Validated from Stakeholders	7	D7.9 available.	**23**
M20	2nd AI4HEALTHSEC Framework Validated from Stakeholders	7, 8	D7.10 and D8.3 available.	**39**
M21	Best Practices and Policy Development Guidelines Available	7	D7.11 delivered.	**39**
M22	First AI4HEALTHSEC Results Contributed to the protection of ehealth domain	8	AI4HEALTHSEC Contributions presented/provided; D8.5 available.	**39**
M23	Open Call completed and results fully evaluated	4	D8.7 Delivered.	**38**

2.3 *Management and coordination activities*

The main coordination actions, as well as the common decisions of the consortium, have been performed in the Project Steering Committee (PSC) meetings, where all the partners, coordinated by the coordination team of the project discuss the possible issues, plan the project's activities, define the procedures, proposes the members of various committees, oversees the project's developments, and take the technical, scientific and administrative decisions about the project. The PSCs have been held regularly and anytime it was necessary (11 PSC have been organised during the project's duration) to assemble all the partners to discuss specific tasks or issues, organised as virtual meetings, in addition to the kick-off meeting, a General Assembly in presence (three days in Naples from 3 to 5 April 2023) and a final event in presence (held in Naples from 30 to 31 October 2023), where the first

day was also dedicated to a project's general meeting (some pictures of the final general assembly event are depicted in the next Figure 2-1 and Figure 2-2).

Figure 2-1. Presentation of the AI4HEALTHSEC final event by the project's coordinator Eng. Giuseppe De Pietro, director of the Institute for High Performance Computing and Networking of Research Council of Italy (ICAR-CNR)

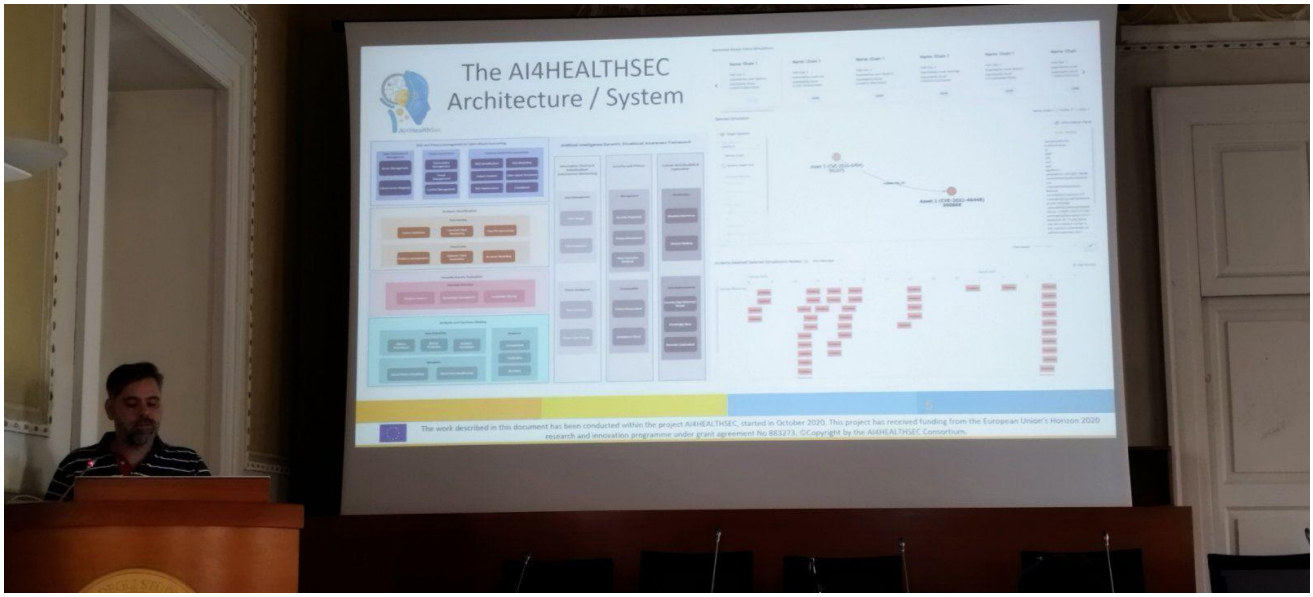

Figure 2-2. Presentation of the final AI4HEALTHSEC architecture by the project's technical coordinator, dr. Spyridon Papastergiou

Various boards and committees have been also established to control, oversee, and support the project development and address specific eventual issues: the Security Advisory Boards, the Quality Management Committee, the Privacy Committee, IPR Committee, User Advisory Board, and the External Advisory Board. These committees met up regularly to oversee their specific tasks related to the project.

The management team also coordinated the partners to develop and request the amendments required during the project's duration (mainly, to include a new partner, University of Essex, to redistribute the efforts and fundings among the partners and to extend the project's duration by three months, as well as to correct minor issues or typographical errors of the original project).

Finally, the management team oversaw and successfully managed all the financial and administrative tasks related to the project.

2.4 *Pilots*

As mentioned above, the AI4HEALTHSEC project foresaw a set of real-world pilots, to test and assess the proposed platform and related methodologies, as well as to evaluate technical objectives and KPIs of the project.

These pilots were designed, implemented, and executed by FHG-IBMT, EBIT, KLINK, and UoB (partners of the project), and not only provided the evaluation of the platform, but also allowed to collect from end users the feedback on the usability, performance, utility of the AI4HEALTHSEC platform, gathering hints for further improvements.

The proposed use cases scenarios tested in the pilot were:

- **Systems acquiring, gathering, and delivering clinical data:** Klinikum Nurnberg provided its hospital information system (HIS) for a pilot scenario.
- **Medical implants:** For this scenario, Fraunhofer IBMT provided a technology platform for programmable active implants with neuro-stimulation and neuro-monitoring functionality in novel clinical applications.
- **Medical wearables**: Fraunhofer IBMT provided a personal health system consisting of the commercial smartwatch ScanWatch of the company Withings[1], in combination with the app Corona Diary of Fraunhofer IBMT and an integration server.
- **Biobanks:** Fraunhofer IBMT developed the specimen management system UBA-PVS[2] to collect, process, store, and manage the specimen and related data. UBA-PVS is provided for this scenario.
- **Real-time patient monitoring and treatment services**: This pilot use case was based on the use of the EBIT solution SUITESTENSA VNA[3] and Portal integrated with the AI4HEALTHSEC security framework to tackle the security challenges raised at any level of the solution.
- **Health Living Labs:** The University of Brighton provided a Digital Health Living lab that is a user-centered, open innovation ecosystem based on a systematic user co-creation/ co-

[1] https://www.withings.com/de/en/scanwatch

[2] https://sourceforge.net/projects/uba-pvs/

[3] https://www.esaote.com/it-IT/healthcare-it/software-per-healthcare-it/p/suitestensa-vna/

production approach, integrating research and innovation processes in a real-life setting and reflects the European Network of Living Labs (ENoLL), Living Labs (LLs) definition.

The project management team supervised, coordinated, and supported the pilots' design and implementation, also providing the required feedback related to ethics issues, with the support of the legal team and the SAB.

Finally, the management team organised the AI4HEALTHSEC final event in Naples, Villa Doria d'Angri on 31 October 2023, presenting AI4HEALTHSEC' results, the pilots results and a live demonstration of the platform to international stakeholders invited to this event, also including an open discussion and feedback from the audience and presentations from international speakers and other projects and consortia on the specific subject of eHealth and cybersecurity.

2.4.1 Open Call

In addition to the above-described pilots, implemented by internal partners of the project and related to cybersecurity issues of the healthcare domain, the project also organised an open call to Open Call to involve external third parties not only from the healthcare domain, but also from other critical domains (transportations, energy, financial, etc.), with the purpose of developing and executing additional pilots, further testing and demonstrating the AI4HEALTHSEC services and capabilities, as well as assessing the wider usability of the proposed methods and platform in different domains, and finally getting other feedback on the platform, suggesting, services and applications to be incorporated, enhancing its efficiency, and facilitating its application to other critical domains.

The management activities of the open call preliminarily included the organisation a raising awareness workshop (organised in March 2022), as well the dissemination of the open call, also before its publication. Then, the consortium defined its objectives, the required procedures for its development and implementation, its main technical and administrative aspects, as well as the timelines (submission, evaluation, development, evaluation of the results, etc.).

When the AI4HEALTHSEC solution was sufficiently mature, the coordinator published the open call (in February 2023), also selecting external experts as reviewers of the submitted proposals (with the support of the consortium), coordinating and supporting its dissemination, implementing a website for the submission of the proposal and the management of their reviews. Seven proposals have been submitted and, at the end of the evaluation and selection, four external companies were admitted: two healthcare domain proposals come from Ethos Hub and Clynxio LDA, while other two proposals from iLink New Technologies and Dot Syntax belonged to the transportation and logistics domain.

The management team implemented all the required administrative and financial procedures related to the external partners. It also coordinated the partners of the projects, organising workshops, as well as technical meetings to support the development and implementation of the external pilots and the use of the AI4HEALTHSEC platform, and then collected their feedback and analysed the obtained results.

The external partners helped the consortium in the assessment and evaluation of the project's results, and, in summary, provided minor suggestions for the improvement of the platform, such as the provision of some additional higher-level analytics for those who do not have deep expertise in

cyber-security. Moreover, the results of the open call pilots confirmed the wider applicability of the AI4HEALTHSEC solution in domains different from the healthcare.

2.5 *Dissemination activities*

The project also implemented several effective and specific dissemination activities. AI4HEALTHSEC project results have been disseminated through traditional communication channels, such as events' attendance (conferences, workshops, etc.), publications of scientific articles in professional journals, and conference proceedings, as well as communications through the AI4HEALTHSEC website and social media posts (on Facebook, LinkedIn, Twitter and YouTube), posters, press releases, newsletters, and, finally, project's presentations to various stakeholders and the general public.

A sample of the events where the consortium participated to disseminate the project's results with specific presentations were: i) *CONCORDIA Open Door*, where stakeholders of all backgrounds (IT, entrepreneurship, education, economy, and policy) discussed societal and technological needs in the cybersecurity field and presented their competencies for potential collaboration with more than 100 partners (universities, industries, and public bodies); ii) *SMART BEAR Infoday*, a meeting organized by the EC-funded SMART BEAR project to explore the latest healthcare challenges, where presentations and discussions by experts from the Health&Care cluster of the European Commission and from well-known independent experts were provided; iii) European FIC 2023 – International Cybersecurity Forum, the largest cybersecurity and digital trust event on the continent, with 19,000 participants, 550 private and public sponsors, 520 speakers and 60 countries represented in 2022, where AI4HEALTHSEC attended different partners, also presenting the project in the pitch sessions and participating in an open discussion with attendants on the project and the developments; iv) Fifth Intersessional Consultation of the United Nations, Office on Drugs and Crime (UNODC)Ad Hoc Committee, where AI4HEALTHSEC was presented, among other cybersecurity-related projects. The next Figure 2-3, Figure 2-4, and Figure 2-5 show some of the aforementioned participations to events.

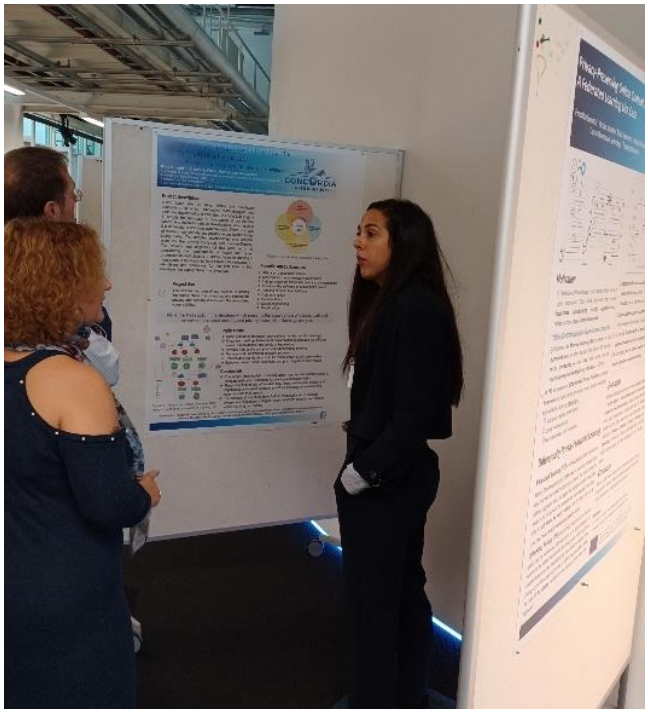

Figure 2-3. AI4HEALTHSEC presentation in CONCORDIA Open Door

Figure 2-4. AI4HEALTHSEC presentation in SMART BEAR Info Day

Figure 2-5.AI4HEALTHSEC presentation in the pitch area of FIC 2023

Moreover, the project participated in several workshops and established collaborations and/or synergies with other EC-funded projects in the domain of eHealth and cybersecurity (HIER[4], SMART BEAR[5], SENTINEL[6], CONCORDIA[7], CYBALLIANCE[8] and DANTE[9] projects).

The scientific results of the projects have been also presented in international scientific conferences, such as, among the others, the 2022 and 2023 editions of the IEEE Symposium on Computers and Communications (ISCC), the 12th International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH 2022), the 2022 and 2023 editions of the International Conference on Applied Human factors and Ergonomics, the 19th International Conference on the Design of Reliable Communication Networks (DRCN2023). The presented articles have been also published in the corresponding conference proceedings. Concerning the publication of the scientific results of the project, also 15 articles in important scientific journals have been published.

A final event of the AI4HEALTHSEC project has been held on October 31st, 2023, in Naples in Villa Doria d'Angri, co-organized with the European funded project DANTE and sponsored by the Università degli Studi di Napoli "Parthenope". This event was designed as an event targeted to the

[4] https://heir2020.eu/at-a-glance/
[5] https://www.smart-bear.eu/
[6] https://sentinel-project.eu/
[7] https://www.concordia-h2020.eu/
[8] https://cyballiance.nr.no/
[9] https://dante-edih.clustersmile.it/en/project/

health organizations in Italy and abroad, and included presentation from AI4HEALTHSEC and the DANTES projects, live demonstrations of the AI4HEALTHSEC solution and an open discussion and feedback from the audience and presentations from international speakers on the specific subject of eHealth and cybersecurity (some pictures of the event are depicted in previous Figure 2-1 and Figure 2-2, and in the following Figure 2-6 and Figure 2-7).

Figure 2-6. Dr. Dmitry Amelin presents the FHG-IBMT pilot during the AI4HEALTHSEC final event

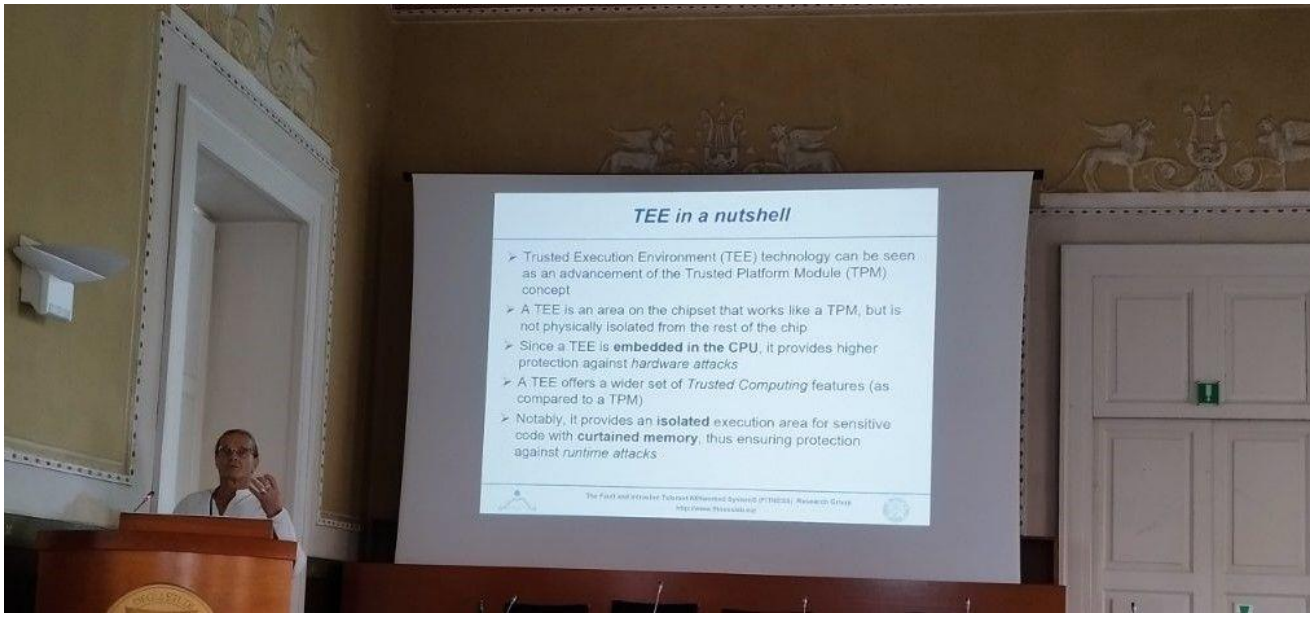

Figure 2-7. Professor Luigi Romano presents a talk on the Protected Execution Environments for eHealth applications during the AI4HEALTHSEC final event

More details on the dissemination and communication activities are available within Deliverables D8.1, D8.2 and D8.3.

2.6 *Policy and Standardisation contributions*

AI4HEALTHSEC provided feedback to relevant policies and authorities within the EU on the subjects related to those of the project, following the recommendation of the European Commission related to the to the priority "Shaping Europe's digital future", the European Commission underlines the need for digital solutions. The project defined and followed a specific methodology to achieve these aims successfully also. As results, the AI4HEALTHSEC project provided a response to the European Commission public consultation to gather the views and experiences of all relevant parties on the forthcoming European Cyber Resilience launched on March 2022 (European Cyber Resilience Act), and to the EC's public consultation to gather the views and experiences of all relevant parties on a proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2019/881 as regards managed security services (EU CSA), launched on April 2023.

Moreover, the partners of the AI4HEALTHSEC project, in collaboration with the HEIR project, provided their opinion on selected provisions of the regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union, producing a position document at adoption of the draft regulation. Some of the recommendations of the AI4HEALTHSEC project the following conclusions were included in the final published regulation.

In the case of standardisation contributions, AI4HEALTHSEC project ran an analysis of existing and developing standards in the focus areas of the project. The objective of this analysis was to become acquainted with the state of the art, to collect valuable information, to build upon them and to identify possible shortcomings. Then, the project team decided to enrich this analysis and map

standards to all the proposed measures of the NIS Cooperation Group (Reference document on security measures for Operators of Essential Services, CG Publication 01/2018 [NIS 2018]).

More details on the policy and standardisation contributions can be found in the Deliverable D7.11.

3 Finals Results and Impacts

This Section briefly presents the AI4HEALTHSEC platform, which is the main result of the project. The platform is a software framework, which integrates several modules that implements the planned functionalities for the DSAF. Moreover, we also summarise the best practises obtained from the exploitation of the project's result, and the planned exploitation.

3.1 *Final Results of the AI4HEALTHSEC project*

The main result of the project is a software framework which implement the proposed DSAF, whose architecture, with the corresponding functionalities, are depicted in Figure 3-1. The architecture includes 4 Horizontal Layers (HLs), where the main functionalities related to the cybersecurity are implemented (HL1: Risk and Privacy Management & Cyber Attack Forecasting, HL2: Incident Identification, HL3: Security Events Evaluation, HL4: Analysis and Decision Making), and 3 Vertical Layers (VLs), where the common functionalities used by all the HLs have been realised (VL1: Information Sharing & Individualised Autonomous Networking, VL2: Security and Privacy, VL3: Context-Rich/Analytical Exploration).

Following this conceptual architecture, the activities carried out during the project development allowed to design, implement, and deploy the software modules (whose main functionalities are also depicted in Figure 3-1), which have been finally integrated in a framework represented by the AI4HEALTHSEC platform.

This platform provides the planned cybersecurity functionalities, realising the awareness and communications systems and the AI-based analytics, also offering the GUI to be used as interface and the dashboards for the analysis of the obtained results. The platform does not require to install any module on the HCII or the ICT infrastructure where is applied, but is capable to provide its services remotely, requiring only the details of the assets of the infrastructure and their logs. Some examples of the GUI and the results obtained using the AI4HEALTHSEC platform (from the pilots) are depicted in the next Figure 3-2, Figure 3-3, and Figure 3-4.

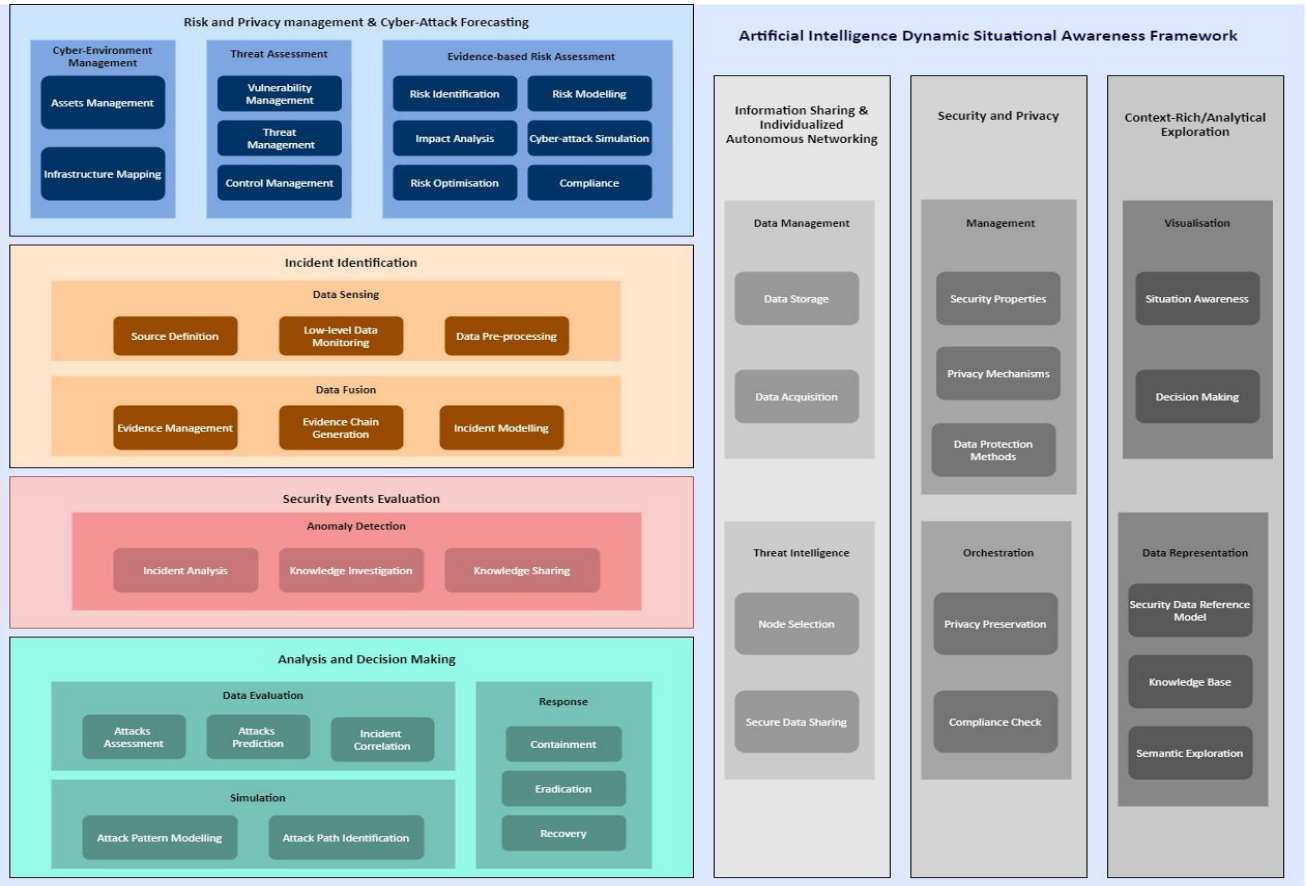

Figure 3-1. AI4HEALTHSEC framework architecture

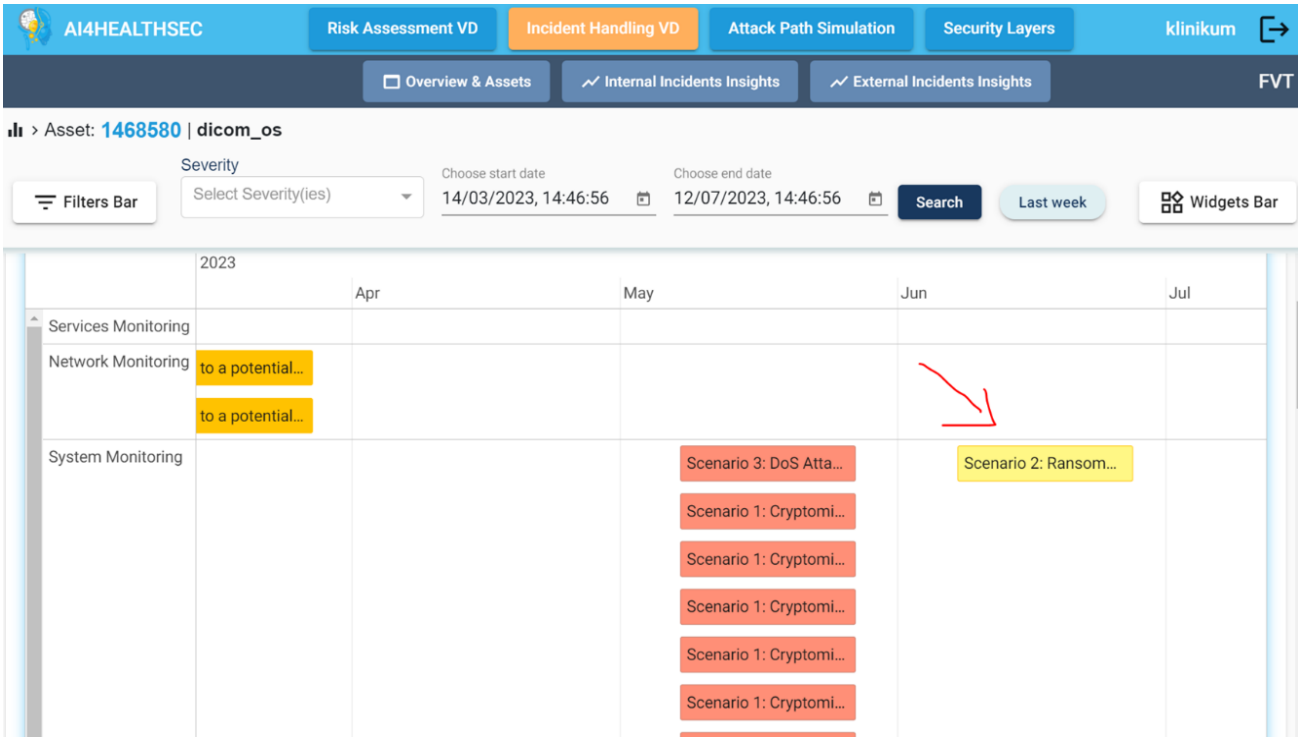

Figure 3-2. AI4HEALTHSEC platform's GUI: Incident Handling of Ransomware Attack Scenario

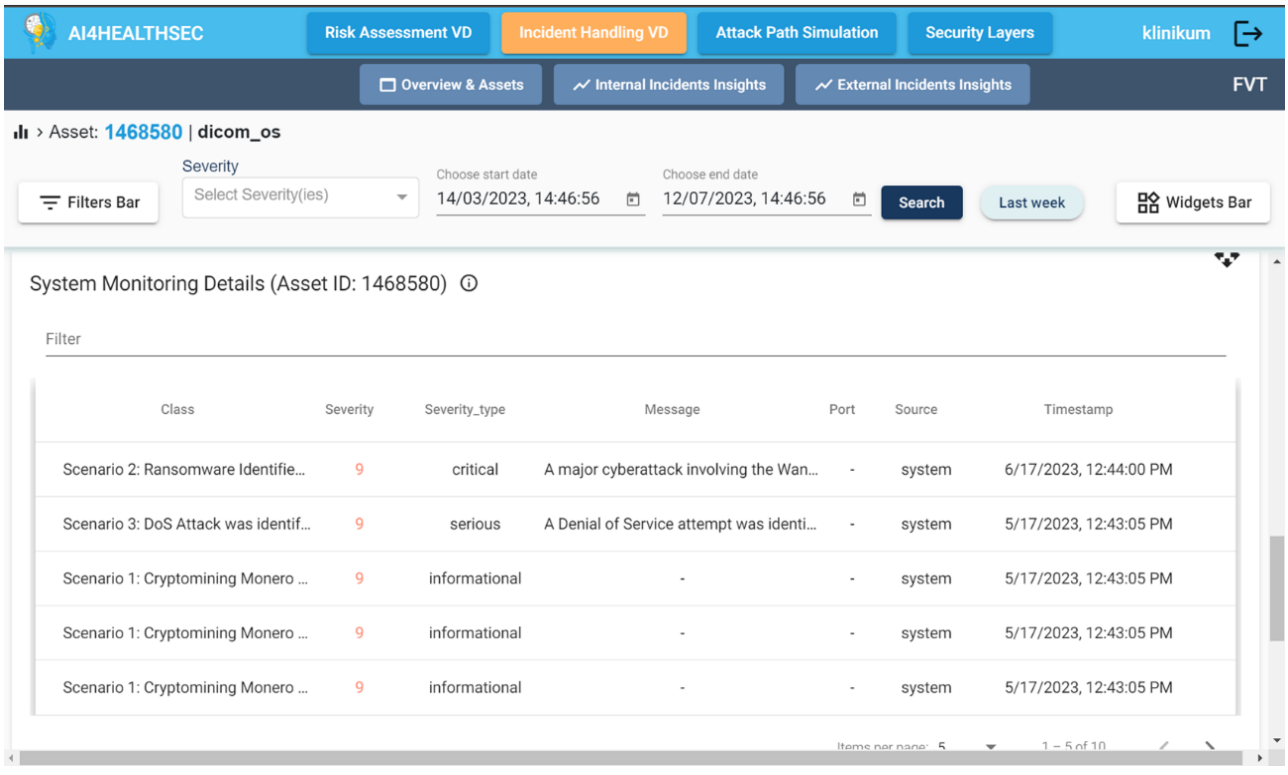

Figure 3-3. AI4HEALTHSEC platform GUI: Incident Handling dashboard

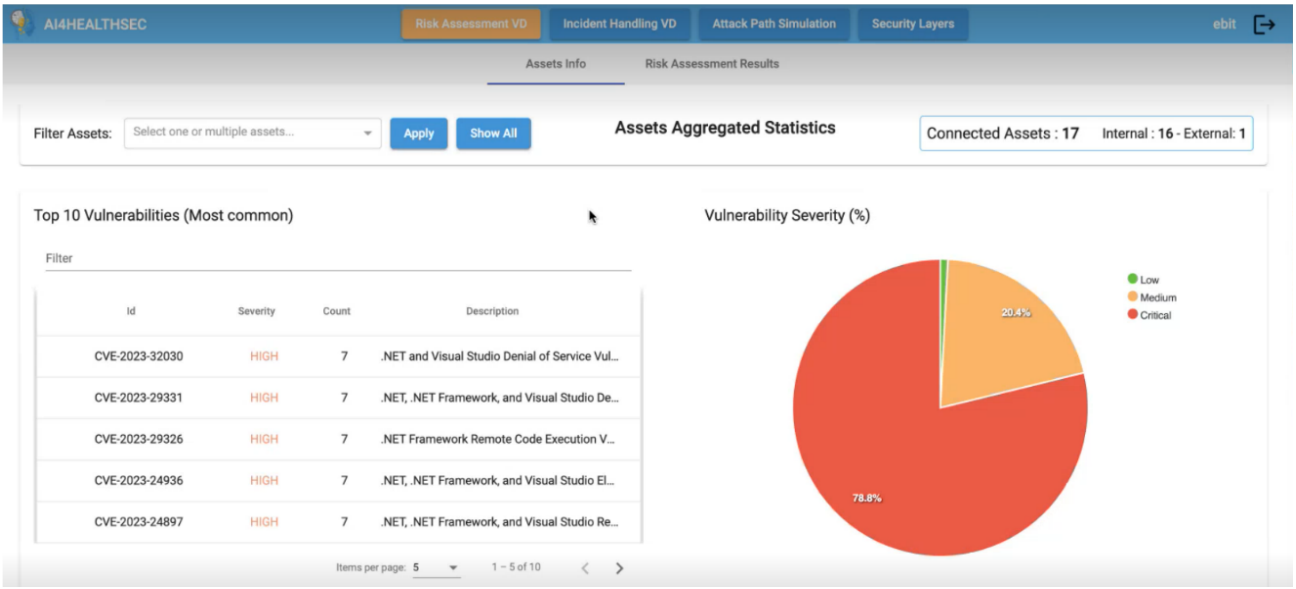

Figure 3-4. AI4HEALTHSEC platform GUI: Risk Assessment report

3.2 *Impact of the results of the project*

In the various cybersecurity scenarios outlined within the AI4HEALTHSEC project (in particular, from pilots' scenarios), several lessons have been learned, as well as best practices that can be applied to enhance security measures, detect threats, and respond effectively to incidents.

In the case of biobank, understanding common attack methods was vital to safeguard sensitive biological data and maintain the integrity of their operations. Biobank encountered a scenario involving failed password logins, where an attacker attempted unauthorized access through various techniques, such as dictionary attacks. Implantable Medical Devices pilot underlined that the attacks to this type of medical devices can also have impacts on the health of a patient, i.e. by discharging rapidly the batteries of the device. In this case, it has been showed that a deep learning model could detect this behaviour, demonstrating the usability of AI-based approaches for their identification and classification. For the wearables pilot, the results of the application of the AI4HEALTHSEC platform showed that a brute force attack with several failed password logins is critical, and the platform is very useful to analyse and mitigate the related risks.

The scenarios tested in the Klinikum pilot demonstrated the AI4HEALTHSEC platform's capability in a real hospital environment and assessed the need of increasing the awareness about cyber security of the medical personnel; moreover, it showed the vulnerabilities and the attack paths for common cases that can be crucial for the operations of the IT systems of an hospital.

The EBIT pilots showed that the details provided by the AI4HEALTHSEC solution, which provides the timestamp, hostname, and user information of unauthorised access attempts, can enable the security teams to investigate the incidents, assess its impacts, and implement appropriate remediation measures, also underlining the importance of the measures to identify and respond promptly to such

incidents. Furthermore, the results of the EBIT pilot assessed the effectiveness and utility of the Machine Learning Intrusion Detection System for the analysis of anomalies in network traffic patterns, suggesting potential malicious activities such as malware infections, unauthorized network access, or unusual data transfer patterns.
The Living Lab scenarios provided logs that acted as a forensic trail, allowing security teams to investigate and respond promptly to any suspicious behaviour, safeguarding user privacy and the integrity of the smart home environment. Moreover, the attack chains identified by the platform, demonstrated that an individual risk and vulnerability assessment can improve the security of the systems, identifying and mitigating the assets' threats that represents a weak point in a complex interconnected ecosystem.
The impact of the open call pilots was firstly the assessment of the larger applicability of the AI4HEALTHSEC solution, proving its applicability in sectors different from the healthcare. In the case of the open call pilot project implemented by Clynxio external partner, AI4HEALTHSEC platform assisted them in identifying the nature and source of potential vulnerabilities and threats to their network, suggesting that a list of relevant and common attacks and vulnerabilities could strengthen a company's or an organisation's security against cyber threats. The Ethos Hub scenarios of the open call showed that the combined use of valuable resources such as NIST, CVE and others, integrated into the AI4HEALTHSEC platform, can provide the users with additional credible information regarding common vulnerabilities and exposures. The iLink New Technologies open call pilot demonstrated that AI4HEALTHSEC offers high business value in vertical sectors, highlighting the importance of self-assessment and optimization of micro-tasks and larger operations within an organisation. Finally, the Dot Syntax scenario showed that the detailed evaluation of the system's assets and the detection of the attack by utilising the features of the AI4HEALTHSEC platform allowed to validate the smooth co-existence of legacy OT and IT equipment with state-of-the-art cyber-security technologies in critical operation environments of high availability restrictions.

3.3 *Applicability and exploitation of the project results*

The management activities performed in this context allowed to identify the KERs of the project, their owners, and all the main IPR eventual issues. The AI4HEALTHSEC partners provided the required feedback regarding the IPR preferences, also providing their input about the post-project commercialization strategy, which could be applied not only to the overall integrated AI4HEALTHSEC platform, but also to single services and subsystems.
Moreover, it was also defined the sustainability plans for the pilots, to assist in the maintenance and extension of an existing software product beyond its intended lifespan and setup standards for the potentially reusable parts.
Finally, a strategy for the replication and the wider use of the deployments was defined, to facilitate and guide the replication of the AI4HEALTHSEC platform within the system of external organisations.