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"

D8.3 – Report on Dissemination and Communication Activities version 2

Due date of deliverable: 31.12.2023
Actual submission date: 31.12.2023

Grant agreement number: 883273
Start date of project: 01/10/2020
Revision 1

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	X
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	

D8.3 – Report on Dissemination and Communication Activities version 2

Editor

Argyro Chatzopoulou (TUV)

Contributors

Karras Apostolos (TUV)
Stylianos Karagiannis (PDMFC)
Djordje Djokic (PN)
Dmitry Amelin (FHG-IBMT)
Georgios Chatzivasilis (STS)
Jihane Najar (AEGIS)
Mario Ciampi, Stefano Silvestri, Rita Capasso (CNR)
Shareeful Islam (FP)
Efstathios Karanastasis (ICCS)
Efthymios Chondrogiannis (ICCS)
Theodora Varvarigou (ICCS)
Evangelos Psomakelis (ICCS)
Eftychia Lakka (FORTH)
Kitty Kioskli (UOE)
Haris Mouratidis (UOE)
Lena Griebel (KLINIK)
Marco Fruscione (EBIT)
Ernst Hermens (PHILIPS)

Reviewers

Manos Athanatos (FORTH)
Anca Bucur (PHILIPS)

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

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
0.1	1/11/2023	Argyro Chatzopoulou Apostolos Karras	Initial Draft Version
0.2	15/12/2023	Argyro Chatzopoulou Apostolos Karras	Comments by project partners
0.3	28/12/2023	Argyro Chatzopoulou Apostolos Karras	Updates based on the results of the quality review
1.0	29/12/2023	Argyro Chatzopoulou Apostolos Karras	1st version for publication

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 is the second version of the report on the communication and dissemination of the AI4HEALTHSEC project results to the general public, other organizations and the academic community. The file includes the description of the main activities performed by the consortium partners towards the related propagation efforts that were carried out for the period Month 20 to the end of the project.

The aim of this report is to provide the updates of the activities to publicize the work carried out by the project, including the list of performed activities.

This (second version) of the report complements two documents previously delivered. Specifically, the document D8.1 – Dissemination and Communication Plan, delivered on 31/03/2021 and the document D8.2 – Report on Dissemination and Communication Activities version 1, delivered on 31/05/2022. The D8.2 – Report on Dissemination and Communication Activities version 1, describes the activities of the project related to dissemination and communication until the 18th of May 2022 (mid M20). This report, picks up the storyline from there and describes the activities of the project regarding dissemination and communication from M20 till the end of the project.

This report provides an overview of the propagation efforts of the AI4HEALTHSEC project through traditional communication channels such as event attendance (conferences, workshops, etc.), project publications (articles in professional journals, etc.), social media posts (on Facebook, LinkedIn and Twitter) and project presentations (to various stakeholders and the general public). Visibility and social media engagement data are also provided in this document.

TÜV TRUST IT coordinates AI4HEALTHSEC communication and dissemination activities, nevertheless, all the project partners are responsible to disseminate AI4HEALTHSEC results through their communication channels and towards their existing communities and have contributed to the development of this document.

Contents

List of acronyms

Acronym	Description
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
EMD	Electronic Medical Devices
GCS/ΕΠΥ	The Greek Computer Society
HCII	Health Care Information Infrastructure
HOU	Hellenic Open University
ICT	Information and Communication Technology
NMIOTC	NATO Maritime Interdiction Operational Training Centre
ME	Micro Enterprises
OWASP	Open Web Application Security Project
PAS	Panhellenic Hematology Conference
RAMA	Risk Assessment of Medical Applications
SDO	Standards Developing Organizations
SME	Small Medium Enterprises
UniWA	University of West Attica
UTH	University of Thessaly
WP	Work package

List of tables

List of figures

1 Introduction

The purpose of this report is to provide an accounting of the efforts performed by the consortium partners from the 20th month of the project until the project end, regarding communication and dissemination of the AI4HEALTHSEC project.

The activities are either managed by the consortium (e.g. social media accounts, website and newsletter) or hosted by external actors (e.g. conferences, EU events, etc). In both cases, partners of the AI4HEALTHSEC consortium are actively involved.

This (second version) of the report complements two documents previously delivered. Specifically, the document D8.1 – Dissemination and Communication Plan, delivered on 31/03/2021 - which established and defines the activities for the visibility and communication of the project, aiming to spread all the activities carried out during the project lifetime and achieve maximum impact - and the document D8.2 – Report on Dissemination and Communication Activities version 1, delivered on 31/05/2022. The D8.2 – Report on Dissemination and Communication Activities version 1, describes the activities of the project related to dissemination and communication until the 18th of May 2022 (mid M20). This report, picks up the storyline from there and describes the activities of the project regarding dissemination and communication from M20 till the end of the project.

This document is structured as follows:

Section 2. provides a high level description of the progression of the Dissemination and Communication planning of the project and a presentation of the dissemination and communication plan for the third year of the project.

Section 3. presents the results of the project through the utilization of traditional communication channels.

Section 4. presents the results of the project through the utilization of online channels (social media, the website, the newsletters and the videos).

Section 5. presents the publications of the project in professional journals & conferences.

Section 6. presents an overview of the project's performance against the dissemination and communication KPIs and

Section 7. includes some closing remarks and conclusions.

2 Dissemination and Communication planning for the 3rd year

Deliverable D8.1, Dissemination and Communication Plan, issued on M6 of the project, presented the initial activities that the project would design to address the subjects of dissemination and communication. After the first review period had elapsed and taking into consideration the comments and recommendations of the first technical review, a further plan was drafted and initiated for the second year of the project. The information regarding the planning for the second year of the project is included in D8.2.

Figure 2-1 displays the different components of the dissemination and communication plan for the AI4HEALTHSEC project within the project duration, as described in the Dissemination and Communication Plan (D8.1). The first year was more focused in the establishment of the communication tools and in the awareness of the project existence to the general public. For the second year, the activities moved towards the communication of the project initiatives and outcomes, whereas the plan for the last year of the project was to focus in the more refined dissemination of the open call, the implementation outcomes, the demonstrators and publications.

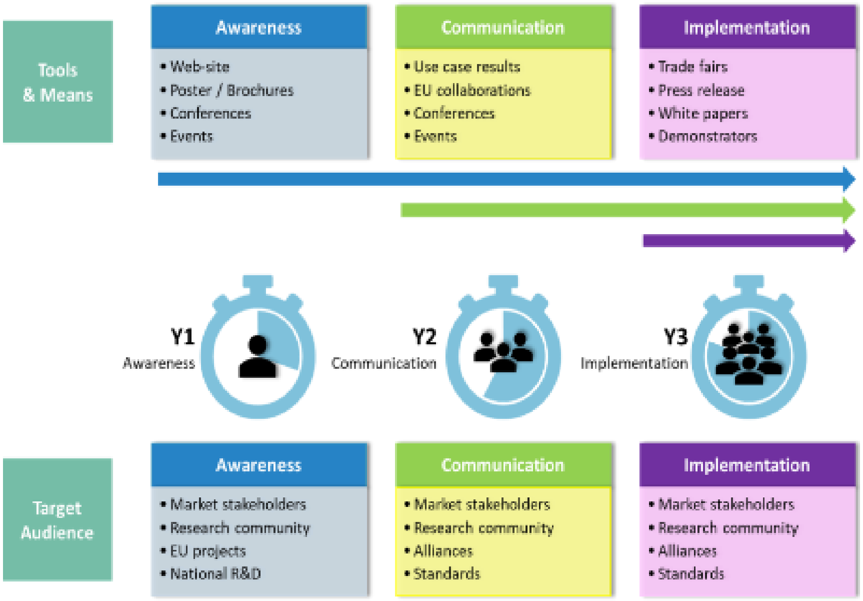


Figure 2-1. An overview of the Tools, means and audience of the dissemination plan of AI4HEALTHSEC project

Table 2-1 contains the activities and directions that have been planned for the Dissemination and Communication of the project within the third and last year of the project.

Objective		Methods
Communication Year 3	• Implementation of the project's outcomes. • Generation of marketing material to target industrial stakeholders. • Promote the solution through live demonstration to the relevant stakeholders.	• Creation of videos describing the components of the AI4HEALTHSEC solution. • Creation of video describing the AI4HEALTHSEC solution, its added value and the benefits for its different stakeholders. • Publication of papers/articles in scientific journals. • Participation in both scientific and industrial events to promote the project and showcase the latest outcomes. • Organizing workshops where outcomes can be presented and reviewed by interested groups. • Collaboration with other EU funded projects within the same subject. • Produce a newsletter at least twice within this third year. • Organization of a workshop within a scientific event. • Publication of the results in the website and the social media of the project. • Generation of workshops / training sessions. • Demonstration of the benefits of the AI4HealthSec solution through the real-world use cases identified. • Promote and support the implementation of the open call. • Analysis of the KPIs regarding dissemination and communication.

Table 2-1. Dissemination and Communication Plan – 3rd year of the project

Moreover, from a management point of view, and in order to mitigate the risks related to poor dissemination and communication performance, the following activities were decided to be implemented:

- Adoption of a specialized tool to facilitate the more organized dissemination of information through the social media channels of the project.
- Establishment of a communication group with the participation of at least one representative from each partner. The objective of the communication group is to improve the management of the communication and dissemination activities of the project, to enhance the flow of information between the partners and to support the decision-making processes.
- Implementation of a regular (monthly) meeting of the communication group.
- Enhancement of the information collected through the relevant file within Basecamp.
- Activation of all partners in relation to Dissemination and Communication.
- Increase the efforts for collaboration with other projects.

3 Traditional communication channels

This section provides an overview of the dissemination and communication activities carried out by the project, through traditional communication channels. Such channels and activities include:

1. Events (physical or virtual)
2. Conferences
3. Workshops
4. Collaboration with other projects

For each one of these channels, a separate subsection is included within this section. It should be noted, that the activities described only cover the ones carried out between Month 20 and the end of the project.

3.1 *Events*

This section provides an accounting of the events attended or organized by the Ai4HealthSec project. In summary, the project partners participated in **8*** events, of which **2** were organized (or co-organized) by the project within the reporting period. In section 7. the KPIs for the entire duration of the project are presented. * It should be noted that the project partners attended or participated also in conferences and workshops which are not counted or depicted here (to avoid duplication). The workshops are depicted in section 3.2 and the conferences are presented in 5.1.3.

3.1.1 CONCORDIA Open Door

The CONCORDIA open door event 2022[1], was the last open-door event of the CONCORDIA project. The event took place physically and virtually (hybrid), on the 26th and 27st of October 2022, at Giesecke+Devrient HQ in Munich, Germany.

The CONCORDIA Open Door (COD) is an opportunity for stakeholders of all backgrounds (such as IT, entrepreneurship, education, economy, and policy) to discuss societal and technological needs in the cybersecurity field and for participants to discover others' competencies for potential collaboration with more than 100 partners (universities, industries, and public bodies).

Different partners from the Ai4HealthSec project attended this open-door event and UoE/UoB participated with a poster presentation on the subject "A privacy-by-design approach to model supply chain of a Living Lab".

[1] https://opendoor.concordia-h2020.eu/2022/

Figure 3-2. Photos from the poster presentation interactions and one of the panels of the CONCORDIA open door 2022

3.1.2 SMART BEAR Infoday

The H2020 project SMART BEAR, organized on information day[2] to explore the latest healthcare challenges. The event took place on the 26th of July 2023 in Sala Napoleonica, in Milano, Italy.

During the event, presentations and discussions by experts from the Health&Care cluster of the European Commission and from well- known independent experts were provided. The topics included covered: AI development, healthcare standards, interoperability, innovation, and collaboration.

The AI4HealthSec project attended this event through different partners and CNR delivered on behalf of Ai4HealthSec Project a keynote presentation with the title: "Cyber Threat Analysis Using Natural Language Processing for a Secure Healthcare System" in the session: Artificial Intelligence in Healthcare. State-of-play in the EC H&C cluster, future perspectives.

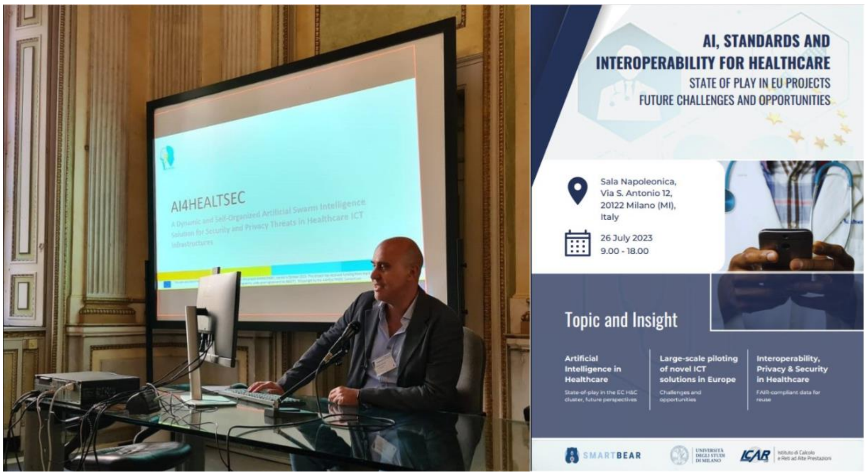

AI4HEALTSEC
AI, STANDARDS AND
INTEROPERABILITY FOR HEALTHCARE
STATE OF PLAY IN EU PROJECTS
FUTURE CHALLENGES AND OPPORTUNITIES
Sala Napoleonica,
Via S. Antonio 12,
20122 Milano (MI),
Italy
26 July 2023
9.00 - 18.00
Topic and Insight
Artificial Intelligence in Healthcare
State-of-play in the EC H&C cluster, future perspectives
Large-scale piloting of novel ICT solutions in Europe
Challenges and opportunities
Interoperability, Privacy & Security in Healthcare
FAIR-compliant data for reuse
SMARTBEAR
UNIVERSITÀ DEGLI STUDI DI MILANO
ICAR
Istituto di Calcolo e Reti ad Alte Prestazioni

Figure 3-3. Photos from the keynote presentation of Mr. Stefano Silvestri and the banner of the Information Day.

[2] https://www.smart-bear.eu/general-meeting-and-information-day/

3.1.3 Joint Webinar for Cybersecurity in Healthcare

The healthcare sector is facing an increasing number of cyber threats, as the digitisation of healthcare and the use of connected medical devices continue to grow. These threats can come from a variety of sources, including malicious hackers, nation-state actors, and even insiders. Cybersecurity incidents in healthcare can have serious consequences, including the loss or theft of sensitive patient data, disruption of vital services, and damage to an organisation's reputation. Safeguarding CybersEcurity iN hEalthcare aims to bring together viewpoints from diverse areas to explore the commonalities of cybersecurity issues and solutions in the healthcare sector.

Taking the above as an input, a webinar was organized on the subject of "Cyber Security Challenges In Healthcare Environments" on the 26th of April 2023. The webinar was presented online and was supported by the EU-funded projects AI4HealthSec, HEIR, AERAS and SMART-BEAR.

The AI4HealthSec project attended this event through different partners and FOCALPOINT presented the Ai4HealthSec project and participated in the relevant Q&A session.

HEIR
AERAS
SMARTBEAR
WEBINAR
26 April 2023 11:00 CEST
CYBER SECURITY CHALLENGES IN HEALTHCARE ENVIRONMENTS
REGISTER NOW!
Funded by the European Union

Figure 3-4. Screenshot from the invitation to register in the Joined Webinar for Cybersecurity in Healthcare

The above-mentioned activity was supported by the activation of a service of the Horizon Results Booster platform by the project HEIR.

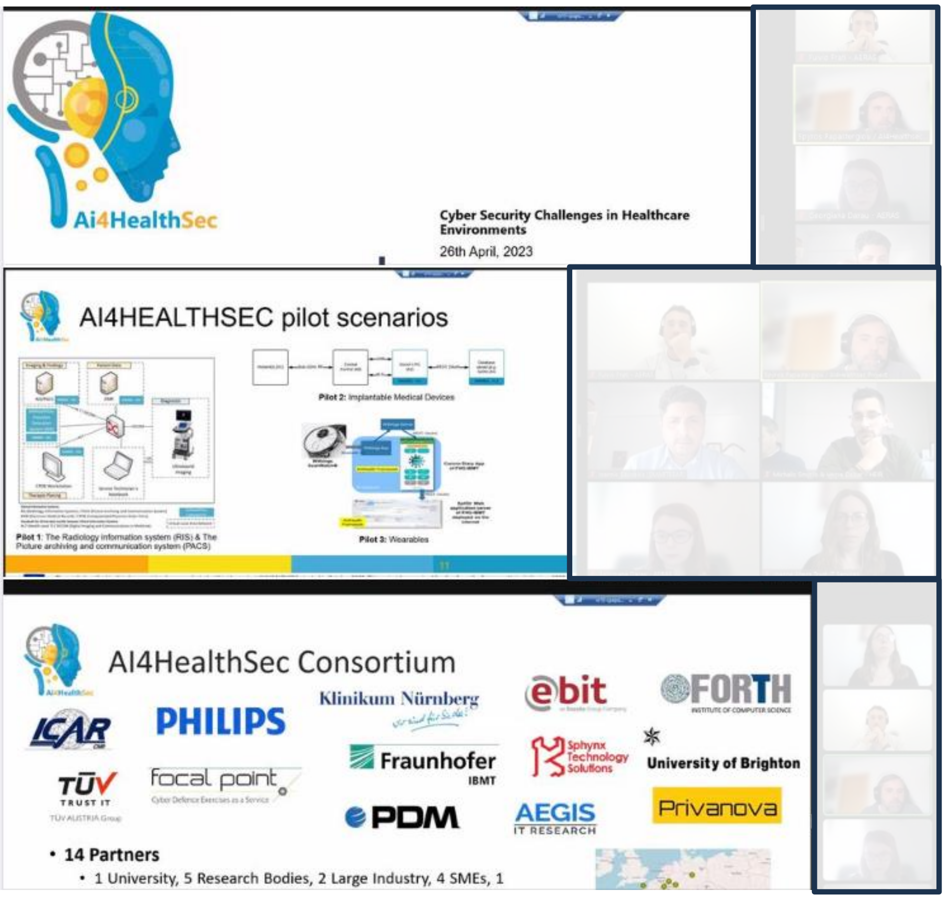
Specifically, the Module A - Identifying and creating the portfolio of R&I project results for the following project HEIR 883275 was activated and Ai4HealthSec participated in the activity as a member of the group of projects.

The project team members were identified as:

Project	Name	Organisation	email
HEIR	Herve Debar Michalis Smyrlis	IMT Sphynx Technology Solutions	herve.debar@telecom-sudparis.eu smyrlis@sphynx.ch
AERAS	Fulvio Frati	University of Milan	Fulvio.frati@unimi.it
AI4HEALTHSEC	Argyro Chatzopoulou	TUV Austria	Argyro.chatzopoulou@tuv.at
E-CORRIDOR	Fabio Martinelli	Istituto di Informatica e Telematica	fabio.martinelli@iit.cnr.it
SMART BEAR	Ioannis Basdekis	Sphynx Technology Solutions	i.basdekis@sphynx.ch

Figure 3-5. Table showing the members of the group of projects under the HSBooster service

and the implementation and promotion of the event was supported by the HSBooster service. More information on the outcomes (briefs) of this activity are presented under the Project publications section.



Cyber Security Challenges in Healthcare Environments
26th April, 2023

AI4HEALTHSEC pilot scenarios

Pilot 1: The Radiology information system (RIS) & The Picture archiving and communication system (PACS)

Pilot 2: Implantable Medical Devices

Pilot 3: Wearables

AI4HealthSec Consortium

- **14 Partners**
  - 1 University, 5 Research Bodies, 2 Large Industry, 4 SMEs, 1

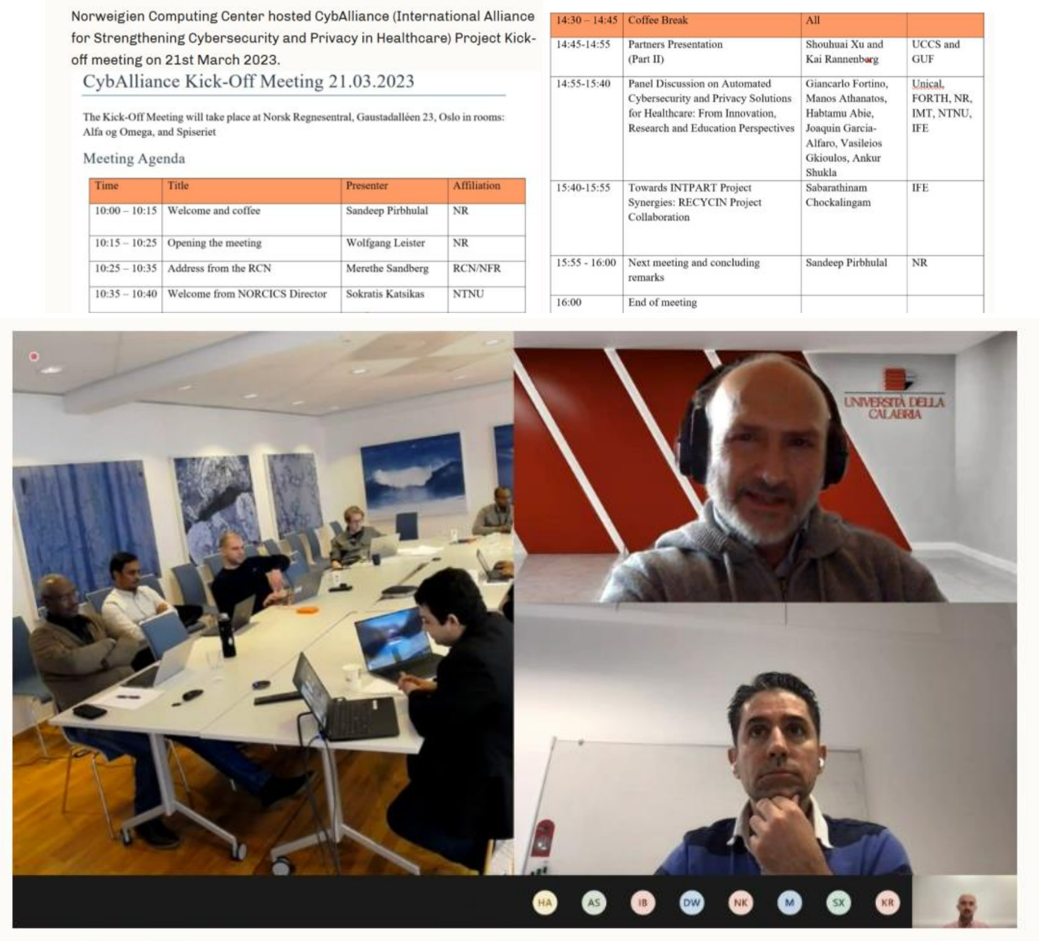
Figure 3-6. Photos from the presentation of Ai4HealthSec at the Joined Webinar for Cybersecurity in Healthcare

3.1.4 CybAlliance project kick-off meeting

The Kick-off meeting of the CybAlliance[3] (International Alliance for Strengthening Cybersecurity and Privacy in Healthcare) project, took place on the 21st March 2023 at NR (Gaustadalleen 23A Kristen Nygaards hus, 0373 Oslo).

Specifically, the kick-off meeting hosted personalities from around the world and covered, not only the project kick-off activities but also a panel discussion on Automated Cybersecurity and Privacy Solutions for Healthcare: From Innovation, Research and Education Perspectives.

FORTH participated in the panel and presented the developments of the Ai4HealthSec project.



Norweigien Computing Center hosted CybAlliance (International Alliance for Strengthening Cybersecurity and Privacy in Healthcare) Project Kick-off meeting on 21st March 2023.

CybAlliance Kick-Off Meeting 21.03.2023

The Kick-Off Meeting will take place at Norsk Regnesentral, Gaustadalléen 23, Oslo in rooms: Alfa og Omega, and Spiseriet

Meeting Agenda

Time	Title	Presenter	Affiliation
10:00 – 10:15	Welcome and coffee	Sandeep Pirbhulal	NR
10:15 – 10:25	Opening the meeting	Wolfgang Leister	NR
10:25 – 10:35	Address from the RCN	Merethe Sandberg	RCN/NFR
10:35 – 10:40	Welcome from NORCICS Director	Sokratis Katsikas	NTNU
14:30 – 14:45	Coffee Break	All	
14:45-14:55	Partners Presentation (Part II)	Shouhuai Xu and Kai Rannenberg	UCCS and GUF
14:55-15:40	Panel Discussion on Automated Cybersecurity and Privacy Solutions for Healthcare: From Innovation, Research and Education Perspectives	Giancarlo Fortino, Manos Athanatos, Habtamu Abie, Joaquin Garcia-Alfaro, Vasileios Gkioulos, Ankur Shukla	Unical, FORTH, NR, IMT, NTNU, IFE
15:40-15:55	Towards INTPART Project Synergies: RECYCIN Project Collaboration	Sabarathinam Chockalingam	IFE
15:55 - 16:00	Next meeting and concluding remarks	Sandeep Pirbhulal	NR
16:00	End of meeting		

Figure 3-7. Photos from the CybAlliance kick-off meeting and the schedule of the event

3.1.5 FIC

In its 15 years of existence, the European FIC – International Cybersecurity Forum[4] – has become 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. Thanks to the support of

[3] https://cyballiance.nr.no/

[4] https://incyber.org/en/fic-2023-detailed-programme/

the Quebec, Canadian and French authorities, the event is crossing the Atlantic to become a biennial event alternating between Europe and the American continent.

The 2023 iteration of the FIC took place on 5,6 and 7 of April in Lille, France.

The AI4HealthSec project attended this event through different partners. Moreover, partners FOCALPOINT and FORTH presented the Ai4HealthSec project in the pitch sessions and participated in an open discussion with attendants on the project and the developments.

Figure 3-8. Photos from the presentation of the Ai4HealthSec project in the Pitch area of the FIC.

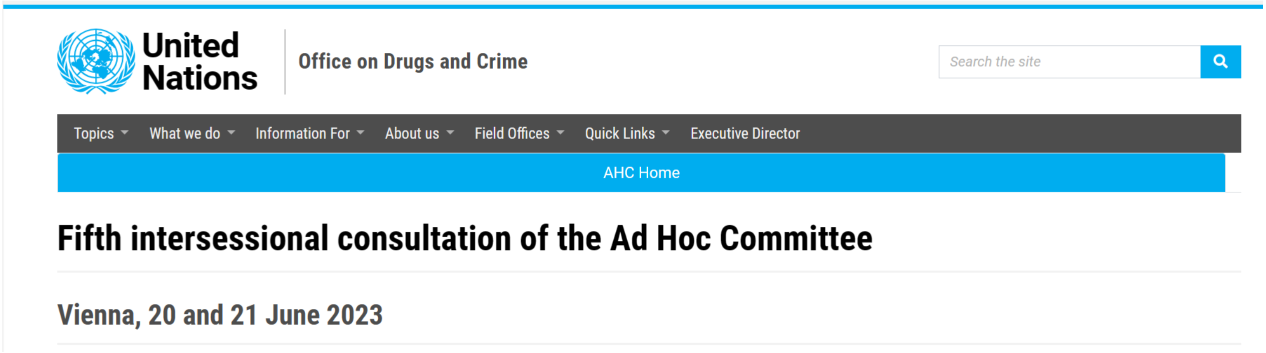
3.1.6 Fifth Intersessional Consultation of the UNODC Ad Hoc Committee

In paragraph 2 of resolution 74/247, the United Nations, Office on Drugs and Crime General Assembly decided to establish the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. Furthermore, in paragraph 10 of resolution 75/282, the General Assembly further decided to encourage the Chair of the Ad Hoc Committee to host intersessional consultations to solicit inputs from a diverse range of stakeholders on the elaboration of the draft convention.

AI4HEALTHSEC was presented, among other cybersecurity-related projects, during the Fifth intersessional consultation of the Ad Hoc Committee[5], currently taking place at the UN General Assembly in Vienna on June 20th and 21st, 2023.

[5] 5th-intersessional-consultation (unodc.org)

The project partner Privanova is a member of this Committee and was able to deliver this presentation.



Fifth intersessional consultation of the Ad Hoc Committee

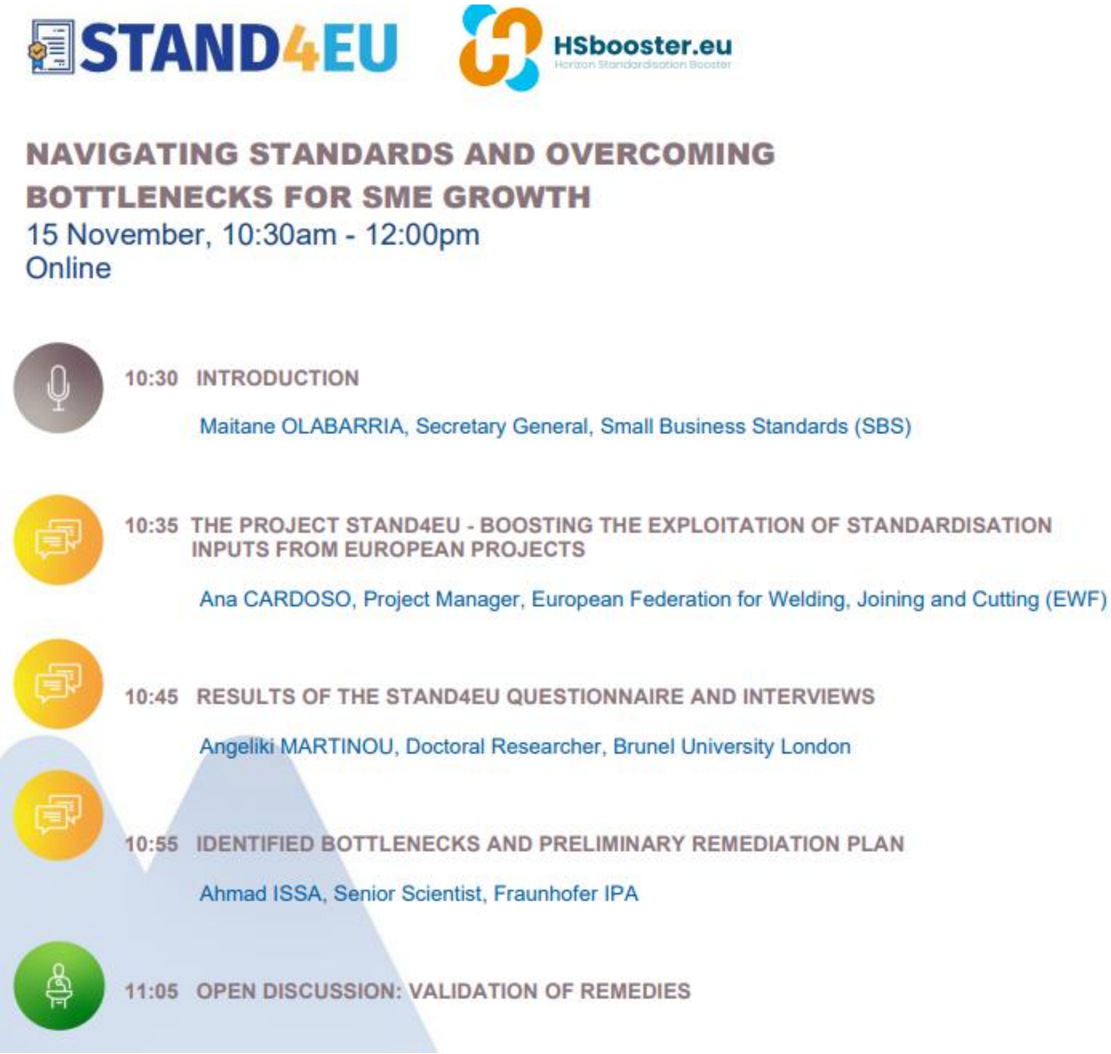
Vienna, 20 and 21 June 2023

Figure 3-9. Screenshot from the webpage of UN.

3.1.7 Navigating standards and overcoming bottlenecks for SME growth

STAND4EU and HSbooster.eu has co-organized an online Workshop entitled “Navigating standards and overcoming bottlenecks for SME growth”. The workshop took place on Wednesday 15 November, from 10:30 am to 12 pm CET. During the interactive workshop, the obstacles identified by STAND4EU in the interplay between research, innovation and standardisation were presented and the participants were allowed to contribute to shaping recommendations on how to make the standards development process more efficient. This event is part of the Meeting Standards campaign organised by Small Business Standards to raise awareness of the importance of standardisation and facilitate knowledge sharing among SMEs.

The AI4HealthSec project attended this event through the attendance and active participation of the project partner TUV.



NAVIGATING STANDARDS AND OVERCOMING BOTTLENECKS FOR SME GROWTH
15 November, 10:30am - 12:00pm
Online

10:30 INTRODUCTION
Maitane OLABARRIA, Secretary General, Small Business Standards (SBS)

10:35 THE PROJECT STAND4EU - BOOSTING THE EXPLOITATION OF STANDARDISATION INPUTS FROM EUROPEAN PROJECTS
Ana CARDOSO, Project Manager, European Federation for Welding, Joining and Cutting (EWF)

10:45 RESULTS OF THE STAND4EU QUESTIONNAIRE AND INTERVIEWS
Angeliki MARTINOU, Doctoral Researcher, Brunel University London

10:55 IDENTIFIED BOTTLENECKS AND PRELIMINARY REMEDIATION PLAN
Ahmad ISSA, Senior Scientist, Fraunhofer IPA

11:05 OPEN DISCUSSION: VALIDATION OF REMEDIES

Figure 3-10. Screenshot from the event agenda.

3.1.8 Ai4HealthSec final event

The final event of the project took place in Naples, on the 31st of October 2023[6]. This final event was co-organized with the European funded project DANTES[7] and was sponsored by the Università degli Studi di Napoli "Parthenope"[8]. Attendance was possible both physically as well as virtually (hybrid event).

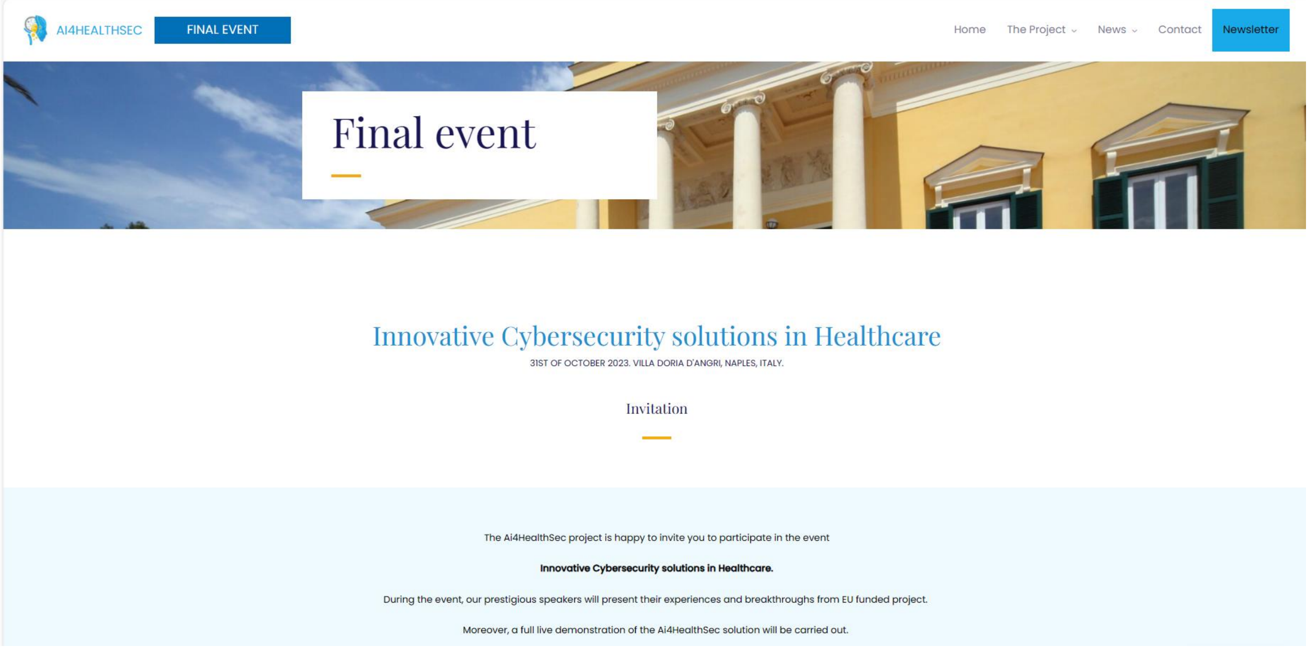
[6] https://www.ai4healthsec.eu/final-event/

[7] https://dante-edih.clustersmile.it/

[8] https://www.uniparthenope.it/Portale-Ateneo/chi-siamo

The event was designed as an event targeted to the health organizations in Italy and abroad. The agenda of the event 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.

A special page within the website of the Ai4HealthSec project was created, to provide information to participants on the final event. The registration to the event and the agenda were available also through this page[9].



Final event

Innovative Cybersecurity solutions in Healthcare

31ST OF OCTOBER 2023. VILLA DORIA D'ANGRI, NAPLES, ITALY.

Invitation

The Ai4HealthSec project is happy to invite you to participate in the event

Innovative Cybersecurity solutions in Healthcare.

During the event, our prestigious speakers will present their experiences and breakthroughs from EU funded project.

Moreover, a full live demonstration of the Ai4HealthSec solution will be carried out.

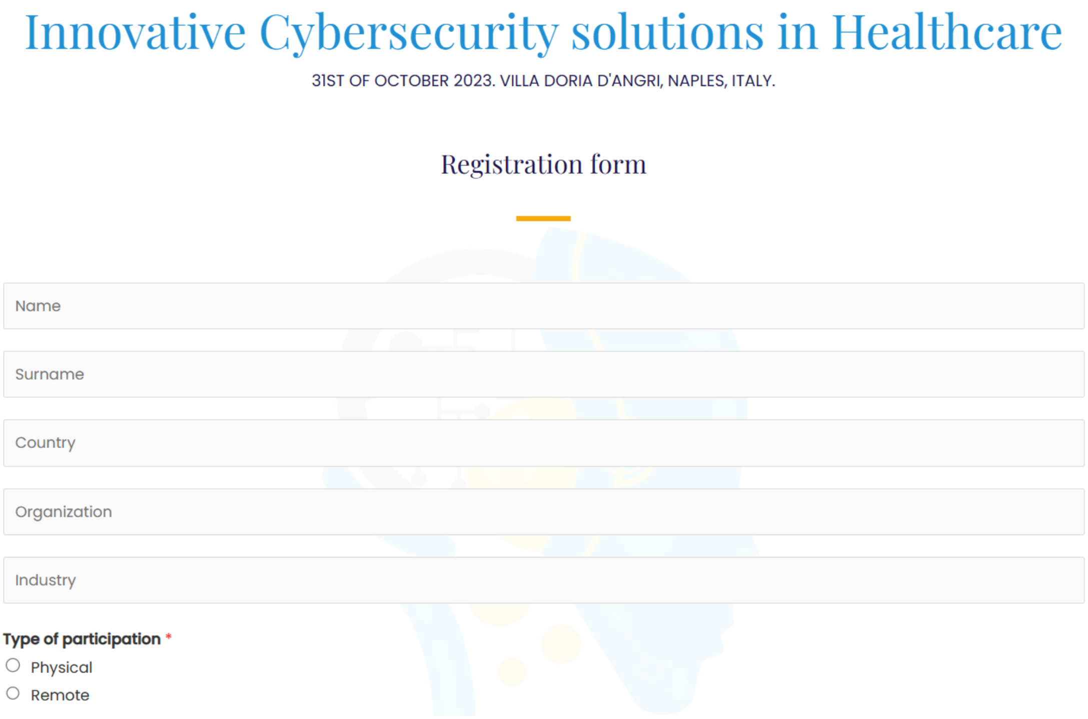
Figure 3-11. Screenshot from the webpage dedicated to the final event of the Ai4HealthSec project

The promotion of the event included campaigns through the website, the social media channels, the relevant page of the project within the cyberwatching platform[10] and through personal invitations to the community of the Ai4HealthSec project.

A special design was created for the event and all relevant publications and communications followed this design.

[9] https://www.ai4healthsec.eu/final-event/

[10] https://www.cyberwatching.eu/projects/3689/ai4healthsec, https://www.cyberwatching.eu/projects/3689/ai4healthsec/events/innovative-cybersecurity-solutions-healthcare



Innovative Cybersecurity solutions in Healthcare

31ST OF OCTOBER 2023. VILLA DORIA D'ANGRI, NAPLES, ITALY.

Registration form

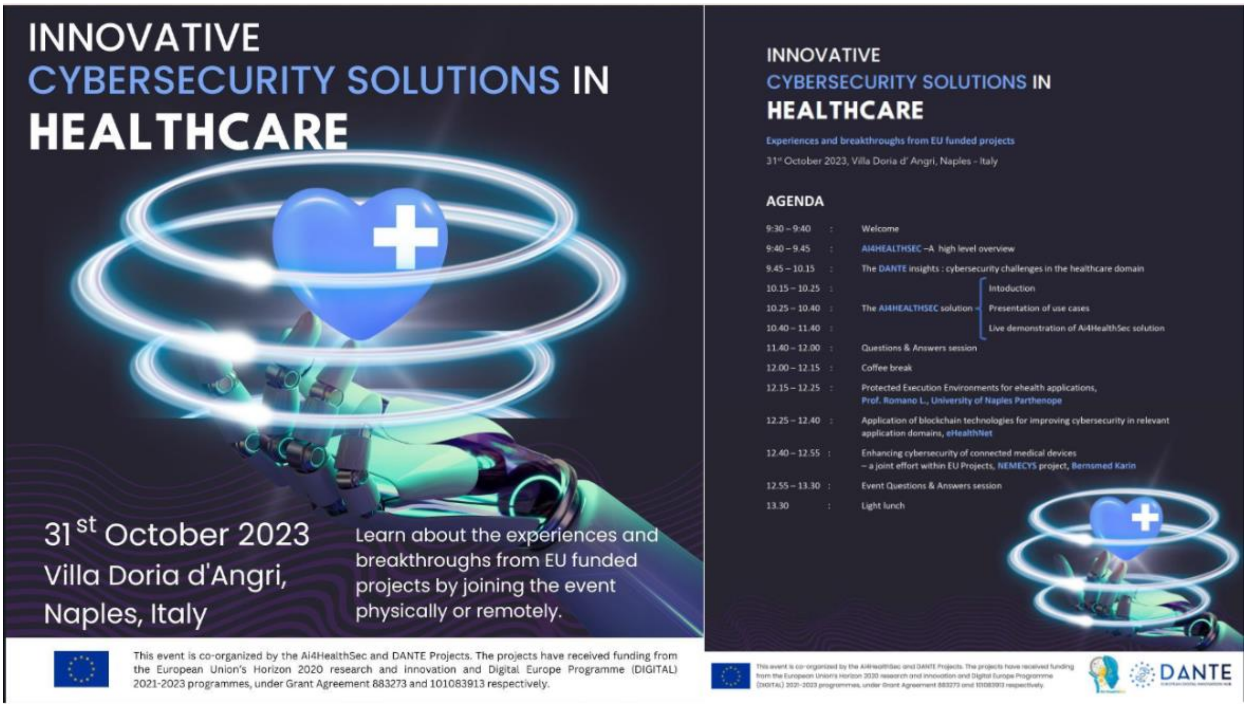
Name
Surname
Country
Organization
Industry

Type of participation *

○ Physical

○ Remote

Figure 3-12. The registration form for the event[11].



INNOVATIVE
CYBERSECURITY SOLUTIONS IN
HEALTHCARE
31st October 2023
Villa Doria d'Angri,
Naples, Italy
Learn about the experiences and breakthroughs from EU funded projects by joining the event physically or remotely.

This event is co-organized by the Ai4HealthSec and DANTE Projects. The projects have received funding from the European Union's Horizon 2020 research and innovation and Digital Europe Programme (DIGITAL) 2021-2023 programmes, under Grant Agreement 883273 and 101083913 respectively.

INNOVATIVE CYBERSECURITY SOLUTIONS IN HEALTHCARE

Experiences and breakthroughs from EU funded projects

31st October 2023, Villa Doria d' Angri, Naples - Italy

AGENDA

9:30 – 9:40	:	Welcome	
9:40 – 9.45	:	AI4HEALTHSEC –A high level overview	
9.45 – 10.15	:	The DANTE insights : cybersecurity challenges in the healthcare domain	
10.15 – 10.25	:	The AI4HEALTHSEC solution	Intoduction
10.25 – 10.40	:		Presentation of use cases
10.40 – 11.40	:		Live demonstration of Ai4HealthSec solution
11.40 – 12.00	:	Questions & Answers session	
12.00 – 12.15	:	Coffee break	
12.15 – 12.25	:	Protected Execution Environments for ehealth applications, Prof. Romano L., University of Naples Parthenope	
12.25 – 12.40	:	Application of blockchain technologies for improving cybersecurity in relevant application domains, eHealthNet	
12.40 – 12.55	:	Enhancing cybersecurity of connected medical devices – a joint effort within EU Projects, NEMECYS project, Bernsmed Karin	
12.55 – 13.30	:	Event Questions & Answers session	
13.30	:	Light lunch	

This event is co-organized by the Ai4HealthSec and DANTE Projects. The projects have received funding from the European Union's Horizon 2020 research and innovation and Digital Europe Programme (DIGITAL) 2021-2023 programmes, under Grant Agreement 883273 and 101083913 respectively.

Figure 3-13. Screenshot from the graphics and agenda created to support the final event of the project.

[11] https://www.ai4healthsec.eu/registration/

61 people registered to participate in the event (both physically and remotely).

Followingly, some pictures from the various stages of the event are presented:

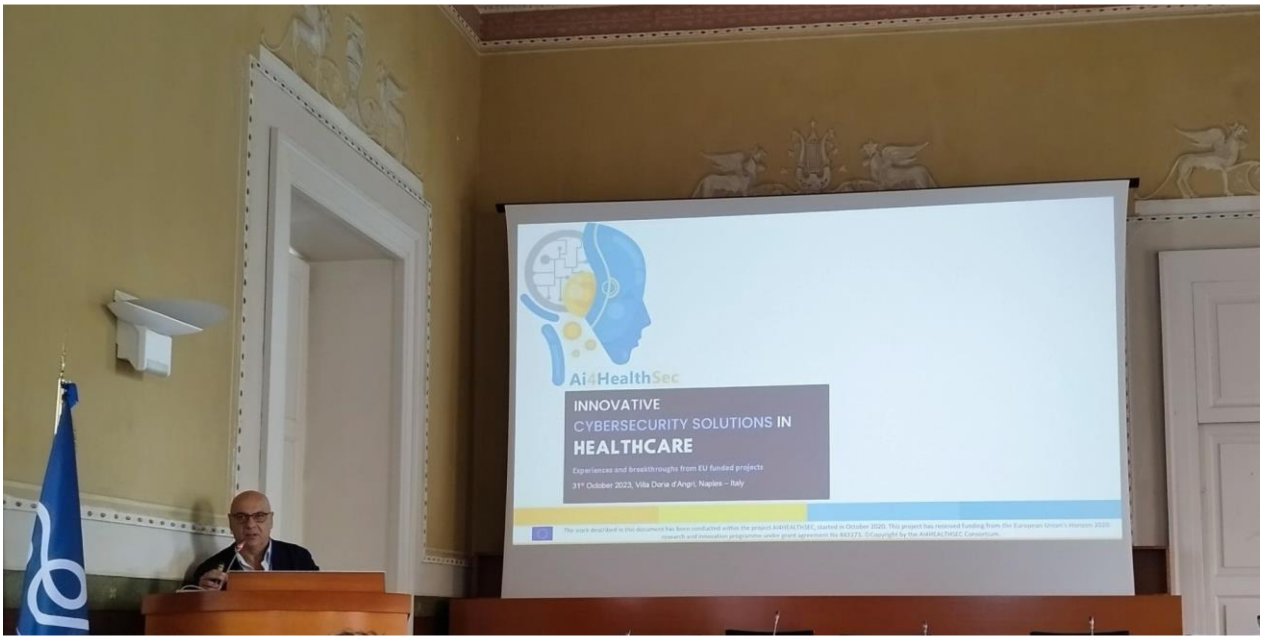

Ai4HealthSec
INNOVATIVE
CYBERSECURITY SOLUTIONS IN
HEALTHCARE
Experiences and breakthroughs from EU funded projects
31st October 2023, Villa Doria d'Angri, Naples – Italy

Figure 3-14. The Coordinator of the Ai4HealthSec project, kicked-off the event with a presentation on the project

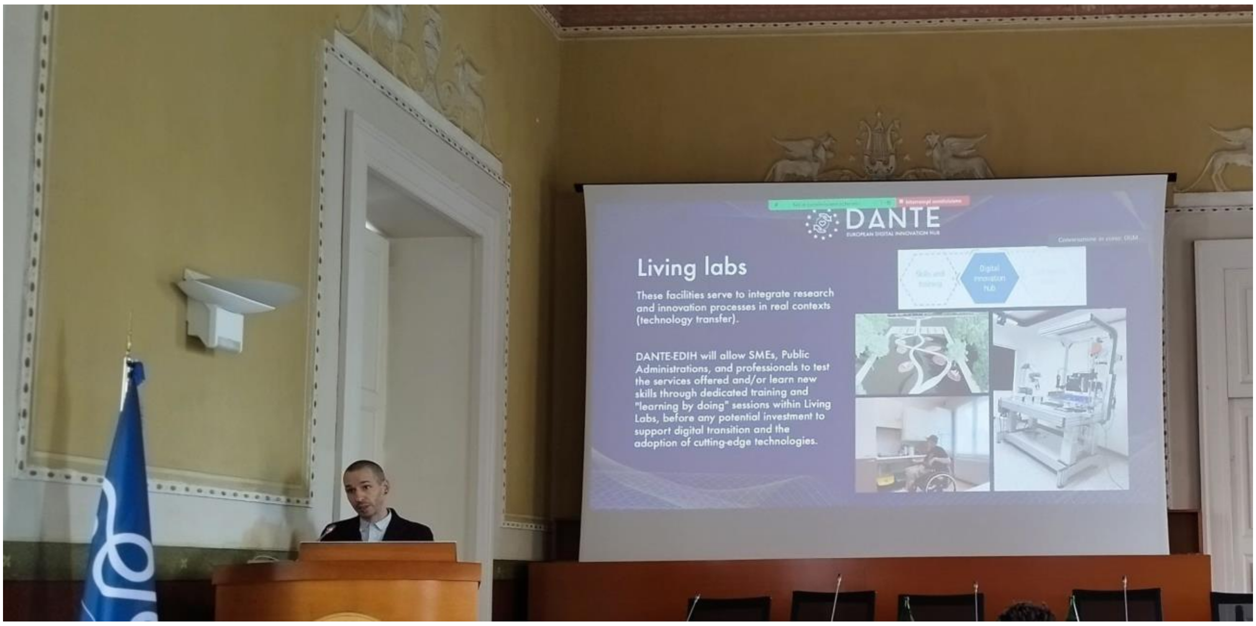

DANTE
EUROPEAN DIGITAL INNOVATION HUB
Living labs
These facilities serve to integrate research and innovation processes in real contexts (technology transfer).
DANTE-EDIH will allow SMEs, Public Administrations, and professionals to test the services offered and/or learn new skills through dedicated training and "learning by doing" sessions within Living Labs, before any potential investment to support digital transition and the adoption of cutting-edge technologies.
Digital innovation hub

Figure 3-15. Patrik Pluchino and Luciano Gamberin presented the DANTE insights: cybersecurity challenges in the healthcare domain

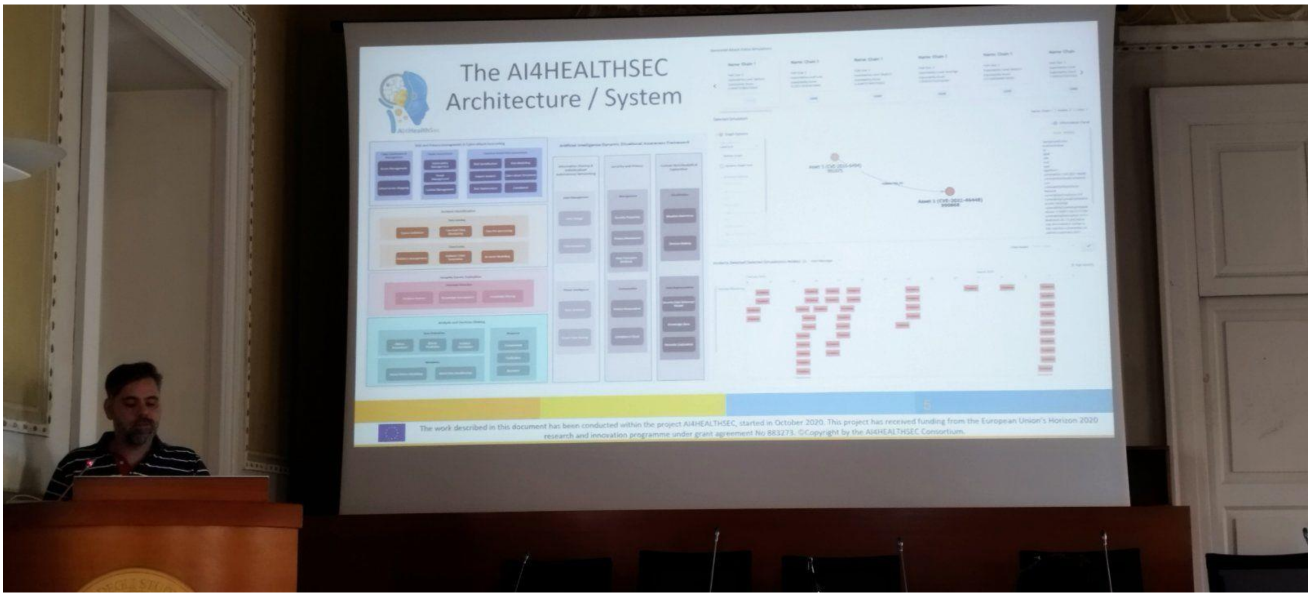

The AI4HEALTHSEC
Architecture / System
The work described in this document has been conducted within the project AI4HEALTHSEC, started in October 2020. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883273. ©Copyright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

Figure 3-16. FOCALPOINT presented of the main characteristics and functionalities of the Ai4HealthSec system

Fraunhofer Pilots – Wearables
Withings Server
REST (JSON)
Withings App
Bluetooth
Withings ScanWatch®
Ai4Health Framework
Corona Diary App of FHG-IBMT
REST (JSON)
XplOit Web application server of FHG-IBMT deployed on the internet
Ai4Health Framework

Figure 3-17. FHG-IBMT presented on the design, implementation and results of the Ai4HealthSec project pilots

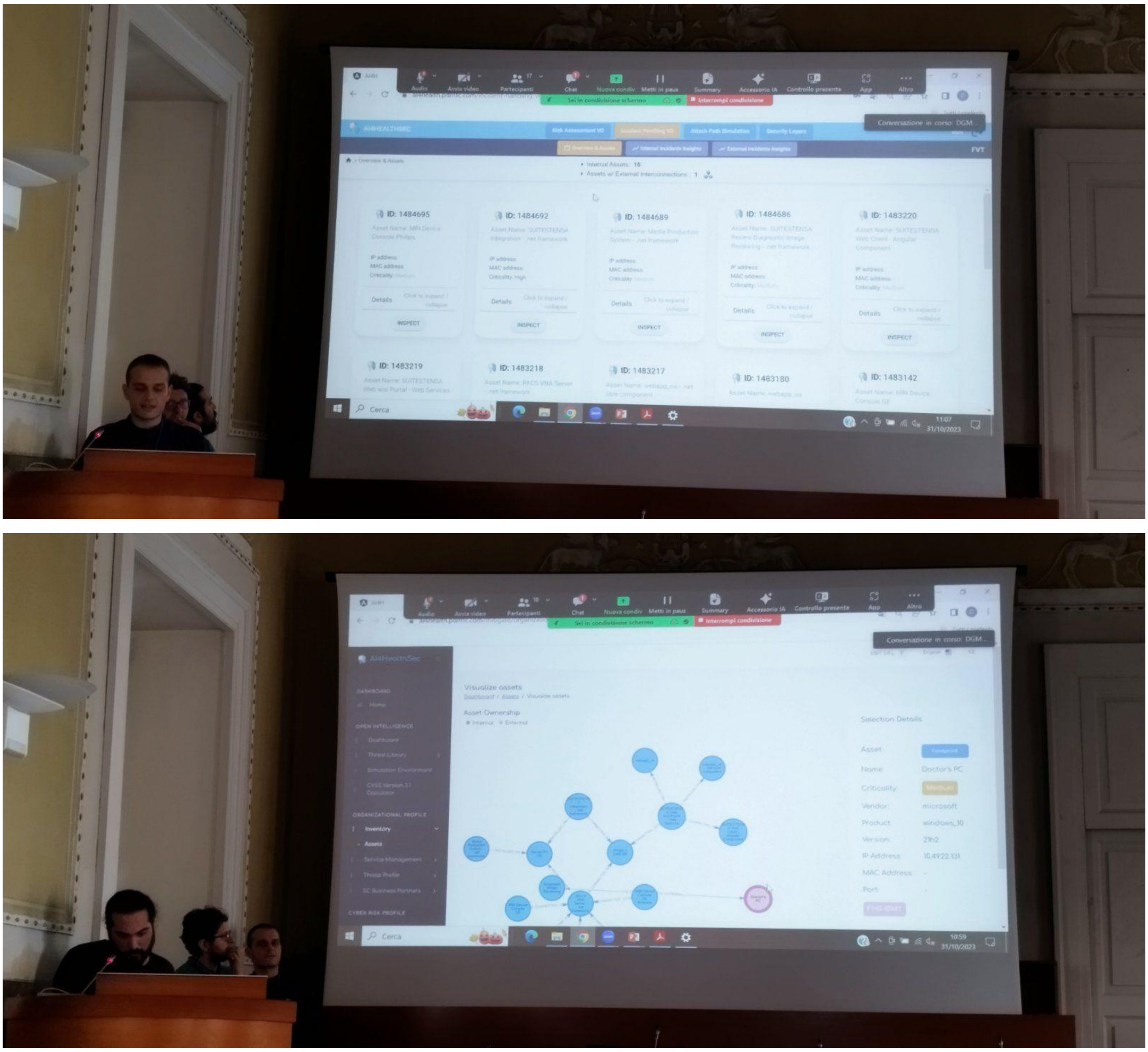
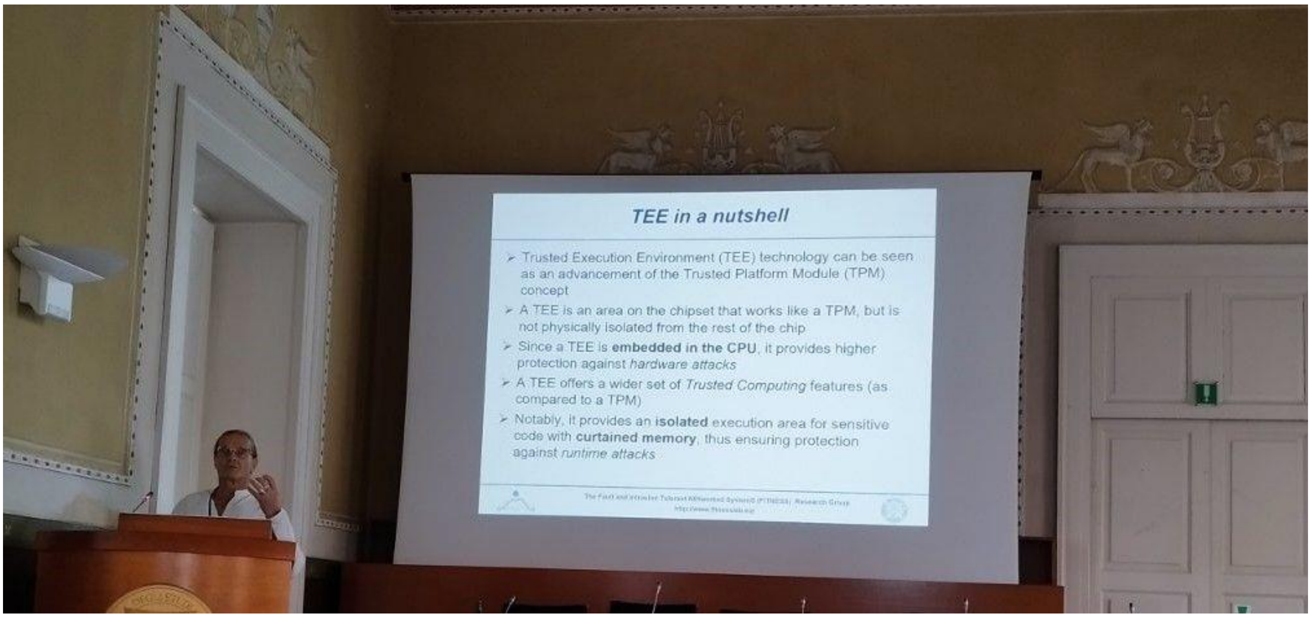


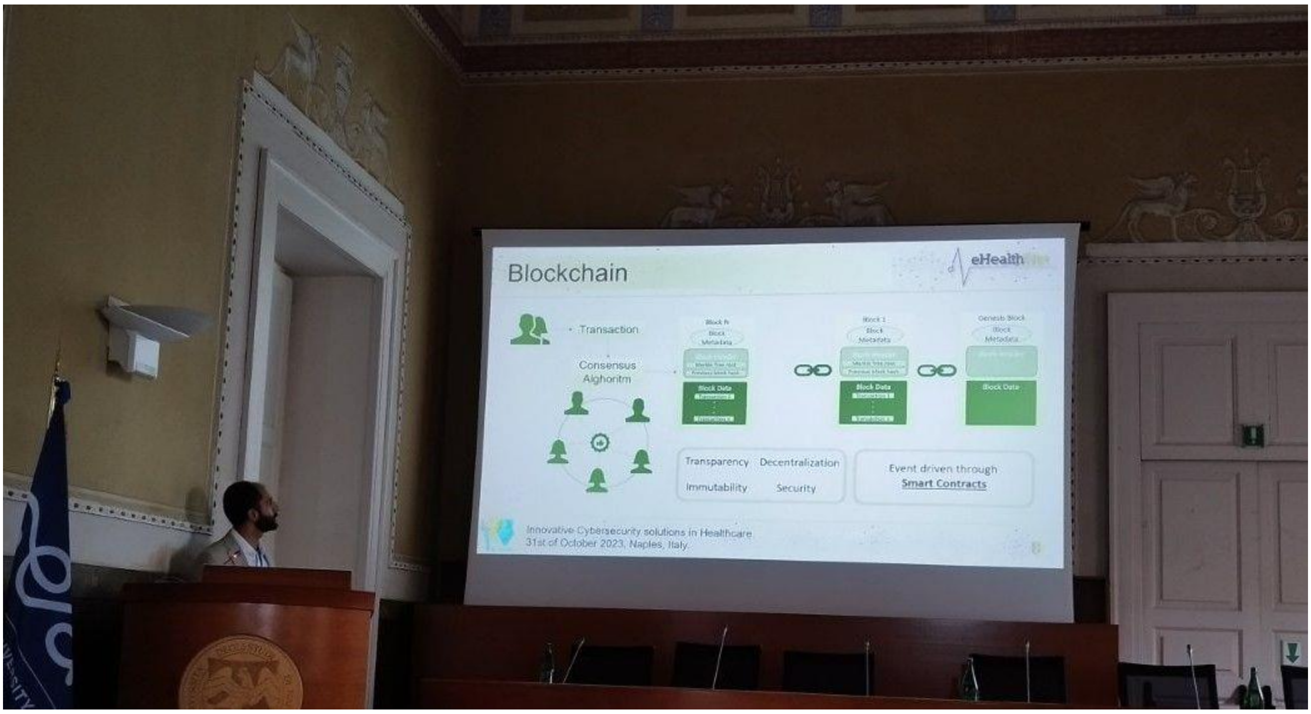
Figure 3-18. Pictures from the live demonstration presented by the Ai4HeathSec partners during the final event



TEE in a nutshell

- Trusted Execution Environment (TEE) technology can be seen as an advancement of the Trusted Platform Module (TPM) concept
- A TEE is an area on the chipset that works like a TPM, but is not physically isolated from the rest of the chip
- Since a TEE is **embedded in the CPU**, it provides higher protection against *hardware attacks*
- A TEE offers a wider set of *Trusted Computing* features (as compared to a TPM)
- Notably, it provides an **isolated** execution area for sensitive code with **curtained memory**, thus ensuring protection against *runtime attacks*

Figure 3-19. Professor Romano presented on the Protected Execution Environments for eHealth applications



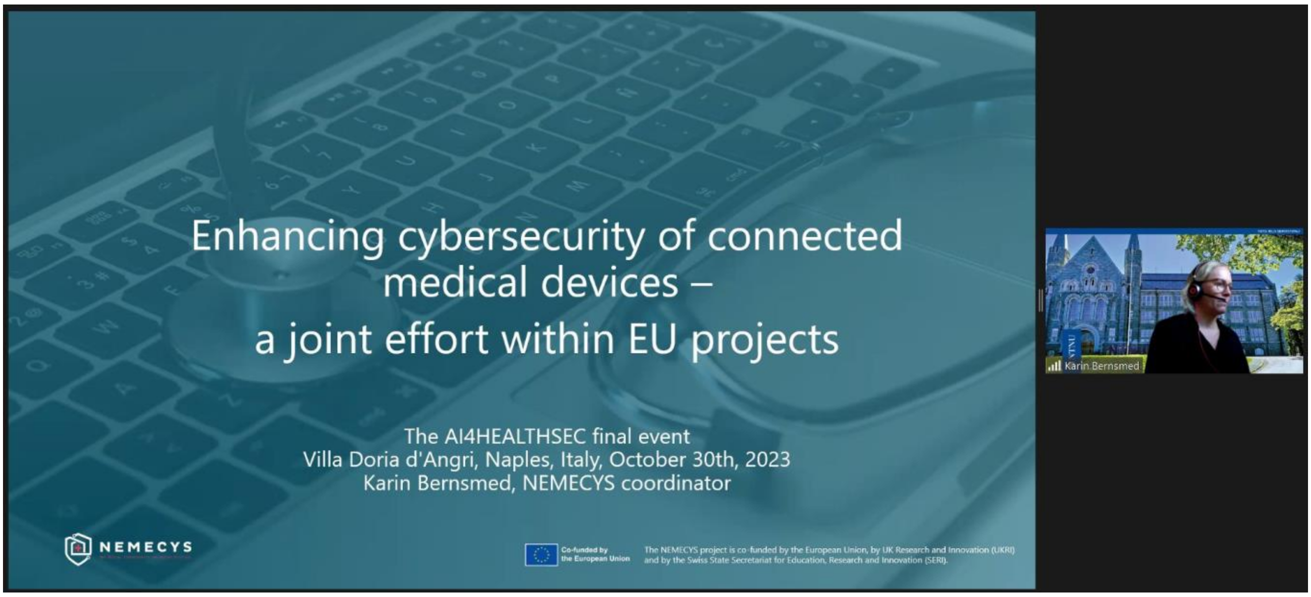
Blockchain

Transparency Decentralization
Immutability Security

Event driven through **Smart Contracts**

Innovative Cybersecurity solutions in Healthcare
31st of October 2023, Naples, Italy

Figure 3-20. Fabrizio Marangio presented on the Application of blockchain technologies for improving cybersecurity in relevant application domains



Enhancing cybersecurity of connected medical devices –
a joint effort within EU projects

The AI4HEALTHSEC final event
Villa Doria d'Angri, Naples, Italy, October 30th, 2023
Karin Bernsmed, NEMECYS coordinator

The NEMECYS project is co-funded by the European Union, by UK Research and Innovation (UKRI) and by the Swiss State Secretariat for Education, Research and Innovation (SERI).

Figure 3-21. **Karin Bernsmed presented on the joint effort within EU project on enhancing cybersecurity of connected medical devices**

Figure 3-22. **The Ai4HealthSec project partners in front of the Villa Doria d'Angri**

Figure 3-23. The physical materials provided to the participants in the event, the light lunch and the view from the Villa Doria d'Angri

3.2 *Workshops*

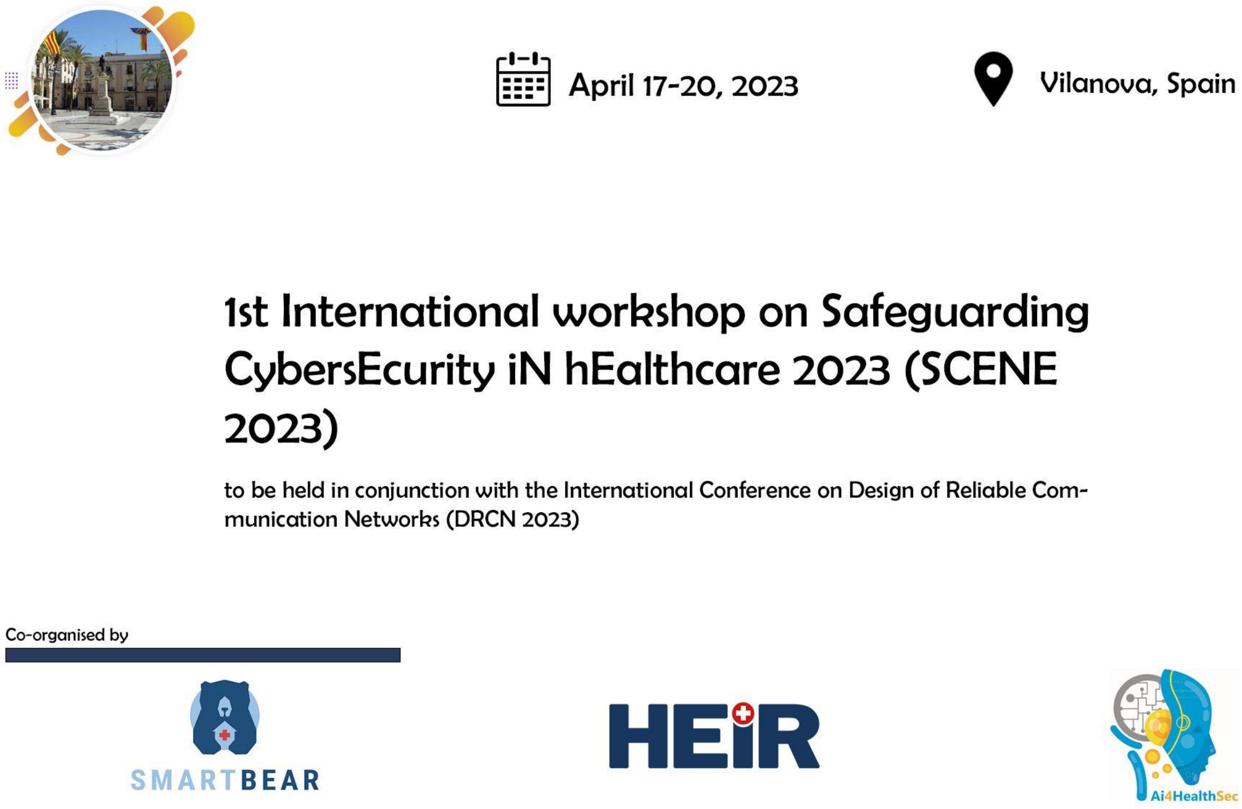
This section provides an accounting of the workshops attended or in other way participated in by the Ai4HealthSec project. In summary, the project partners participated in **4** workshops within the reporting period. In section 7. The KPIs for the entire duration of the project are presented.

3.2.1 1st International Workshop on Safeguarding CybersEcurity iN hEalthcare

The healthcare sector is facing an increasing number of cyber threats, as the digitization of healthcare and the use of connected medical devices continue to grow. These threats can come from a variety of sources, including malicious hackers, nation-state actors, and even insiders. Cybersecurity incidents in healthcare can have serious consequences, including the loss or theft of sensitive patient data, disruption of vital services, and damage to an organization's reputation. Safeguarding CybersEcurity iN hEalthcare[12] aims to bring together viewpoints from diverse areas to explore the commonalities of cybersecurity issues and solutions in the healthcare sector. The workshop is supported by

[12] DRCN | Workshop SCENE 2023 (upc.edu)

the EU-funded projects AI4HealthSec (https://www.ai4healthsec.eu/), HEIR (https://heir2020.eu/), ASCAPE https://www.ascape-project.eu/, and SMART-BEAR (https://www.smart-bear.eu/).



April 17-20, 2023

Vilanova, Spain

1st International workshop on Safeguarding CybersEcurity iN hEalthcare 2023 (SCENE 2023)

to be held in conjunction with the International Conference on Design of Reliable Communication Networks (DRCN 2023)

Co-organised by

SMARTBEAR

HEiR

Ai4HealthSec

Figure 3-24. Screenshot from the social media for the promotion of the SCENE 2023

3.2.2 HEIR – SENTINEL – AI4HEALTHSEC collaboration workshop

As a first collaboration result, the projects AI4HEALTHSEC, HEIR, and SENTINEL are co-organizing the "International Workshop on Information & Operational Technology (IT & OT) Security Systems – (IOSec 2022[13])" under the "17th International Conference on Availability, Reliability and Security (ARES 2022)". The conference and the workshop will be held in August 2022 in Vienna, where further face-to-face interaction and collaboration is expected between the projects' partners.

[13] ARES Conference » Vienna, Austria (ares-conference.eu)

Stylianos Karagiannis
PDM FC S.A / Ionian University
Portugal
ARES Conference
PROGRAM GUIDE
ARES 2022
17th International Conference on Availability, Reliability and Security
August 23-26, 2022
Vienna, Austria

Figure 3-25. Photos from the participation in ARES 2022

3.2.3 CyberHOT Summer School

AI4HEALTHSEC was very proud to support and participate in the CyberHOT[14] Summer School. The Cybersecurity Hands-On Training (CyberHOT) Summer School took place on Thursday 29th and Friday 30th of September 2022 under the auspices of NATO Maritime Inter-diction Operational Training Centre (NMIOTC[15]).

During the event, a Hands-on Cybersecurity Training was provided on:

- Threat and Attack Monitoring

[14] https://sites.google.com/cyberhot.eu/cyberhot2022/home

[15] https://nmiotc.nato.int/wp-content/uploads/2022/10/PRESS-RELEASE-No-50-CyberHOT-School-Sep-22-1.pdf

- Evaluate strategies, tools & procedures
- Apply System Administration
- Monitoring of networks
- Detecting & responding to attacks

The AI4HealthSec project attended this event through different partners. Moreover, partner FORTH presented the Ai4HealthSec project and the developments.

Figure 3-26. Photos from the presentation of the Ai4HealthSec project in the CyberHOT Summer School.

3.2.4 Second ECSCI Workshop on Critical Infrastructure Protection and Resilience[16]

Modern critical infrastructures (or critical entities) are becoming increasingly complex, turning into distributed, large-scale cyber-physical systems. Furthermore, cyber-physical attacks are increasing in number, scope, and sophistication, making it difficult to predict their total impact. Successfully addressing these issues, needs coordinated and integrated responses, which must be disseminated and exploited further to the EU funded projects' frameworks or individual research studies, through raising awareness initiatives, such as the 2nd ECSCI Workshop on CIP.

The 2nd ECSCI Workshop presented the different approaches on integrated (hybrid, cyber and physical) security in several different industrial sectors, such as finance, healthcare, energy, transport, communications, water, etc. The peculiarities of CIP in each of these sectors have been discussed and addressed by the different projects of the ECSCI cluster that presented their outcomes, from the research, technical, ethical and societal point of view.

The AI4HealthSec project attended this event through different partners. Moreover, partner TUV presented the work implemented by the Ai4HealthSec project on "Standards and NIS compliance".

The Consolidated Proceedings of the Workshop have been developed are available through open access publication[17].

Chatzopoulou, A. (2022, April). Standards and NIS compliance. In: Abie, H., Ferrario, D., Troiano, E., Soldatos, J., & Di Peppo, F. (eds.) Consolidated Proceedings of the first ECSCI Workshop on Critical Infrastructure Protection. https://www.steinbeis-edition.de/shop/Tagungsbaende/Tagungen-Symposien/Consolidated-Proceedings-of-theSecond-ECSCI-Workshop-on-Critical-Infrastructure-Protection-and-Resilience.html

3.3 Collaboration with other projects

3.3.1 HEIR

The EU-funded HEIR[18] project designs a complete threat identification and cybersecurity knowledge base system for local and global applications. The system comprises real-time threat hunting services supported by innovative machine learning technologies, reliable sensitive data sharing through the HEIR privacy aware scheme, and advanced benchmarking based on the measurement of Risk Assess-

[16] https://ec.europa.eu/newsroom/cipr/items/752425/en

[17] https://www.steinbeis-edition.de/shop/Tagungsbaende/Tagungen-Symposien/Consolidated-Proceedings-of-the-Second-ECSCI-Workshop-on-Critical-Infrastructure-Protection-and-Resilience.html

[18] https://heir2020.eu/at-a-glance/

ment of Medical Applications score. The project establishes the Observatory for the Security of Electronic Medical Devices that will be accessible by different stakeholders, offering advanced visualisation and awareness on EMD-related threats.

The HEIR project is a European funded project under SU-DS05-2018-2019 - Digital security, privacy, data protection and accountability in critical sectors and the specific call for proposal: H2020-SU-DS-2018-2019-2020.

The collaboration between the projects was extensive and included bilateral meetings, participation in events and joined activities. Some of the activities are: the Joint Webinar for Cybersecurity in Healthcare, the Position Paper[19] of the AI4HealthSec and HEIR projects on the Regulation of the European Parliament and of the Council laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union and the organization of the “International Workshop on Information & Operational Technology (IT & OT) Security Systems – (IOSec 2022[20])” under the “17th International Conference on Availability, Reliability and Security (ARES 2022)”.

3.3.2 SMART-BEAR

The EU-funded SMART BEAR[21] project will develop a platform based on a variety of sensors and mobile instruments that will permanently collect data on their daily life and analyse these to provide personalised interventions. The SMART BEAR solution will be tested in large-scale pilots involving 5.000 elderly people living at home in France, Greece, Italy, Romania and Spain.

The SMART BEAR project is a European funded project under DT-TDS-01-2019 - Smart and healthy living at home and the specific call for proposal: H2020-SC1-FA-DTS-2018-2020.

The collaboration between the projects was extensive and included bilateral meetings, participation in events and joined activities. One of the examples of such activities is the delivery of a keynote speech by the Ai4HealthSec project in the SMART BEAR[22] infoday.

3.3.3 SENTINEL

The EU-funded SENTINEL[23] project will develop an energy system modelling framework that will support the transition. The framework, built with a renewable energy system in mind, will enable various decision makers to address critical design challenges. It will be modular in structure incorporating many separate models that will examine specific technological, geographic, and societal aspects of the transition to a low-carbon energy system. All the models will be linked together, and along with data, will be accessible via an online platform.

[19] https://www.ai4healthsec.eu/wp-content/uploads/Position-Paper_Reg_EU_institutions.pdf

[20] ARES Conference » Vienna, Austria (ares-conference.eu)

[21] https://www.smart-bear.eu/

[22] https://www.smart-bear.eu/general-meeting-and-information-day/

[23] https://sentinel-project.eu/

The SENTINEL project is a European funded project under LC-SC3-CC-2-2018 - Modelling in support to the transition to a Low-Carbon Energy System in Europe and the specific call for proposal: H2020-LC-SC3-2018-2019-2020.

The collaboration between the projects included bilateral meetings, participation in events and joined activities. A key example of this collaboration was the joint organization of the “International Workshop on Information & Operational Technology (IT & OT) Security Systems – (IOSec 2022[24])” under the “17th International Conference on Availability, Reliability and Security (ARES 2022)”.

3.3.4 CONCORDIA

CONCORDIA[25], an EU-funded multi-disciplinary research and innovation project, has set out to address this current fragmentation and further enhance the EU's digital sovereignty. The project aims to interconnect all of Europe’s cybersecurity capabilities into a network of expertise to help build a secure, trusted, resilient and competitive ecosystem. Moreover, it will develop the EU Cybersecurity Research and Innovation Roadmap.

The CONCORDIA project is a European funded project under SU-ICT-03-2018 - Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap and the specific call for proposal: H2020-SU-ICT-2018-2020.

The collaboration between the projects revolved around the subject cybersecurity in healthcare and included joint events (See report 8.2) and presentations. An example of this collaboration was the presentation and participation of Ai4HealthSec project partners in the final CONCORDIA open door event.

3.3.5 CYBALLIANCE

The main purpose of the proposed INTPART[26] project is to establish a long-term partnership between the Norwegian Computing Center (NR, Norway), the Norwegian University of Science and Technology (NTNU, Norway), Oslo University Hospital (OUS, Norway), University of Colorado (UCCS, USA), Institut Mines Telecom/Telecom SudParis (IMT, France), and Goethe University Frankfurt (GUF, Germany). This project aims to strengthen the existing collaboration between relevant national and international partners of the ASCERT (AI-Based Scenario Management for Cyber Range Training) and SFI NORCICS (Norwegian Centre for Cybersecurity in Critical Sectors) and projects. This involves extending the originally envisioned activities among the involved education and research institutions. Along with existing collaborators of ASCERT and NORCICS partners, two additional partners OUS (national), and UCCS (international) partners are also part of the CybAlliance consortium to further advance the research, education, dissemination, and networking activities of ASCERT and NORCICS at national and international levels. This international partnership is centred around activities that promote excellence in both research and education in cybersecurity and privacy in the healthcare sector in Norway, USA, France, and Germany.

[24] ARES Conference » Vienna, Austria (ares-conference.eu)

[25] https://www.concordia-h2020.eu/

[26] https://cyballiance.nr.no/

CybAlliance will provide added value to both qualifying projects by offering international collaboration and support to extend the originally envisioned activities. CybAlliance also brings in added value on its own, beyond its support of ASCERT and NORCICS, by boosting the collaboration in cybersecurity and privacy research and education community. To facilitate the dissemination of the CybAlliance results globally, the project will have a direct link with two stakeholders “Norway Health Tech (NHT)” and "European Cluster for Securing Critical Infrastructures (ECSCI)" to disseminate project outcomes to the national and international NHT and ECSCI members. The collaboration between the project has started with the invitation of a project partner to present during the project kick off meeting.

3.3.6 DANTE

The project denominated “DANTE: Digital Solutions for a Healthy, Active and Smart Life”[27] has been presented under the EU call “DIGITAL-2021-EDIH-01 — European Digital Innovation Hubs” by the National Technological Cluster on “Smart Living Technologies”, as project coordinator.

The project will have a duration of 36 months from the 1st of October 2022 to the 30th of September 2025.

DANTE is a cutting-edge project insofar as it focuses on supporting the digital transformation of Small and Medium Enterprises (SMEs), Organizations in the public sector, and professionals that operate in the domains of healthy and active ageing, ambient assisted living (AAL), and smart environments. The aim is to ensure that these players can respond to the current digital challenges. To foster the digital transformation of the European Economy the Digital Transformation Accelerator (DTA) will support effectively and efficiently the network of Digital Innovation Hubs (EDIHs).

The project will have relevant social impacts at different levels: on people, mainly the ones who have difficulties as the elderly and the individuals with disabilities try to increment their level of autonomy in daily life in terms of safety, avoiding loneliness, and support in case of physical and mental pathologies; on caregivers (professionals and not), providing them with digital information, abilities, tools to monitor continuously their patients to streamline the management of care processes; on social and health services, by reducing the costs and ensuring quality support for the elderly to foster their ability to remain active in the society; on the policies and Public Administration, in terms of supporting the connections between social and health policies (at regional, national, and international level) and the citizens, professionals, and companies operating in the area of healthy and active ageing, the technology-driven “smart” life.

The DANTE project brings together 13 partners, some of them being Innovation Hubs (Pitagora ICT Innovation Hub and Innovative Tertiary Sector), consortium companies (eHealthNet) and Technological Districts (Technological District for Active & Assisted Living and Technological District for Human Health and Biotechnologies). This unique composition of the project, creates an ecosystem of more than 1.100 entities.

The Ai4HealthSec and DANTE projects co-organized the final event of the Ai4HealthSec project.

[27] https://dante-edih.clustersmile.it/en/project/

4 On-line

This section provides an overview of the dissemination and communication activities carried out by the project, through on-line communication channels. Such channels and activities include:

1. Social Media
   a. Facebook
   b. Linkedin
   c. Twitter - X
2. The project website
3. The project newsletters
4. Videos
5. Cyberwatching

For each one of these channels, a separate subsection is included within this section. It should be noted, that the activities described only cover the ones carried out between Month 20 and the end of the project.

4.1 *Social media*

The AI4HEALTHSEC project has created and maintains the following Social Media accounts:

FACEBOOK: https://www.facebook.com/Ai4HealthSec

TWITTER: https://twitter.com/aifourhealthsec

LINKEDIN: https://www.linkedin.com/company/ai4healthsec-eu-h2020-project/

These accounts are managed (maintained and operated) by the project partner TUV.

During the reporting period, several campaigns have run in all social media.

Specifically:

- In May and June 2022, a series of 12 deliverables of the project were presented in a series of posts.
- In September, October and November 2022, the videos created by the project partners presenting their participating in the Ai4HealthSec project were promoted.
- In November 2022, a series of 11 deliverables of the project were presented in a series of posts.
- In February and March 2023, the open call process of the project was promoted.
- In June 2023, the videos created by the project partners demonstrating the Ai4healthSec solution in general, the incident handling process and the attack path simulation function were promoted.
- In October 2023, the final even to the Ai4HealthSec was promoted.

Apart from the targeted campaigns, all activities and developments of the project were also promoted, disseminated and communicated through the social media channels of the project. Such content included the organization of event, the participation of the partners or the project in activities, the developments of the project, the newsletters of the project and others.

4.1.1 Facebook

The *Facebook*[28] account (up to November 2023) counts 167 followers. The picture below depicts the results, in general, of the account for the period January 2023 - November 2023[29].

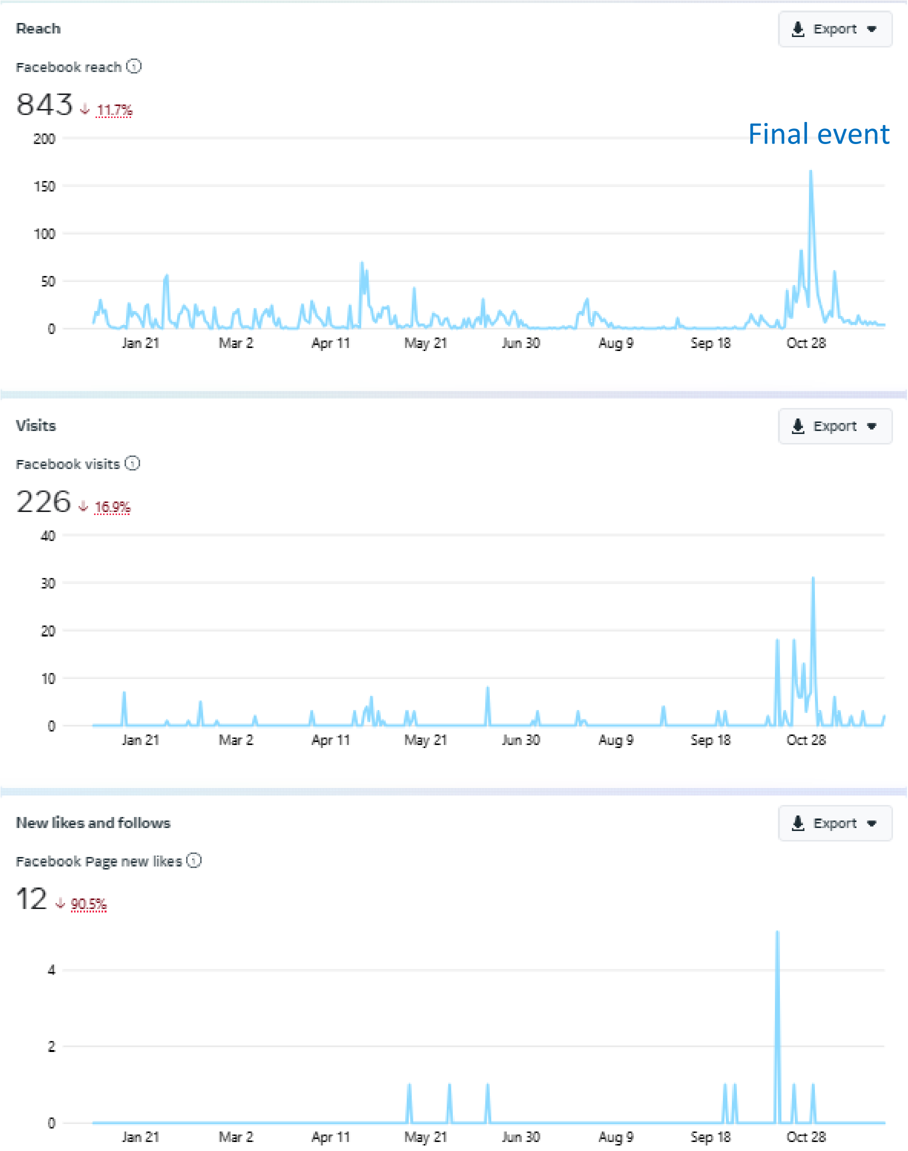
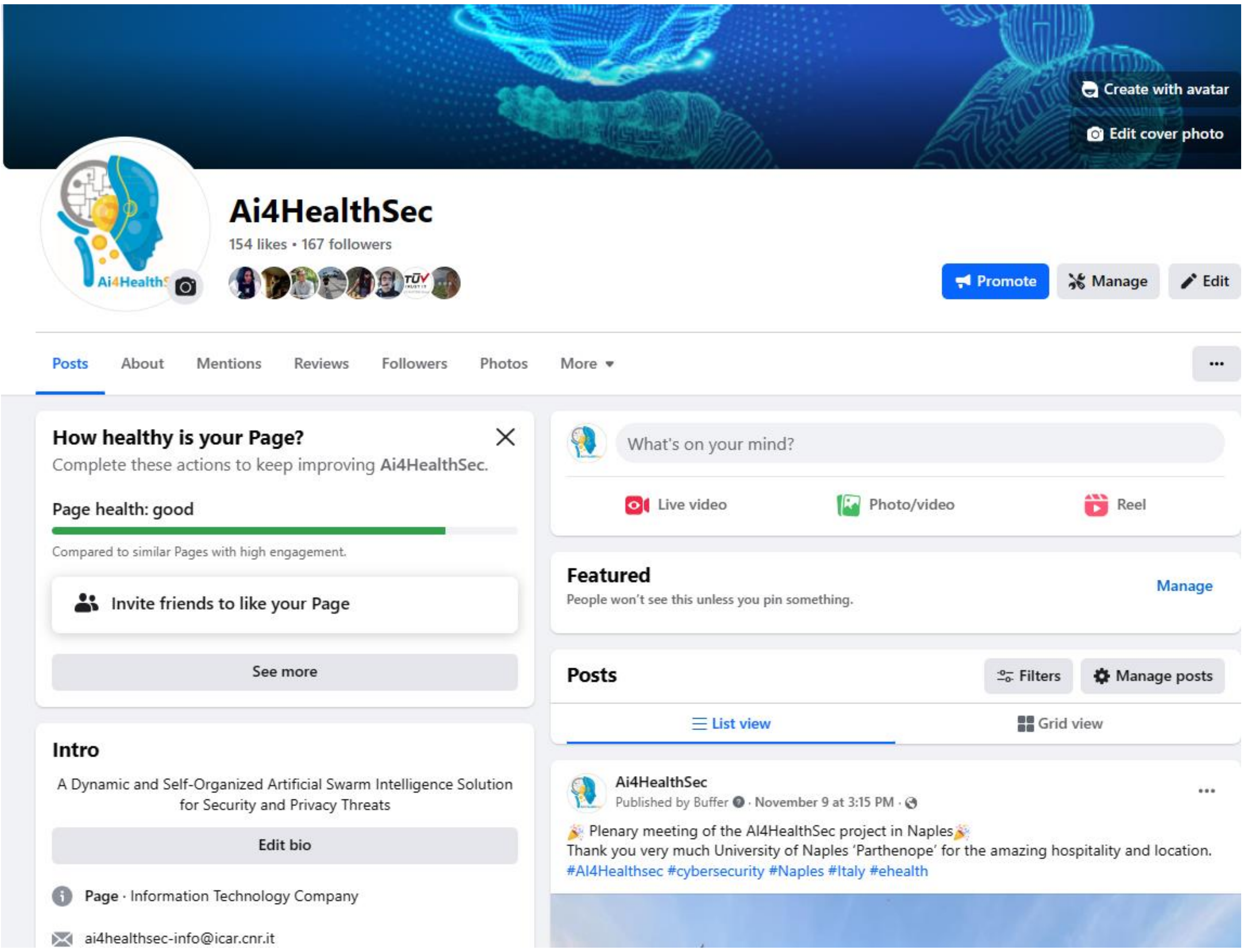


Figure 4-27. Facebook general results.

[28] https://www.facebook.com/Ai4HealthSec

[29] The period of the chart is restricted for two reasons 1) the system does not allow to extract information on performance prior to January 2023 and 2) the graphs were exported in the beginning of December to facilitate the preparation of this deliverable.



Create with avatar

Edit cover photo

Ai4HealthSec

154 likes • 167 followers

Promote Manage Edit

Posts About Mentions Reviews Followers Photos More

How healthy is your Page?

Complete these actions to keep improving Ai4HealthSec.

Page health: good

Compared to similar Pages with high engagement.

Invite friends to like your Page

See more

Intro

A Dynamic and Self-Organized Artificial Swarm Intelligence Solution for Security and Privacy Threats

Edit bio

Page · Information Technology Company

ai4healthsec-info@icar.cnr.it

What's on your mind?

Live video Photo/video Reel

Featured

People won't see this unless you pin something.

Manage

Posts

Filters Manage posts

List view Grid view

Ai4HealthSec

Published by Buffer · November 9 at 3:15 PM ·

🎉 Plenary meeting of the AI4HealthSec project in Naples🎉
Thank you very much University of Naples 'Parthenope' for the amazing hospitality and location.
#AI4Healthsec #cybersecurity #Naples #Italy #ehealth

Figure 4-28. Facebook page.

Facebook Statistics	
Posts May-December 2023	117
Posts January 2023 – November 2023	118
Reach January 2023 – November 2023	3830
Clicks January 2023 – November 2023	174
Likes January 2023 – November 2023	437

Table 4-2. Facebook statistics

FORESIGHT 2030 THREATS
enisa
EUROPEAN UNION AGENCY
D8.3 - Fully implemented 1st Vertical Layer Report version 2
AI4HEALTHSEC RISK ASSESSMENT
European Parliament
ENISA AI CYBERSECURITY CONFERENCE
7 June, Brussels
AI4HEALTHSEC ATTACK PATH SIMULATION
ENISA THREAT LANDSCAPE: HEALTH SECTOR
Artificial Intelligence Risk Management Framework (AI RMF 1.0)
NIST
MITRE ATT&CK
Best Practices for MITRE ATT&CK® Mapping
EDPB
Guidelines
CYBER SECURITY CHALLENGES IN HEALTHCARE ENVIRONMENTS
GOV.UK
Guidelines 9/2022 on personal data breach notification under GDPR
OPEN CALL
APPLY NOW!
CLOUD CYBERSECURITY MARKET ANALYSIS
ENISA report
ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE
AR-IN-A-BOX
A GUIDE TO CREATING YOUR OWN AWARENESS RAISING PROGRAMMES
ENGINEERING PERSONAL DATA SHARING
The Global Risks Report 2023
JRC TECHNICAL REPORT
ARTIFICIAL INTELLIGENCE
HEIR

Figure 4-29. Indicative Facebook posts

4.1.2 LinkedIn

The *LinkedIn*[30] account (up to November 2023) counts 239 followers. The picture below depicts the results, in general, of the account for the period November 2022 - November 2023[31].

The AI4HEALTHSEC LinkedIn corporative account is entitled **AI4HEALTHSEC EU H2020 Project**. **(https://www.linkedin.com/company/AI4HEALTHSEC-eu-h2020-project/)**

[30] https://www.linkedin.com/company/ai4healthsec-eu-h2020-project

[31] The period of the chart is restricted for two reasons 1) the system does not allow to extract information on performance prior to November 2022 and 2) the graphs were exported in the beginning of December to facilitate the preparation of this deliverable.

LinkedIn Statistics from November 2022 – November 2023	
Followers	239
Unique visitors	206
Overview page views	536
Total page views	572
Posts	137
Reposted posts	64
Impressions	21635
Clicks	721
Reactions	1364

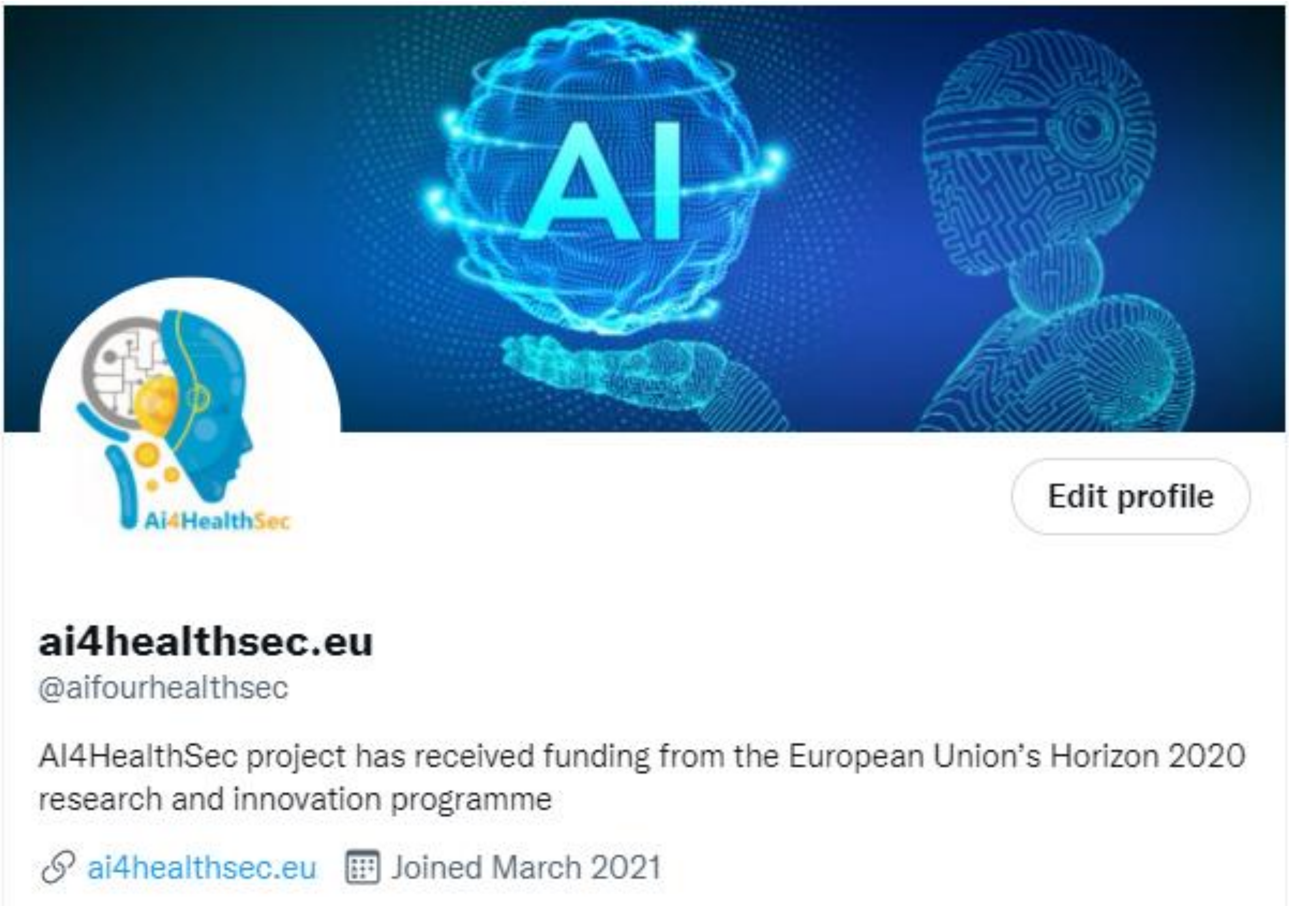
Table 4-3. LinkedIn statistics

Ai4HealthSec EU H2020 Project
FORESIGHT 2030 THREATS
enisa
AI4HEALTHSEC ATTACK PATH SIMULATION
GOOD PRACTICES FOR SUPPLY CHAIN CYBERSECURITY
AI4HEALTHSEC OVERVIEW
ARTIFICIAL INTELLIGENCE AND CYBERSECURITY RESEARCH
ENISA AI CYBERSECURITY CONFERENCE
7 June, Brussels
European Parliament
ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE
Question 1: What will be the implications of recent developments in AI on global economic growth, as they mature over the upcoming decade?
AI, STANDARDS AND INTEROPERABILITY FOR HEALTHCARE
RATs and InfoStealer: Mission Spain and Catalonia
ENISA Single Programming Document 2023-2025

Figure 4-30. Indicative LinkedIn posts

4.1.3 Twitter - X

AI4HEALTHSEC *Twitter*[32] account is mainly used for smaller posts that relate to the project, due to the character limitation. The account has earned 115 followers.



ai4healthsec.eu
@aifourhealthsec

AI4HealthSec project has received funding from the European Union's Horizon 2020 research and innovation programme

ai4healthsec.eu Joined March 2021

Figure 4-31. Twitter account home page

Twitter Statistics from December 2022 – November 2023												
	DEC 2022	JAN 2023	FEB 2023	MAR 2023	APR 2023	MAY 2023	JUN 2023	JUL 2023	AUG 2023	SEP 2023	OCT 2023	NOV 2023
Tweets	14	14	13	11	17	12	13	7	4	1	22	1
Tweet impressions	749	815	1215	965	1890	1549	1407	930	472	150	1537	800
New followers	2	0	4	6	4	0	1	3	4	0	2	2

Table 4-4. Twitter statistics

[32] https://twitter.com/aifourhealthsec

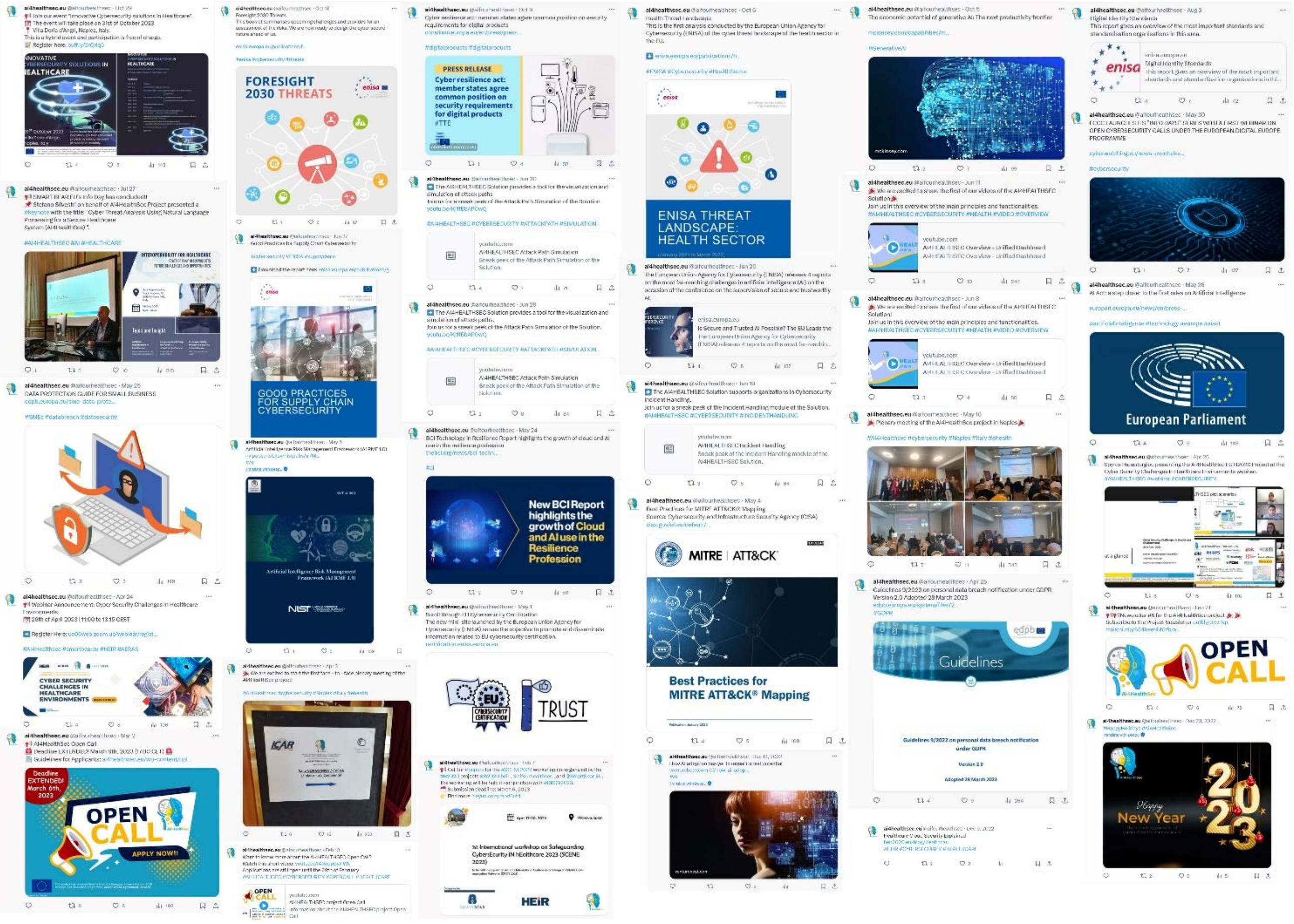
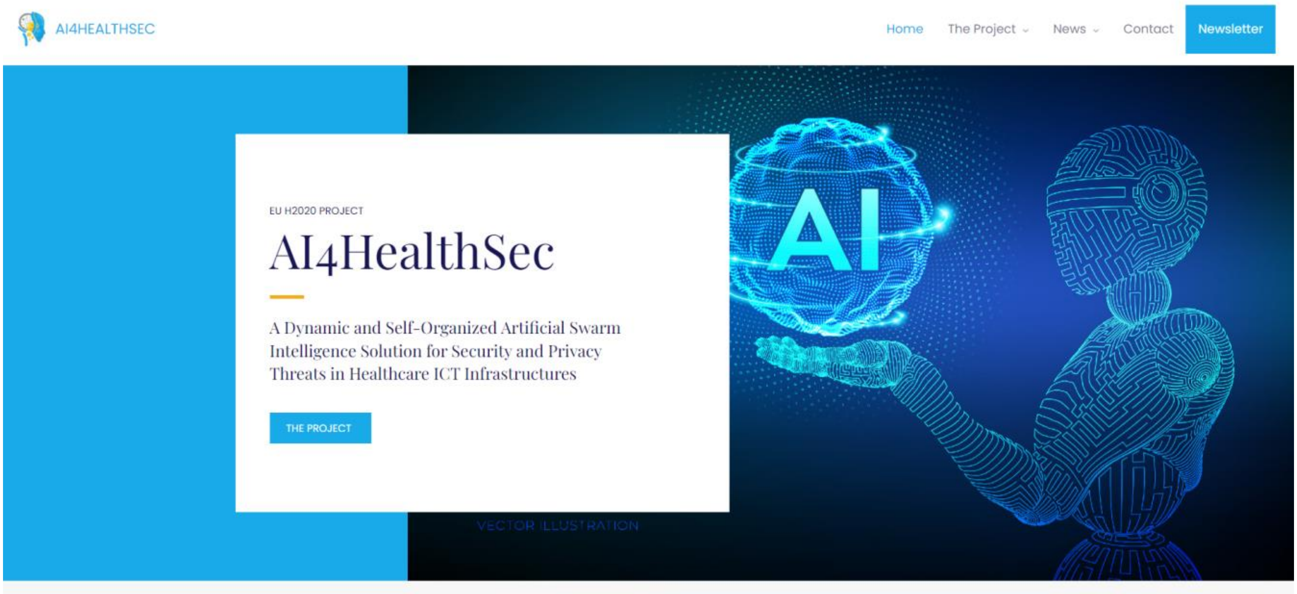


Figure 4-32. Indicative twitter posts

4.2 *Website*

The *AI4HEALTHSEC website* has been available since M3 of the project at https://www.AI4HEALTHSEC.eu/. This website was created in order to present the project and the relevant information related to the project, such as the partners involved in the project, the objectives of the project, the challenges and the impact for the implementation of the project.

The website has been developed by CNR and managed and updated regularly according to the communication needs of each stage of the communication plan by CNR and TUV.



EU H2020 PROJECT

AI4HealthSec

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

Figure 4-33. The AI4HEALTHSEC website

The website pages have the following options and information:

Homepage: Offers a comprehensive view of the sections of the website and the content available. It includes the challenges and the impact of the project and it also features the icons and links to the project social media accounts such as *Twitter*, *Facebook* and *LinkedIn*. Finally, the footer includes the statement regarding the funding of the project and the number of the Grand Agreement.

Project: This section provides information on the vision, the consortium and the workplan of the project.

- Vision: provides information on the vision of the AI4HEALTHSEC project.
- Consortium: contains the partners of the AI4HEALTHSEC project. Each partner is depicted by their logo and a link to their respective websites is provided.
- Workplan: descriptions of the AI4HEALTHSEC Work packages are depicted in a roadmap in this page.
- Open Call: provides information and guidelines regarding the Open Call of the project. (This functionality was added in February 2023 to facilitate the promotion and implementation of the open call application process).

News: This section provides information on the Events, Deliverables, Publications, Newsletters and Articles of the AI4HEALTHSEC project.

- Events: illustrates the events (i.e., conferences, events and workshops) that the AI4HEALTHSEC is participating are displayed. More details on each one is provided in subsection 3. of this document.
- Deliverables: contains the published deliverables of the project. Deliverables classified as public can be directly accessed through this webpage.

- Publications: displays the published articles and presentations in Scientific Journals and conferences.
- Newsletters: contains the links to the published newsletters of the AI4HEALTHSEC project.
- Articles: presents articles written by the project partners on the subjects of the project.
- Videos: contains videos that have been created for the project and they are linked with the project YouTube channel. (This functionality was added in September 2022 to facilitate the promotion of the project videos)

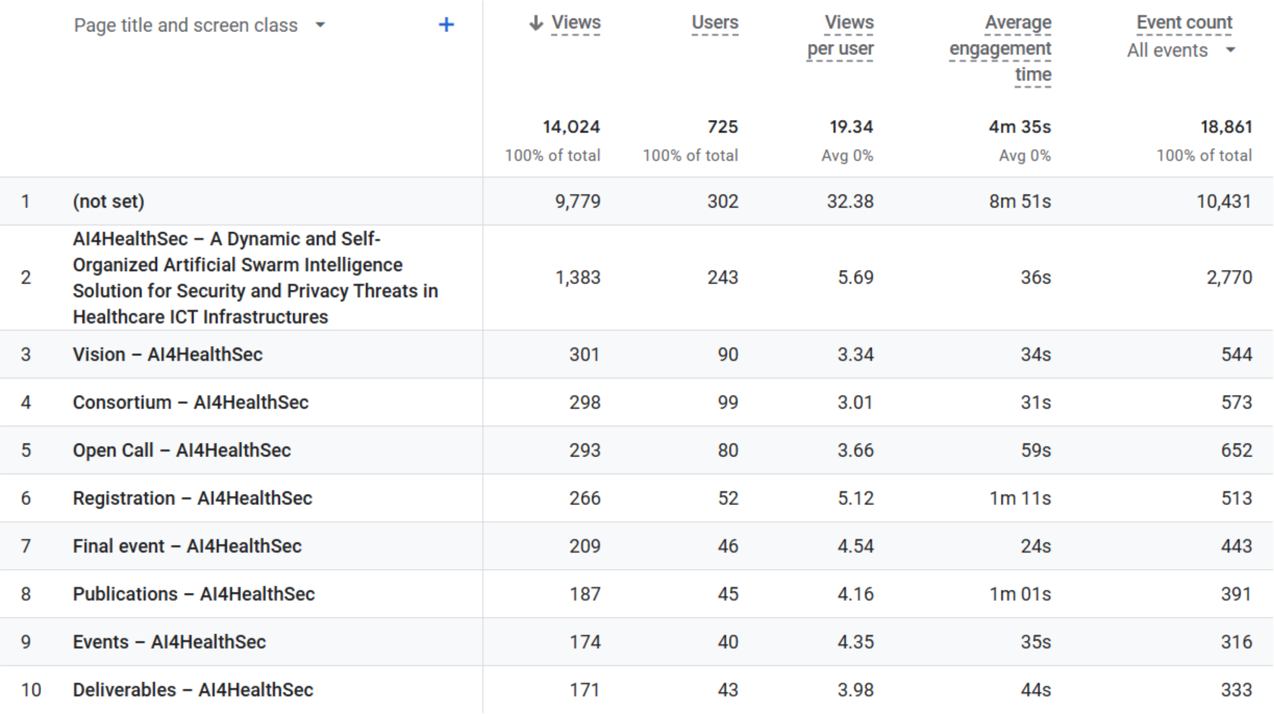
Contact us: informs available means to communicate with the project coordination. It also provides information on the project coordinator and the project technical manager.

Newsletter: provides the interface to subscribe to the Project Newsletter.

Final Event: contains information for the final event that took place on 31st of October 2023 at Villa Doria d'Angri, Naples, Italy. Also provides information regarding the registration to the event and the agenda. (This functionality was added in October 2023 to facilitate the promotion and registration to the final event of the project).

In collaboration with the DPO of the project, the privacy related settings and documents of the website were prepared. Specifically, a cookie banner and a cookie and privacy policy have been incorporated to the website.

Website statistics



	Page title and screen class ▾ +	↓ Views	Users	Views per user	Average engagement time	Event count All events ▾
		14,024 100% of total	725 100% of total	19.34 Avg 0%	4m 35s Avg 0%	18,861 100% of total
1	(not set)	9,779	302	32.38	8m 51s	10,431
2	AI4HealthSec – A Dynamic and Self-Organized Artificial Swarm Intelligence Solution for Security and Privacy Threats in Healthcare ICT Infrastructures	1,383	243	5.69	36s	2,770
3	Vision – AI4HealthSec	301	90	3.34	34s	544
4	Consortium – AI4HealthSec	298	99	3.01	31s	573
5	Open Call – AI4HealthSec	293	80	3.66	59s	652
6	Registration – AI4HealthSec	266	52	5.12	1m 11s	513
7	Final event – AI4HealthSec	209	46	4.54	24s	443
8	Publications – AI4HealthSec	187	45	4.16	1m 01s	391
9	Events – AI4HealthSec	174	40	4.35	35s	316
10	Deliverables – AI4HealthSec	171	43	3.98	44s	333

Figure 4-34. Views by Page title

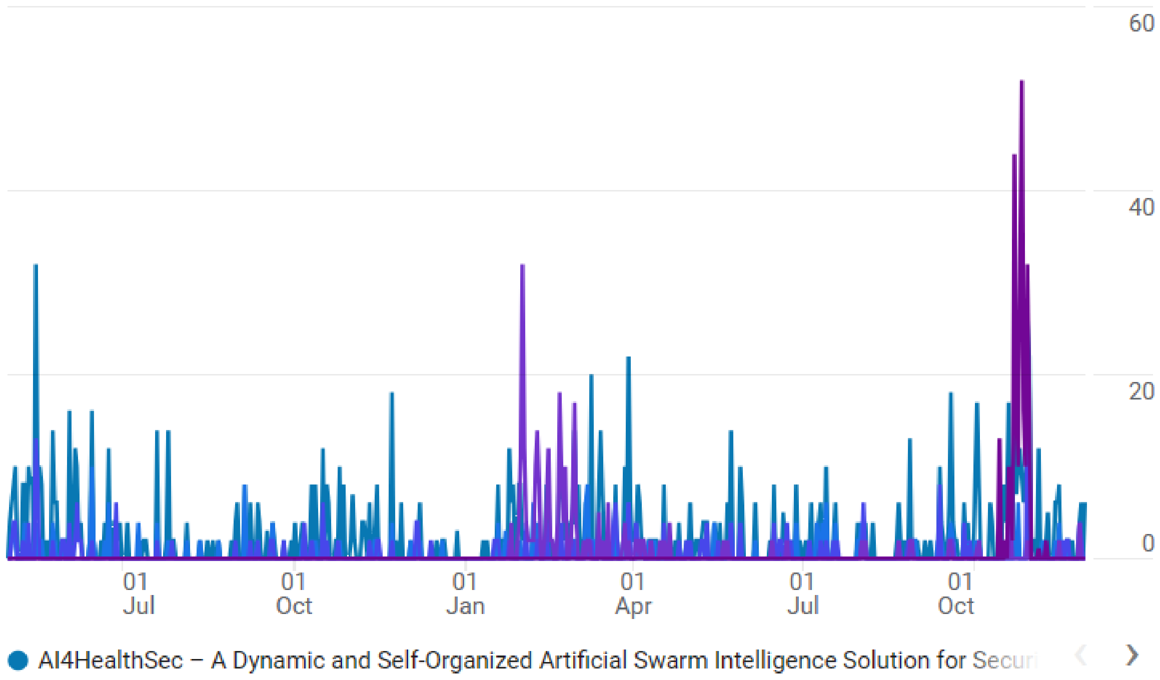
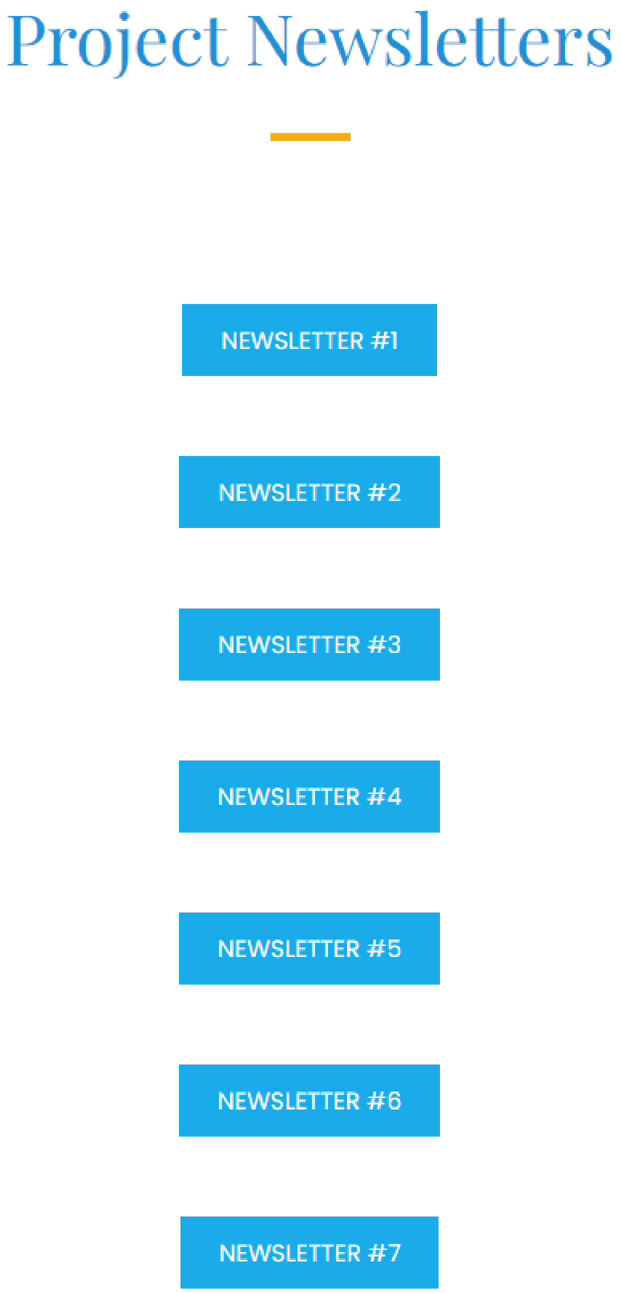


Figure 4-35. Views by Page title chart

4.3 *Newsletters*

The newsletter subscription[33] is one of the channels used by the AI4HEALTHSEC project in order to communicate with the various interested parties. The website contains an archive of the newsletters and a form where a person can subscribe to the newsletter.

[33] https://www.ai4healthsec.eu/newsletter/

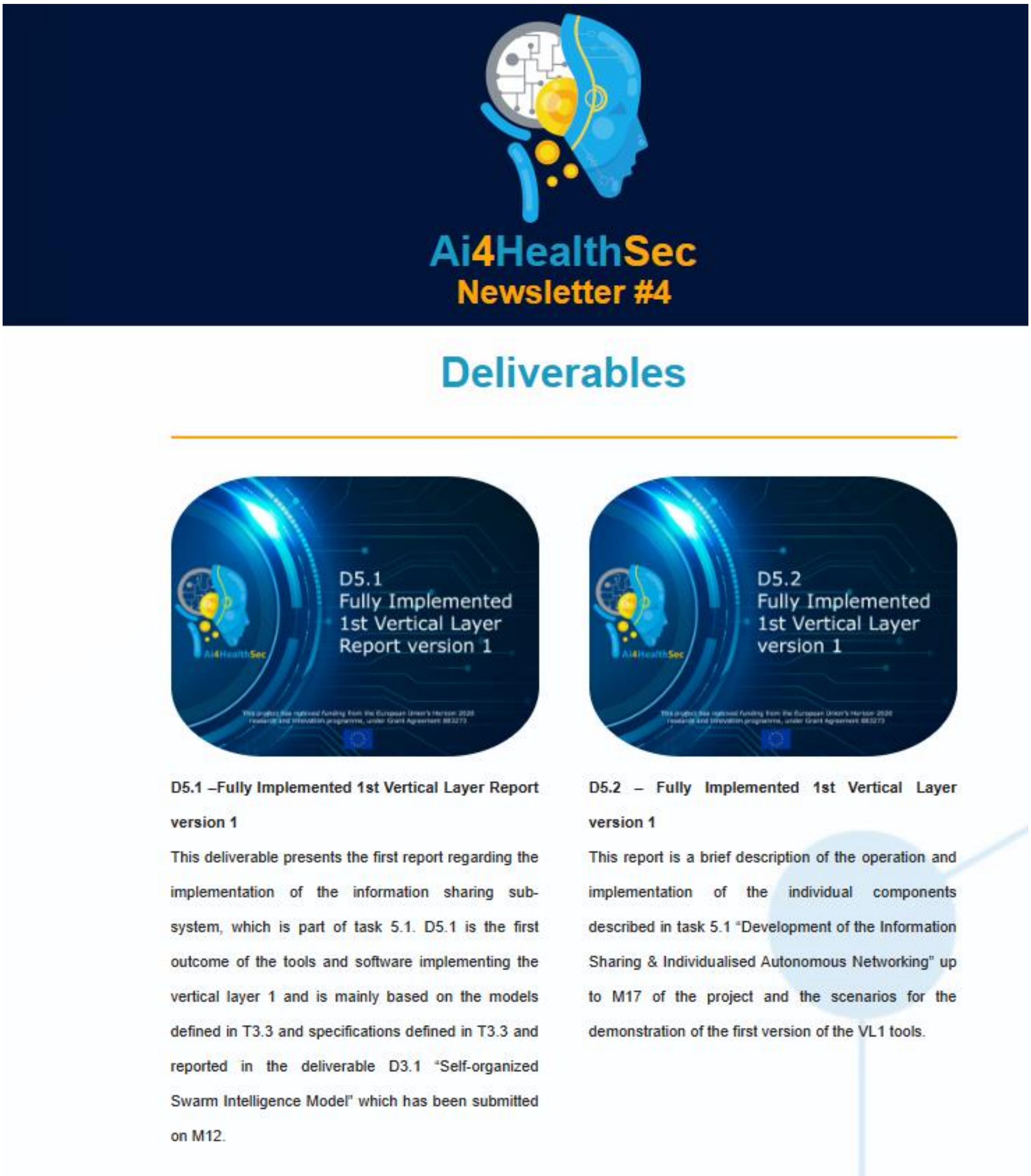


Project Newsletters

Figure 4-36. Extract from the website (https://www.AI4HEALTHSEC.eu/newsletters/)

Until November 2023, 7 newsletters have been designed and communicated. A final one is planned to be issued at the end of the project. (Since this report is drafted in early December 2023, this final newsletter is not included here). Four (4) of the newsletters have been issued within the reporting period.

Newsletter #4



Ai4HealthSec
Newsletter #4

Deliverables

D5.1 –Fully Implemented 1st Vertical Layer Report version 1

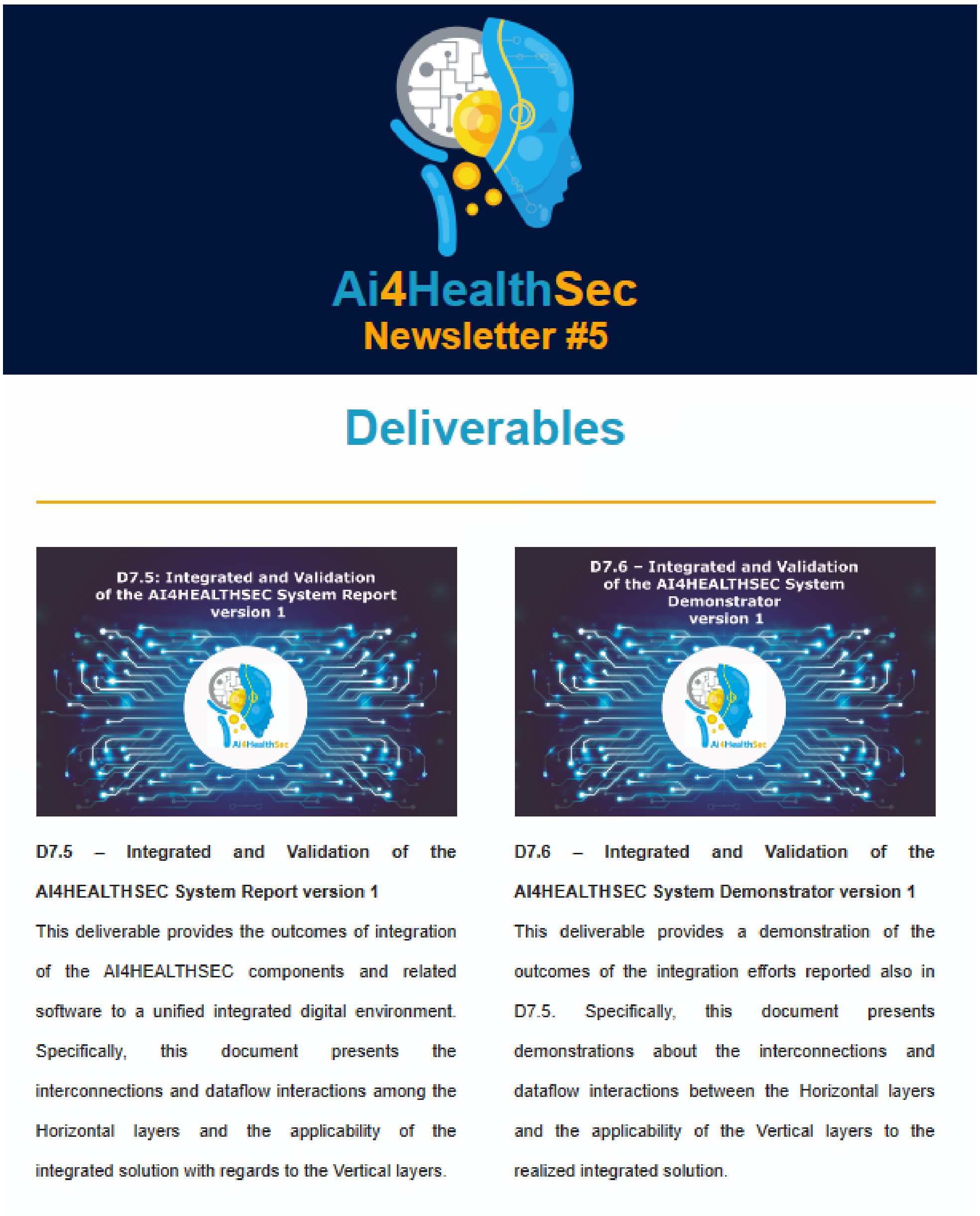
This deliverable presents the first report regarding the implementation of the information sharing sub-system, which is part of task 5.1. D5.1 is the first outcome of the tools and software implementing the vertical layer 1 and is mainly based on the models defined in T3.3 and specifications defined in T3.3 and reported in the deliverable D3.1 "Self-organized Swarm Intelligence Model" which has been submitted on M12.

D5.2 – Fully Implemented 1st Vertical Layer version 1

This report is a brief description of the operation and implementation of the individual components described in task 5.1 "Development of the Information Sharing & Individualised Autonomous Networking" up to M17 of the project and the scenarios for the demonstration of the first version of the VL1 tools.

Figure 4-37. Screenshot of the 4th project Newsletter

Newsletter #5



Ai4HealthSec
Newsletter #5

Deliverables

D7.5: Integrated and Validation of the AI4HEALTHSEC System Report version 1

D7.5 – Integrated and Validation of the AI4HEALTHSEC System Report version 1

This deliverable provides the outcomes of integration of the AI4HEALTHSEC components and related software to a unified integrated digital environment. Specifically, this document presents the interconnections and dataflow interactions among the Horizontal layers and the applicability of the integrated solution with regards to the Vertical layers.

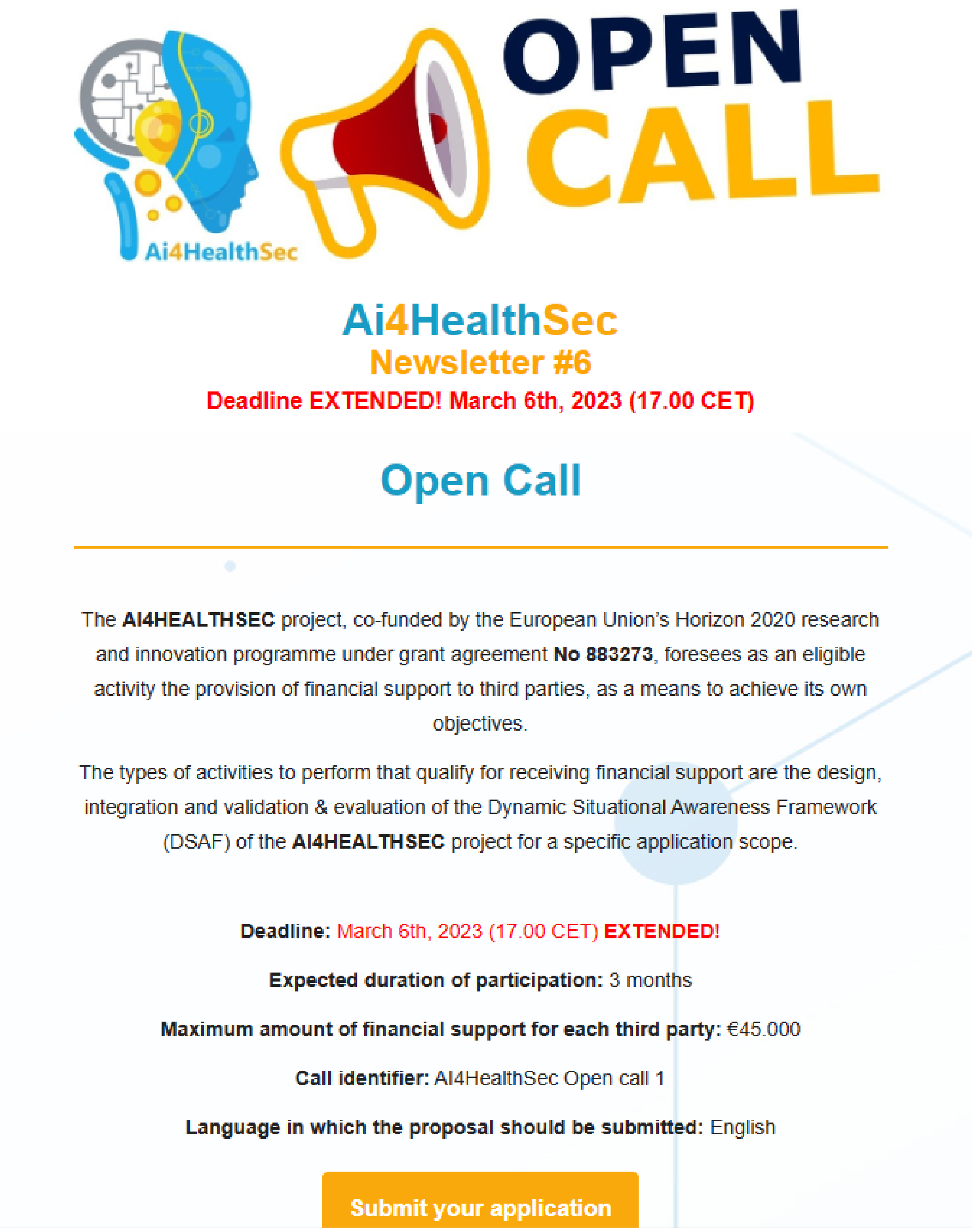
D7.6 – Integrated and Validation of the AI4HEALTHSEC System Demonstrator version 1

D7.6 – Integrated and Validation of the AI4HEALTHSEC System Demonstrator version 1

This deliverable provides a demonstration of the outcomes of the integration efforts reported also in D7.5. Specifically, this document presents demonstrations about the interconnections and dataflow interactions between the Horizontal layers and the applicability of the Vertical layers to the realized integrated solution.

Figure 4-38. Screenshot of the 5th project Newsletter

Newsletter #6



Ai4HealthSec

Newsletter #6

Deadline EXTENDED! March 6th, 2023 (17.00 CET)

Open Call

The **AI4HEALTHSEC** project, co-funded by the European Union's Horizon 2020 research and innovation programme under grant agreement **No 883273**, foresees as an eligible activity the provision of financial support to third parties, as a means to achieve its own objectives.

The types of activities to perform that qualify for receiving financial support are the design, integration and validation & evaluation of the Dynamic Situational Awareness Framework (DSAF) of the **AI4HEALTHSEC** project for a specific application scope.

Deadline: March 6th, 2023 (17.00 CET) **EXTENDED!**

Expected duration of participation: 3 months

Maximum amount of financial support for each third party: €45.000

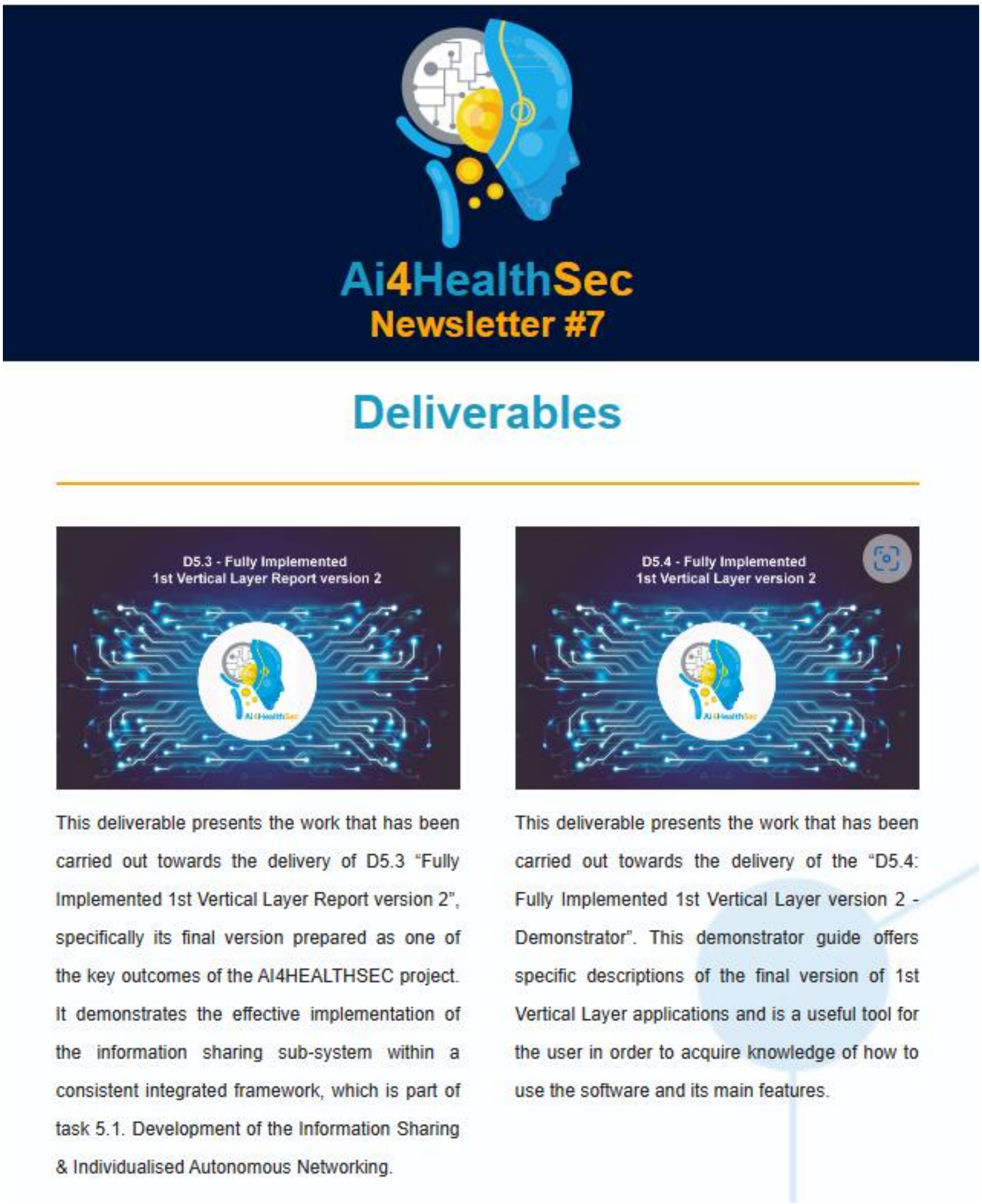
Call identifier: AI4HealthSec Open call 1

Language in which the proposal should be submitted: English

Submit your application

Figure 4-39. Screenshot of the 6th project Newsletter

Newsletter #7



Ai4HealthSec
Newsletter #7

Deliverables

This deliverable presents the work that has been carried out towards the delivery of D5.3 "Fully Implemented 1st Vertical Layer Report version 2", specifically its final version prepared as one of the key outcomes of the AI4HEALTHSEC project. It demonstrates the effective implementation of the information sharing sub-system within a consistent integrated framework, which is part of task 5.1. Development of the Information Sharing & Individualised Autonomous Networking.

This deliverable presents the work that has been carried out towards the delivery of the "D5.4: Fully Implemented 1st Vertical Layer version 2 - Demonstrator". This demonstrator guide offers specific descriptions of the final version of 1st Vertical Layer applications and is a useful tool for the user in order to acquire knowledge of how to use the software and its main features.

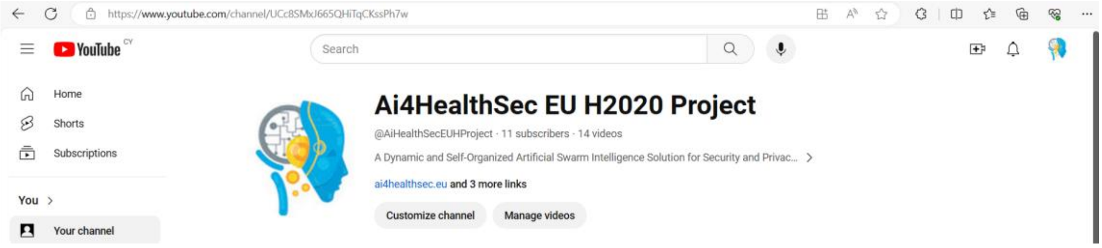
Figure 4-40. Screenshot of the 7th project Newsletter

4.4 Videos

The YouTube channel[34] is one of the channels used by the AI4HEALTHSEC project in order to disseminate the outputs of the project. All videos are available in the AI4HEALTHSEC YouTube channel but also in AI4HEALTHSEC website https://www.ai4healthsec.eu/videos/.

The project has created the following categories of videos:

- Videos introducing project partners and their involvement in the project (8)
- Videos demonstrating parts of the Ai4HealthSec solution (4)
- Videos created to support the open call (2)
- Video created as a holiday greeting's card for the project (1)
- Video summing up the pilots and providing some quoted from the feedback received (1)[35]



https://www.youtube.com/channel/UCc8SMxJ665QHiTqCKssPh7w

Ai4HealthSec EU H2020 Project

@AiHealthSecEUHProject · 11 subscribers · 14 videos

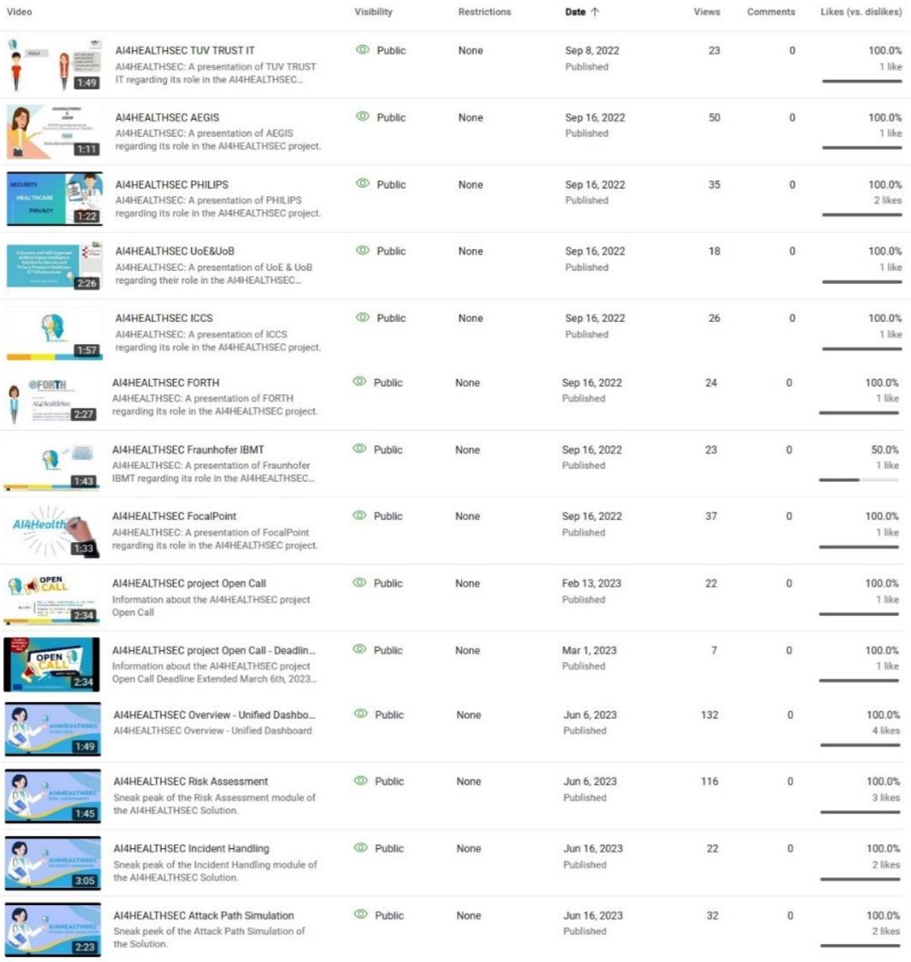
A Dynamic and Self-Organized Artificial Swarm Intelligence Solution for Security and Privac...

ai4healthsec.eu and 3 more links

Figure 4-41. YouTube Ai4HEALTHSEC project Channel homepage

[34] https://www.youtube.com/channel/UCc8SMxJ665QHiTqCKssPh7w

[35] This video is the last video of the project and is currently under preparation. It is expected to be promoted at the end of the project period.



Video	Visibility	Restrictions	Date ↑	Views	Comments	Likes (vs. dislikes)
1:49 AI4HEALTHSEC TUV TRUST IT AI4HEALTHSEC: A presentation of TUV TRUST IT regarding its role in the AI4HEALTHSEC...	Public	None	Sep 8, 2022 Published	23	0	100.0% 1 like
1:11 AI4HEALTHSEC AEGIS AI4HEALTHSEC: A presentation of AEGIS regarding its role in the AI4HEALTHSEC project.	Public	None	Sep 16, 2022 Published	50	0	100.0% 1 like
1:22 AI4HEALTHSEC PHILIPS AI4HEALTHSEC: A presentation of PHILIPS regarding its role in the AI4HEALTHSEC project.	Public	None	Sep 16, 2022 Published	35	0	100.0% 2 likes
2:26 AI4HEALTHSEC UoE&UoB AI4HEALTHSEC: A presentation of UoE & UoB regarding their role in the AI4HEALTHSEC...	Public	None	Sep 16, 2022 Published	18	0	100.0% 1 like
1:57 AI4HEALTHSEC ICCS AI4HEALTHSEC: A presentation of ICCS regarding its role in the AI4HEALTHSEC project.	Public	None	Sep 16, 2022 Published	26	0	100.0% 1 like
2:27 AI4HEALTHSEC FORTH AI4HEALTHSEC: A presentation of FORTH regarding its role in the AI4HEALTHSEC project.	Public	None	Sep 16, 2022 Published	24	0	100.0% 1 like
1:43 AI4HEALTHSEC Fraunhofer IBMT AI4HEALTHSEC: A presentation of Fraunhofer IBMT regarding its role in the AI4HEALTHSEC...	Public	None	Sep 16, 2022 Published	23	0	50.0% 1 like
1:33 AI4HEALTHSEC FocalPoint AI4HEALTHSEC: A presentation of FocalPoint regarding its role in the AI4HEALTHSEC project.	Public	None	Sep 16, 2022 Published	37	0	100.0% 1 like
2:34 AI4HEALTHSEC project Open Call Information about the AI4HEALTHSEC project Open Call	Public	None	Feb 13, 2023 Published	22	0	100.0% 1 like
2:34 AI4HEALTHSEC project Open Call - Deadlin... Information about the AI4HEALTHSEC project Open Call Deadline Extended March 6th, 2023...	Public	None	Mar 1, 2023 Published	7	0	100.0% 1 like
1:49 AI4HEALTHSEC Overview - Unified Dashbo... AI4HEALTHSEC Overview - Unified Dashboard	Public	None	Jun 6, 2023 Published	132	0	100.0% 4 likes
1:45 AI4HEALTHSEC Risk Assessment Sneak peak of the Risk Assessment module of the AI4HEALTHSEC Solution.	Public	None	Jun 6, 2023 Published	116	0	100.0% 3 likes
3:05 AI4HEALTHSEC Incident Handling Sneak peak of the Incident Handling module of the AI4HEALTHSEC Solution.	Public	None	Jun 16, 2023 Published	22	0	100.0% 2 likes
2:23 AI4HEALTHSEC Attack Path Simulation Sneak peek of the Attack Path Simulation of the Solution.	Public	None	Jun 16, 2023 Published	32	0	100.0% 2 likes

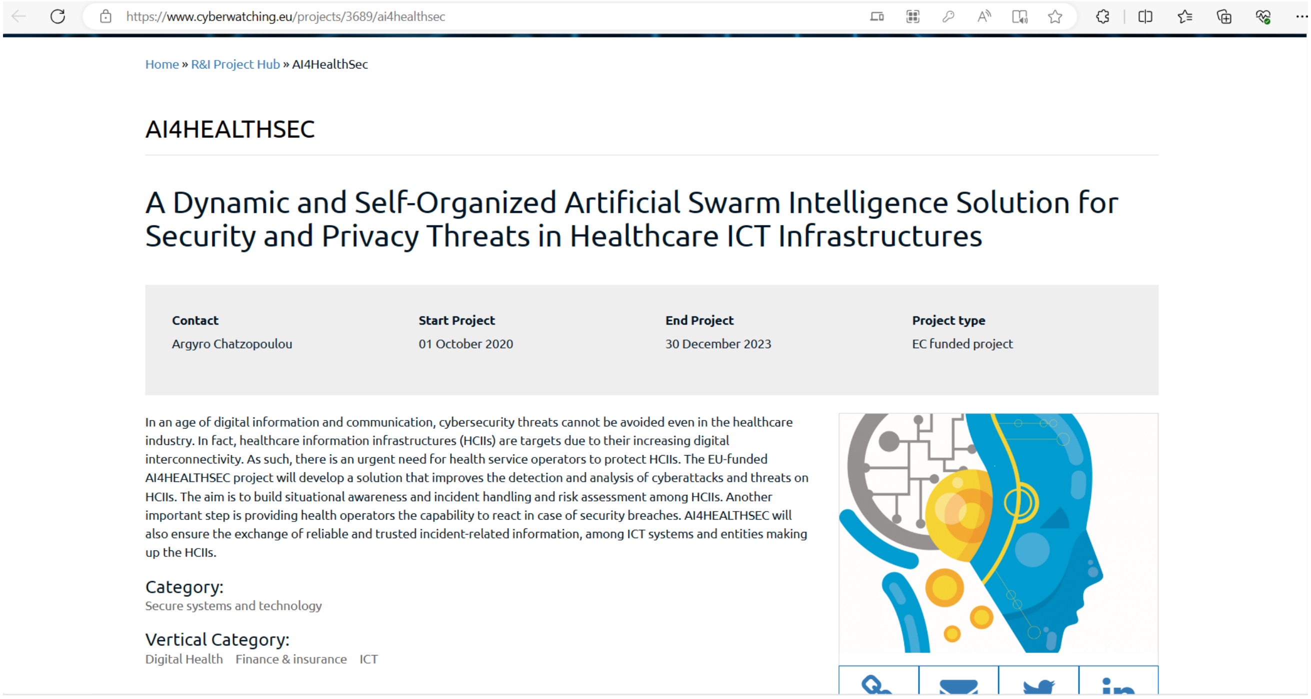
Figure 4-42. Videos uploaded in the YouTube channel

4.5 Cyberwatching

Cyberwatching.eu[36] is a project funded by the European Commission under the Horizon 2020 framework program. It is part of the European Union's efforts to enhance and promote cybersecurity and privacy in the digital landscape. Cyberwatching.eu aims to support the European cybersecurity ecosystem by providing a centralized platform for information, collaboration, and awareness.

The Ai4HealthSec project, has been registered as a project within the cyberwatching platform and a mini-project page has been created.

[36] https://www.cyberwatching.eu/



Home » R&I Project Hub » AI4HealthSec

AI4HEALTHSEC

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

Contact	Start Project	End Project	Project type
Argyro Chatzopoulou	01 October 2020	30 December 2023	EC funded project

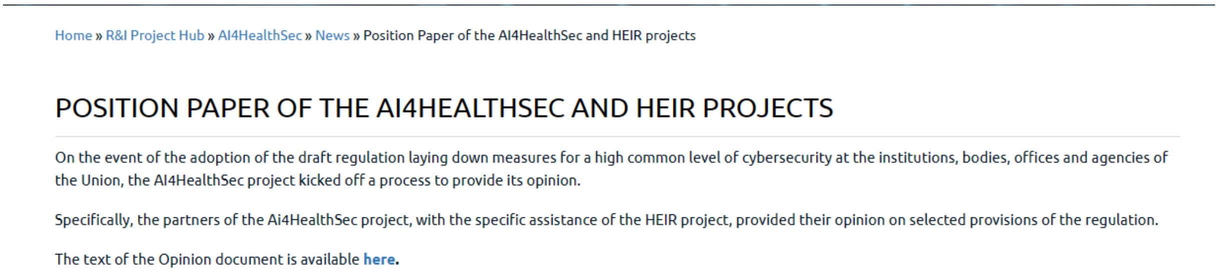
In an age of digital information and communication, cybersecurity threats cannot be avoided even in the healthcare industry. In fact, healthcare information infrastructures (HCIIs) are targets due to their increasing digital interconnectivity. As such, there is an urgent need for health service operators to protect HCIIs. The EU-funded AI4HEALTHSEC project will develop a solution that improves the detection and analysis of cyberattacks and threats on HCIIs. The aim is to build situational awareness and incident handling and risk assessment among HCIIs. Another important step is providing health operators the capability to react in case of security breaches. AI4HEALTHSEC will also ensure the exchange of reliable and trusted incident-related information, among ICT systems and entities making up the HCIIs.

Category:
Secure systems and technology

Vertical Category:
Digital Health Finance & insurance ICT

Figure 4-43. AI4HEALTHSEC in cyberwatching.eu

Through this page, the Position Paper of the AI4HealthSec and HEIR projects on the event of the adoption of the draft regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union was further promoted.



Home » R&I Project Hub » AI4HealthSec » News » Position Paper of the AI4HealthSec and HEIR projects

POSITION PAPER OF THE AI4HEALTHSEC AND HEIR PROJECTS

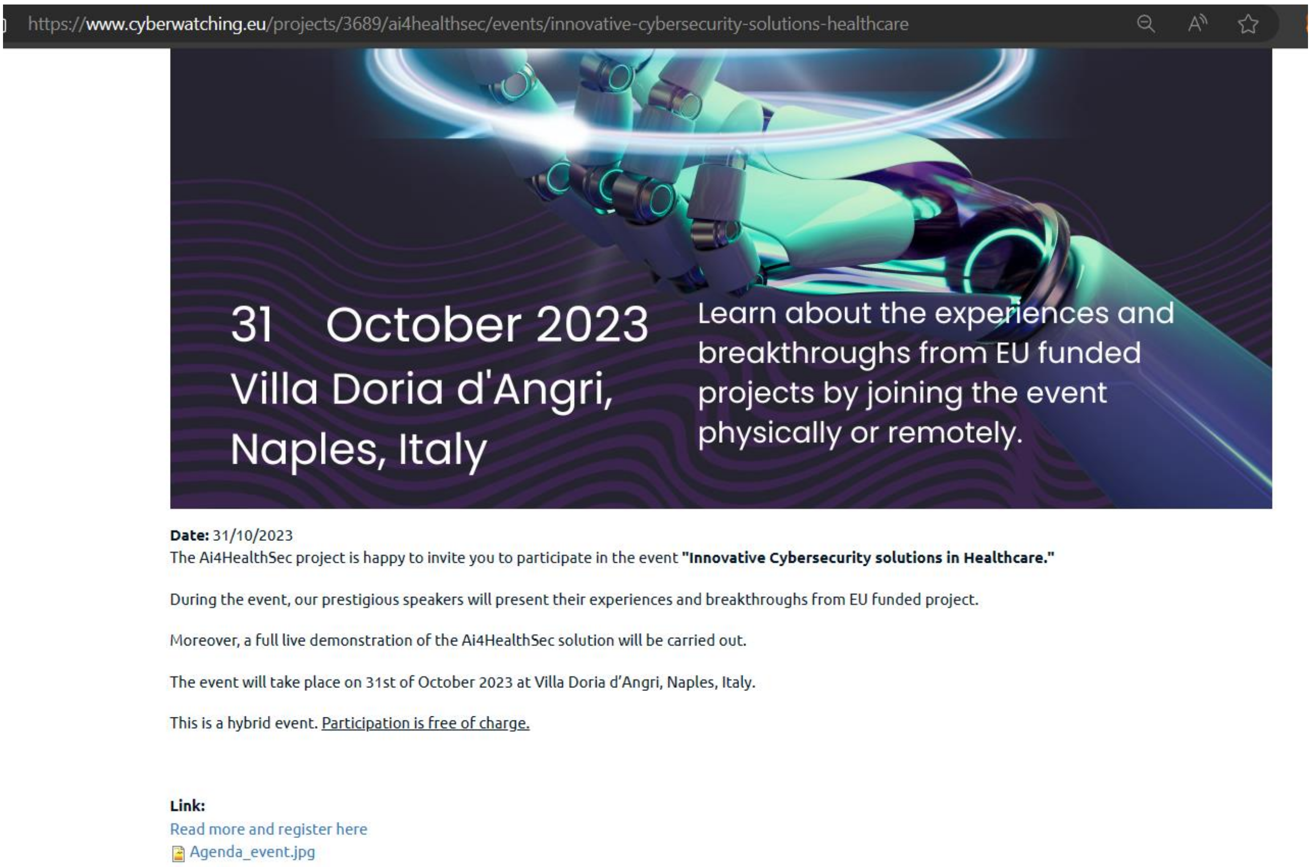
On the event of the adoption of the draft regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union, the AI4HealthSec project kicked off a process to provide its opinion.

Specifically, the partners of the Ai4HealthSec project, with the specific assistance of the HEIR project, provided their opinion on selected provisions of the regulation.

The text of the Opinion document is available **here**.

Figure 4-44. AI4HEALTHSEC in cyberwatching.eu

Moreover, the final event of the Ai4HealthSec project, was also promoted through the cyberwatching platform.



https://www.cyberwatching.eu/projects/3689/ai4healthsec/events/innovative-cybersecurity-solutions-healthcare
31 October 2023
Villa Doria d'Angri,
Naples, Italy
Learn about the experiences and breakthroughs from EU funded projects by joining the event physically or remotely.

Date: 31/10/2023

The Ai4HealthSec project is happy to invite you to participate in the event **"Innovative Cybersecurity solutions in Healthcare."**

During the event, our prestigious speakers will present their experiences and breakthroughs from EU funded project.

Moreover, a full live demonstration of the Ai4HealthSec solution will be carried out.

The event will take place on 31st of October 2023 at Villa Doria d'Angri, Naples, Italy.

This is a hybrid event. Participation is free of charge.

Link:
Read more and register here
Agenda_event.jpg

Figure 4-45. AI4HEALTHSEC in cyberwatching.eu

The Ai4HealthSec project also participated in the project radar functionality of the cyberwatching platform.

Since 2004, the European Commission has launched 115 calls which were either explicitly supporting projects in the domain of cybersecurity and privacy or from which projects in this area were supported. This resulted in awarding over 260 consortia with funding grants to the tune of €1.1 billion.

Targeting policy makers and researchers across Europe, the new live European Project Radar makes sense of this busy landscape providing bird's eye view of the European Cybersecurity research landscape making it easier to gather swift yet statistically sound information on the state of the art of the landscape. Indeed, the Radar's primary value proposition therefore is that of saving the user time and money by processing and analysing detailed landscape data for them.[37]

Based on the well known "Technology Radar" methodology developed and open-sourced by ThoughtWorks, the Cyberwatching.eu project uses a number of underpinning information sources to visualise the state of the art of these projects as a means to maintain oversight of the larger European Cybersecurity research landscape. The radar has many uses and here are just a few:

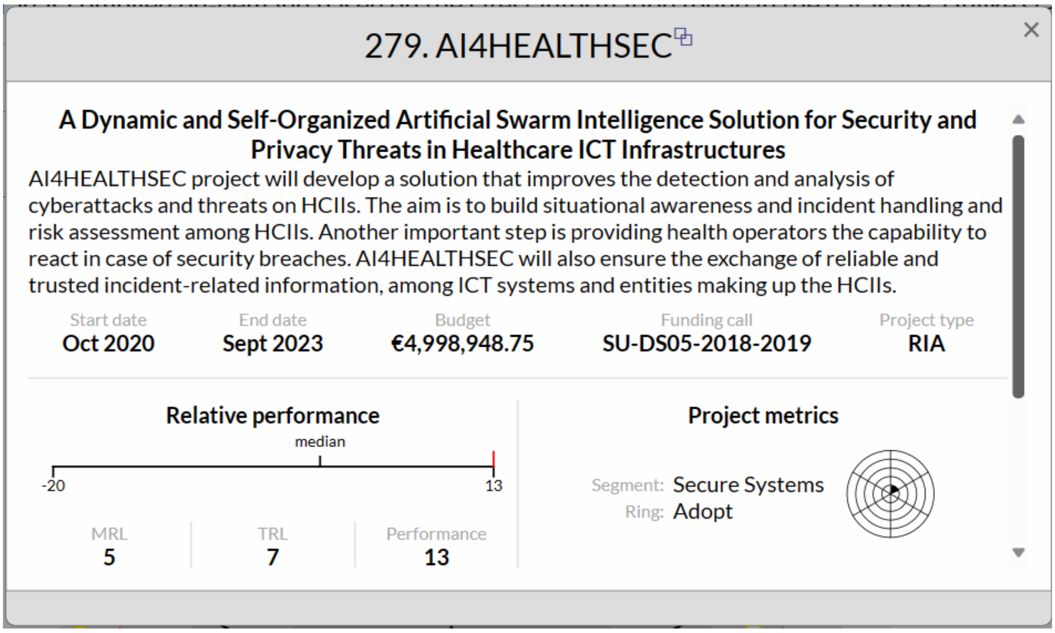
- Identify low and over-developed/funded spaces based on the cybersecurity R&I taxonomy

[37] https://www.cyberwatching.eu/technology-radar

- Map projects based on JRC taxonomy: cybersecurity domain, vertical sectors, technology and use cases
- Identify projects for clustering activities & events
- Track project progress and maturity in the project lifecycle.
- Access information on projects' Market and Technology readiness level
- Get up-to-date informatoin on the project through their mini-site hosted by cyberwatching.eu
- Contact the project directly through the radar
- Update your own project's information directly and make sure you are visible

The new 2021 radar is both autonomous with real-time information management for projects

The entry of the Ai4HealthSec project within the cyberwatching radar is shown through Figure 2-1Figure 4-46, Figure 4-47**Errore. L'origine riferimento non è stata trovata.** and Figure 4-48**Errore. L'origine riferimento non è stata trovata.**.



279. AI4HEALTHSEC

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

AI4HEALTHSEC project will develop a solution that improves the detection and analysis of cyberattacks and threats on HCIIs. The aim is to build situational awareness and incident handling and risk assessment among HCIIs. Another important step is providing health operators the capability to react in case of security breaches. AI4HEALTHSEC will also ensure the exchange of reliable and trusted incident-related information, among ICT systems and entities making up the HCIIs.

Start date	End date	Budget	Funding call	Project type
Oct 2020	Sept 2023	€4,998,948.75	SU-DS05-2018-2019	RIA

Relative performance

MRL	TRL	Performance
5	7	13

Project metrics

Segment: Secure Systems
Ring: Adopt

Figure 4-46. AI4HEALTHSEC in cyberwatching Project Radar (1)

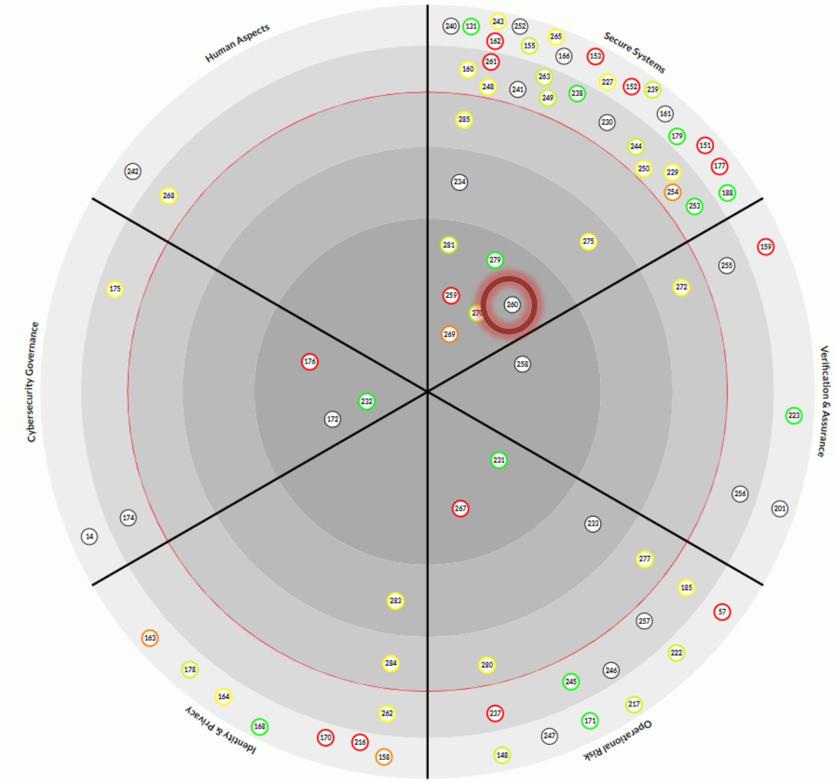
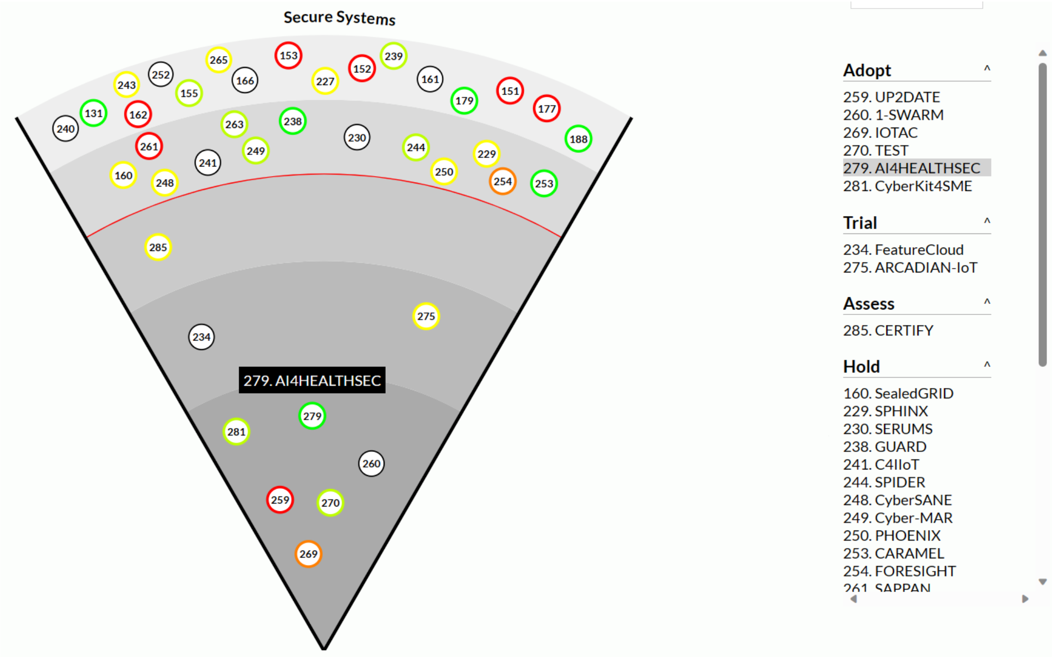


Figure 4-47. AI4HEALTHSEC in cyberwatching Project Radar (2) – Project 279



Adopt

259. UP2DATE
260. 1-SWARM
269. IOTAC
270. TEST
279. AI4HEALTHSEC
281. CyberKit4SME

Trial

234. FeatureCloud
275. ARCADIAN-IoT

Assess

285. CERTIFY

Hold

160. SealedGRID
229. SPHINX
230. SERUMS
238. GUARD
241. C4IIoT
244. SPIDER
248. CyberSANE
249. Cyber-MAR
250. PHOENIX
253. CARAMEL
254. FORESIGHT
261. SAPPAN

Figure 4-48. AI4HEALTHSEC in cyberwatching Project Radar (3)

5 Project publications

5.1.1 Brochures / leaflets and promotional material

For the final Event of the AI4HEALTHSEC project the printed material was created for the communication and dissemination of the event.

Specifically, the printed material included :

- A business folder with the project logo and details and
- The agenda of the final event.

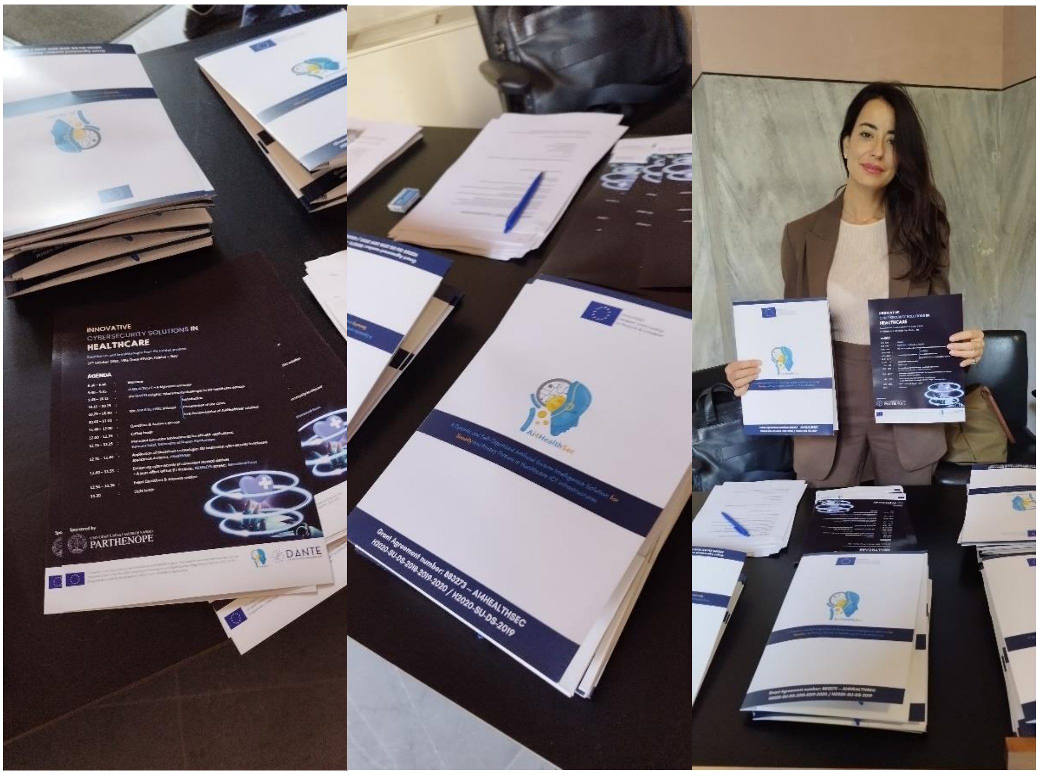

INNOVATIVE
CYBERSECURITY SOLUTIONS IN
HEALTHCARE
AGENDA
PARTHENOPE
DANTE
Ai4HealthSec
Grant Agreement number: 883273 – AI4HEALTHSEC
H2020-SU-DS-2018-2019-2020 / H2020-SU-DS-2019

Figure 5-49. AI4HEALTHSEC final event promotional material

5.1.2 Publications in professional journals

This section provides an accounting of the Journal publications of the Ai4HealthSec project In summary, the project partners published **12** Journal publications within the reporting period. In section 7. The KPIs for the entire duration of the project are presented.

Vulnerability prediction for secure healthcare supply chain service delivery

Islam, S., Abba, A., Ismail, U., Mouratidis, H., & Papastergiou, S. (2022). Vulnerability prediction for secure healthcare supply chain service delivery. Integrated Computer-Aided Engineering, (Preprint), 1-21. http://doi.org/10.3233/ICA-220689

Healthcare organisations are constantly facing sophisticated cyberattacks due to the sensitivity and criticality of patient health care information and wide connectivity of medical devices. Such attacks can pose potential disruptions to critical services delivery. There are number of existing works that focus on using Machine Learning (ML) models for predicting vulnerability and exploitation but most of these works focused on parameterized values to predict severity and exploitability. This paper proposes a novel method that uses ontology axioms to define essential concepts related to the overall healthcare ecosystem and to ensure semantic consistency checking among such concepts. The application of ontology enables the formal specification and description of healthcare ecosystem and the key elements used in vulnerability assessment as a set of concepts. Such specification also strengthens the relationships that exist between healthcare-based and vulnerability assessment concepts, in addition to semantic definition and reasoning of the concepts. Our work also makes use of Machine Learning techniques to predict possible security vulnerabilities in health care supply chain services. The paper demonstrates the applicability of our work by using vulnerability datasets to predict the exploitation. The results show that the conceptualization of healthcare sector cybersecurity using an ontological approach provides mechanisms to better understand the correlation between the healthcare sector and the security domain, while the ML algorithms increase the accuracy of the vulnerability exploitability prediction. Our result shows that using Linear Regression, Decision Tree and Random Forest provided a reasonable result for predicting vulnerability exploitability.

The supply chain of a Living Lab: Modelling security, privacy, and vulnerability issues alongside with their impact and potential mitigation strategies

Kioskli, K., Dellagiacoma, D., Fotis, T., & Mouratidis, H. (2022). The supply chain of a Living Lab: Modelling security, privacy, and vulnerability issues alongside with their impact and potential mitigation strategies. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 13(2), 147-182. http://doi.org/10.22667/JOWUA.2022.06.30.147

Worldwide, vulnerabilities and weak security strategies are exploited everyday by adversaries in healthcare organizations. Healthcare is targeted because these crimes are high-reward and low-risk. The attacks differ every time, from hacking medical devices, such as sensors, to stealing patients' data from electronic health records databases. The effects of these attacks are both short and long term lived, depending on the incidence handling process that each sector is adopting. The Covid-19 pandemic has exposed, in full, that healthcare systems are vulnerable and vastly unprotected while representing a threat to global public health. An important part of the healthcare ecosystem, for the development and validation of innovative tools and methodologies, is the Living Labs which are community-based and adopt co-creation as their primary approach. Because of the many stakeholders involved in the processes of the Living Labs, cybersecurity ought to be in their center. Besides the proven great importance of the Living Labs as part of healthcare, there is no research on security and privacy issues around them. The main purpose of this paper is to explore the supply chain of a Living Lab and identify its security and privacy challenges alongside with its vulnerabilities. The SecTro tool has been used to provide a thorough analysis which follows the Privacy-by-Design approach. The originality and novelty of our work are shown from: (i) moving one step further from desk studies by including requirements from citizens and professionals; (ii) being integrated into an effort from various researchers to supply a holistic approach to Data Privacy Governance; (iii) the first time which a paper is considering and analysing the supply chain of the Living Labs.

Iterative Annotation of Biomedical NER Corpora with Deep Neural Networks and Knowledge Bases

Silvestri, S., Gargiulo, F., & Ciampi, M. (2022). Iterative annotation of biomedical ner corpora with deep neural networks and knowledge bases. Applied Sciences, 12(12), 5775. http://doi.org/10.3390/app12125775

The large availability of clinical natural language documents, such as clinical narratives or diagnoses, requires the definition of smart automatic systems for their processing and analysis, but the lack of annotated corpora in the biomedical domain, especially in languages different from English, makes it difficult to exploit the state-of-art machine-learning systems to extract information from such kinds of documents. For these reasons, healthcare professionals lose big opportunities that can arise from the analysis of this data. In this paper, we propose a methodology to reduce the manual efforts needed to annotate a biomedical named entity recognition (B-NER) corpus, exploiting both active learning and distant supervision, respectively based on deep learning models (e.g., Bi-LSTM, word2vec FastText, ELMo and BERT) and biomedical knowledge bases, in order to speed up the annotation task and limit class imbalance issues. We assessed this approach by creating an Italian-language electronic health record corpus annotated with biomedical domain entities in a small fraction of the time required for a fully manual annotation. The obtained corpus was used to train a B-NER deep neural network whose performances are comparable with the state of the art, with an F1-Score equal to 0.9661 and 0.8875 on two test sets.

Process Authentication through Blockchain: Three Case Studies

Ciampi, M., Romano, D., & Schmid, G. (2022). Process Authentication through Blockchain: Three Case Studies. Cryptography, 6(4), 58. http://doi.org/10.3390/cryptography6040058

In this work, we elaborate on the concept of process authenticity, which intuitively corresponds to the validity of all process steps and their proper binding. It represents the most exciting forefront of distributed ledger technology research concerning the primary challenge of reliably connecting distributed ledger networks to the physical context it must operate. More in detail, the paper describes a novel methodological approach to ensure the authenticity of business processes through blockchain and several security mechanisms applied to the digital twins of the actual processes. We illustrate difficulties and opportunities deriving from implementing process authenticity in concrete case studies in which we were involved as software designers belonging to three critical application domains: document dematerialization, e-voting, and healthcare.

Cyberattack Path Generation and Prioritisation for Securing Healthcare Systems

Islam, S.; Papastergiou, S.; Kalogeraki, E.-M.; Kioskli, K. Cyberattack Path Generation and Prioritisation for Securing Healthcare Systems. Appl. Sci. 2022, 12, 4443. https://doi.org/10.3390/app12094443

Cyberattacks in the healthcare sector are constantly increasing due to the increased usage of information technology in modern healthcare and the benefits of acquiring a patient healthcare record. Attack path discovery provides useful information to identify the possible paths that potential attackers might follow for a successful attack. By identifying the necessary paths, the mitigation of potential attacks becomes more effective in a proactive manner. Recently, there have been several works that focus on cyberattack path discovery in various sectors, mainly on critical infrastructure. However, there is a lack of focus on the vulnerability, exploitability and target user profile for the attack path generation. This is important for healthcare systems where users commonly have a lack of awareness and knowledge about the overall IT infrastructure. This paper presents a novel methodology for the cyberattack path discovery that is used to identify and analyse the possible attack paths and prioritise the ones that require immediate attention to ensure security within the healthcare ecosystem. The proposed methodology follows the existing published vulnerabilities from common vulnerabilities and exposures. It adopts the common vulnerability scoring system so that base metrics and exploitability features can be used to determine and prioritise the possible attack paths based on the threat actor capability, asset dependency and target user profile and evidence of indicator of compromise. The work includes a real example from the healthcare use case to demonstrate the methodology used for the attack path generation. The result from the studied context, which processes big data from healthcare applications, shows that the uses of various parameters such as CVSS metrics, threat actor profile, and Indicator of Compromise allow us to generate realistic attack paths. This certainly supports the healthcare practitioners in identifying the controls that are required to secure the overall healthcare ecosystem.

An integrated cyber security risk management framework and risk predication for the critical infrastructure protection

Kure, H.I., Islam, S. & Mouratidis, H. An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. Neural Computing & Application, 34, 15241–15271 (2022). https://doi.org/10.1007/s00521-022-06959-2

Cyber security risk management plays an important role for today's businesses due to the rapidly changing threat landscape and the existence of evolving sophisticated cyber attacks. It is necessary for organisations, of any size, but in particular those that are associated with a critical infrastructure, to understand the risks, so that suitable controls can be taken for the overall business continuity and critical service delivery. There are a number of works that aim to develop systematic processes for risk assessment and management. However, the existing works have limited input from threat intelligence properties and evolving attack trends, resulting in limited contextual information related to cyber security risks. This creates a challenge, especially in the context of critical infrastructures, since attacks have evolved from technical to socio-technical and protecting against them requires such contextual information. This research proposes a novel integrated cyber security risk management (i-CSRM) framework that responds to that challenge by supporting systematic identification of critical assets through the use of a decision support mechanism built on fuzzy set theory, by predicting risk types through machine learning techniques, and by assessing the effectiveness of existing controls. The framework is composed of a language, a process, and it is supported by an automated tool. The paper also reports on the evaluation of our work to a real case study of a critical infrastructure. The results reveal that using the fuzzy set theory in assessing assets' criticality, our work supports stakeholders towards an effective risk management by assessing each asset's criticality. Furthermore, the results have demonstrated the machine learning classifiers' exemplary performance to predict different risk types including denial of service, cyber espionage and crimeware.

Chidroid: A Mobile Android Application for Log Collection and Security Analysis in Healthcare and IoMT

Karagiannis, S., Ribeiro, L. L., Ntantogian, C., Magkos, E., & Campos, L. M. (2023). Chidroid: A Mobile Android Application for Log Collection and Security Analysis in Healthcare and IoMT. Applied Sciences, 13(5), 3061. http://doi.org/10.3390/app13053061

The Internet of Medical Things (IoMT) is a growing trend that has led to the use of connected devices, known as the Internet of Health. The healthcare domain has been a target of cyberattacks, especially with a large number of IoMT devices connected to hospital networks. This factor could allow attackers to access patients' personal health information (PHI). This research paper proposes Chidroid, an innovative mobile Android application that can retrieve, collect, and distribute logs from smart healthcare devices. The proposed approach enables the creation of datasets, allowing non-structured data to be parsed into semi-structured or structured data that can be used for machine learning and deep learning, and the proposed approach can serve as a universal policy-based tool to examine and analyse security issues in most recent Android versions by distributing logs for analysis. The validation tests demonstrated that the application could retrieve logs and system metrics from various assets and devices in an efficient manner. The collected logs can provide visibility into the device's activities and help to detect and mitigate potential security risks. This research introduces a way to perform a security analysis on Android devices that uses minimal system resources and reduces battery consumption by pushing the analysis stage to the edge.

A Machine Learning Approach for the NLP-Based Analysis of Cyber Threats and Vulnerabilities of the Healthcare Ecosystem

Silvestri, S., Islam, S., Papastergiou, S., Tzagkarakis, C., & Ciampi, M. (2023). A Machine Learning Approach for the NLP-Based Analysis of Cyber Threats and Vulnerabilities of the Healthcare Ecosystem. Sensors, 23(2), 651. http://doi.org/10.3390/s23020651

Digitization in healthcare systems, with the wide adoption of Electronic Health Records, connected medical devices, software and systems providing efficient healthcare service delivery and management. On the other hand, the use of these systems has significantly increased cyber threats in the healthcare sector. Vulnerabilities in the existing and legacy systems are one of the key causes for the threats and related risks. Understanding and addressing the threats from the connected medical devices and other parts of the ICT health infrastructure are of paramount importance for ensuring security within the overall healthcare ecosystem. Threat and vulnerability analysis provides an effective way to lower the impact of risks relating to the existing vulnerabilities. However, this is a challenging task due to the availability of massive data which makes it difficult to identify potential patterns of security issues. This paper contributes towards an effective threats and vulnerabilities analysis by adopting Machine Learning models, such as the BERT neural language model and XGBoost, to extract updated information from the Natural Language documents largely available on the web, evaluating at the same time the level of the identified threats and vulnerabilities that can impact on the healthcare system, providing the required information for the most appropriate management of the risk. Experiments were performed based on CS news extracted from the Hacker News website and on Common Vulnerabilities and Exposures (CVE) vulnerability reports. The results demonstrate the effectiveness of the proposed approach, which provides a realistic manner to assess the threats and vulnerabilities from Natural Language texts, allowing adopting it in real-world Healthcare ecosystems.

Co-creation in a digital health living lab: A case study

Fotis, T., Kioskli, K., Sundaralingam, A., Fasihi, A., & Mouratidis, H. (2023). Co-creation in a digital health living lab: A case study. Frontiers in Public Health, 10, 892930. http://doi.org/10.3389/fpubh.2022.892930

Co-creation in healthcare, especially in developing digital health solutions, has been widely identified as a fundamental principle for person-centered technologies that could accelerate the adaptation of innovation. A Digital Health Living Lab based on community offers a sustainable and real-life environment to ideate, develop, and evaluate digital health solutions addressing the needs of multiple stakeholders. This article presents the experience of the School of Sport and Health Sciences at the University of Brighton in establishing a Digital Health Living Lab. In addition, we share a proposed step-by-step approach to establishing such a living lab in the community, supplemented by a case study of product development.

The Importance of Conceptualising the Human-Centric Approach in Maintaining and Promoting Cybersecurity-Hygiene in Healthcare 4.0

Kioskli, K., Fotis, T., Nifakos, S., & Mouratidis, H. (2023). The Importance of Conceptualising the Human-Centric Approach in Maintaining and Promoting Cybersecurity-Hygiene in Healthcare 4.0. Applied Sciences, 13(6), 3410. http://doi.org/10.3390/app13063410

The cyberspace depicts an increasing number of difficulties related to security, especially in healthcare. This is evident from how vulnerable critical infrastructures are to cyberattacks and are unprotected against cybercrime. Users, ideally, should maintain a good level of cyber hygiene, via regular software updates and the development of unique passwords, as an effective way to become resilient to cyberattacks. Cyber security breaches are a top priority, and most users are aware that their behaviours may put them at risk; however, they are not educated to follow best practices, such as protecting their passwords. Mass cyber education may serve as a means to offset poor cyber security behaviours; however, mandatory education becomes a questionable point if the content is not focused on human factors, using human-centric approaches and taking into account end users' behaviours, which is currently the case. The nature of the present paper is largely exploratory, and the purpose is two-fold: To present and explore the cyber hygiene definition, context and habits of end users in order to strengthen our understanding of users. Our paper reports the best practices that should be used by healthcare organisations and healthcare professionals to maintain good cyber hygiene and how these can be applied via a healthcare use case scenario to increase awareness related to data privacy and cybersecurity. This is an issue of great importance and urgency considering the rapid increase of cyberattacks in healthcare organisations, mainly due to human errors. Further to that, based on human-centric approaches, our long-term vision and future work involves facilitating the development of efficient practices and education associated with cybersecurity hygiene via a flexible, adaptable and practical framework.

Cyber threat assessment and management for securing healthcare ecosystems using natural language processing

Stefano Silvestri, Shareful Islam, Dmitry Amelin, Gabriele Weiler, Spyridon Papastergiou & Mario Ciampi. (2023, October). Cyber threat assessment and management for securing healthcare ecosystems using natural language processing. https://doi.org/10.1007/s10207-023-00769-w

The healthcare sectors have constantly faced significant challenge due to the rapid rise of cyber threats. These threats can pose any potential risk within the system context and disrupt the critical healthcare service delivery. It is therefore necessary for the healthcare organisations to understand and tackle the threats to ensure overall security and resilience. However, threats are continuously evolved and there is large amount of unstructured security-related textual information is available. This makes the threat assessment and management task very challenging. There are a number of existing works that consider Machine Learning models for detection and prediction of cyber attack but they lack of focus on the Natural Language Processing (NLP) to extract the threat information from unstructured security-related text. To this end, this work proposes a novel method to assess and manage threats by adopting natural language processing. The proposed method has been tailored for the healthcare ecosystem and allows to identify and assess the possible threats within healthcare information infrastructure so that appropriate control and mitigation actions can be taken into consideration to tackle the threat. In detail, NLP techniques are used to extract the useful threat information related to specific assets of the healthcare ecosystems from the largely available security-related information on Internet (e.g. cyber security news), to evaluate the level of the identified threats and to select the required mitigation actions. We have performed experiments on real healthcare ecosystems in Fraunhofer Institute for Biomedical Engineering, considering in particular three different healthcare scenarios, namely implantable medical devices, wearables, and biobank, with the purpose of demonstrating the feasibility of our approach, which is able to provide a realistic manner to identify and assess the threats, evaluate the threat level and suggest the required mitigation actions.

A Swarm-Based Clinical Validation Framework of Artificial Intelligence Solutions for Non-Communicable Diseases

Kitty Kioskli, Spyridon Papastergiou, Theofanis Fotis. (2023, October). A Swarm-Based Clinical Validation Framework of Artificial Intelligence Solutions for Non-Communicable Diseases. 10.55708/js0209001

Non-communicable diseases (NCDs) present complex challenges in patient care. Artificial Intelligence (AI) offers transformative potential, but its implementation requires addressing key issues. This study proposes a swarm intelligence-inspired clinical validation framework for NCDs, promoting openness, trustworthiness, and continuous self-validation. The framework creates a collaborative environment, connecting healthcare entities, patients, caregivers, and professionals. The swarm-based approach enhances diagnostic accuracy, enables personalized treatment, improves prognosis, supports clinical decision-making, engages patients, enables real-time monitoring, and promotes continuous learning. These implications have the power to revolutionize NCD management and improve patient outcomes.

Evidence based Cybersecurity Risk Management for Enhancing Healthcare Sector Cybersecurity and Creating Common Situational Awareness ***(Under Development)***

Stefano Silvestri, Shareeful Islam, Dmitry Amelin, Gabriele Weiler, Spyridon Papastergiou, Mario Ciampi

Unveiling the Role of Forensics Visualization in Securing Exchange of Medical Information Across Connected Environments ***(Pending approval)***

Jihane Najar, Andreas Alexopoulos, Vasilis Tountopoulos, Vassilis Prevelakis

An Intrusion detection system based on state of the art ML techniques for improving security in healthcare environments ***(Under Development)***

Efthymios Chondrogiannis, Efstathios Karanastasis, Vassiliki Andronikou and Theodora Varvarigou

Enhancing Cyber Threat Hunting: A VisualApproach with the Forensic Visualization Toolkit ***(Under Development)***

Jihane Najar, Marinos Tsantekidis, Aris Sotiropoulos, and Vassilis Prevelakis

5.1.3 Publications and presentations in conferences

This section provides an accounting of the presentations related to the Ai4HealthSec project implemented in conferences attended as well as the publications in conferences. In summary, the project partners published in **12** conferences and presented in **1** conference within the reporting period. In section 7. The KPIs for the entire duration of the project are presented.

5.1.3.1 ICTS4eHealth IEEE Conference on ICT Solutions for eHealth

ISCC 2022[38], in its 27th edition, provides an insight into the unique world stemming from the interaction between the fields of computers and communications. ISCC 2022 provides an international technical forum for experts from industry and academia to exchange ideas and present results of on-going research in most state-of-the-art areas of computers and communications.

The AI4HealthSec project attended this event through different partners. Moreover, partners CNR and FORTH presented the Ai4HealthSec project and its developments.

[38] 27th IEEE Symposium on Computers and Communications (ISCC 2022) (unipi.gr)

18

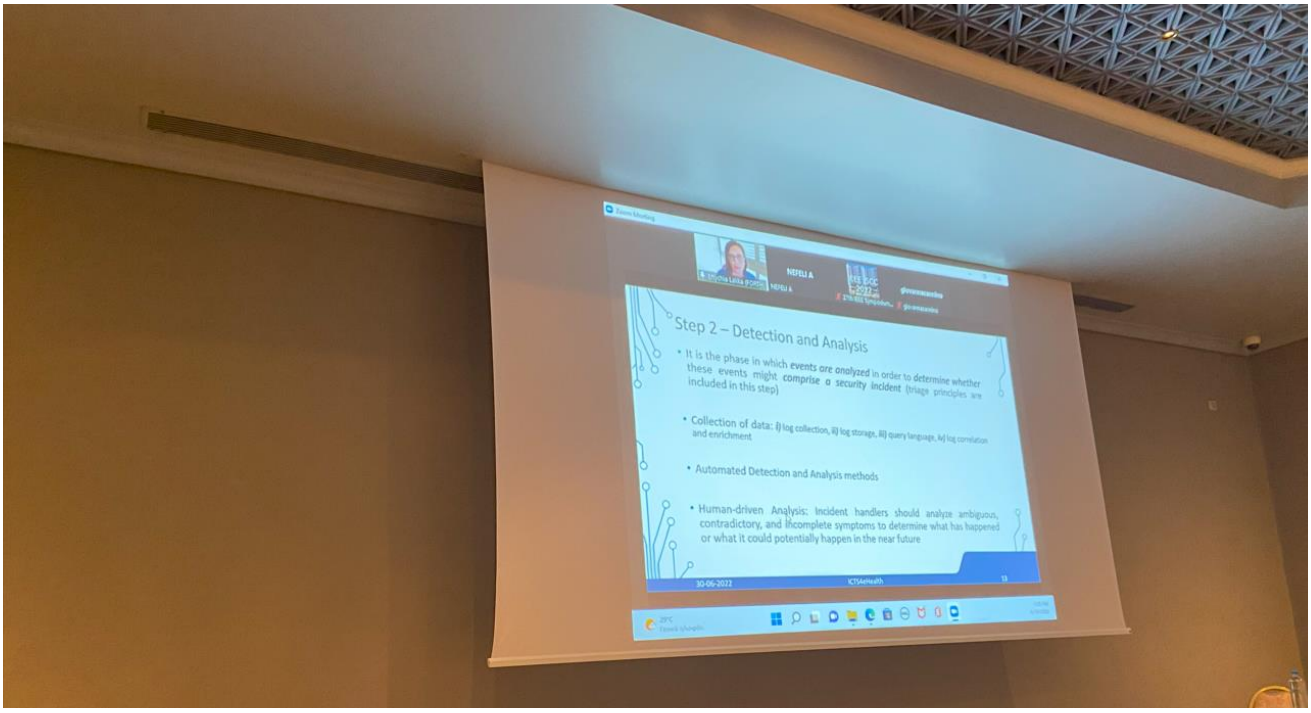
AI4HEALTHSEC Platform

H2020 EC-Funded Project

Dynamic Situational Awareness Framework (**DSAF**) that helps the operators of the HCIIs to:

- Assess the threats and vulnerabilities of all cyber assets
- Evaluate the probability of cyber-attacks
- Identify the relationships between indicators of compromise, threats, and adversaries
- Estimate the cascading effects of attacks in the **Interdependent HCIIs** and identify how these attacks propagate across the **HCSCS**
- Provide technical assistance and guidance on investigating and handling complex, interrelated cyber security incidents and data breaches and extracting all relevant information
- Combine and analyse all security incident-related information in an effective and accurate manner

Figure 5-50. **Photos from the presentation of the Ai4HealthSec project in the ISCC 2022.**



Step 2 – Detection and Analysis

- It is the phase in which **events are analyzed** in order to determine whether these events might **comprise a security incident** (triage principles are included in this step)
- Collection of data: i) log collection, ii) log storage, iii) query language, iv) log correlation and enrichment
- Automated Detection and Analysis methods
- Human-driven Analysis: Incident handlers should analyze ambiguous, contradictory, and incomplete symptoms to determine what has happened or what it could potentially happen in the near future

30-06-2022 ICTS4eHealth 13

Figure 5-51. Photos from the presentation of the Ai4HealthSec project in the ISCC 2022.

5.1.3.2 13th International Conference on Applied Human factors and Ergonomics (AHFE2022)

Estimating Attackers' Profiles Results in More Realistic Vulnerability Severity Scores

Kioskli, K., Polemi, N. (2022). Estimating Attackers' Profiles Results in More Realistic Vulnerability Severity Scores. In: Tareq Ahram and Waldemar Karwowski (eds) Human Factors in Cybersecurity. AHFE (2022) International Conference. AHFE Open Access, vol 53. AHFE International, USA.

http://doi.org/10.54941/ahfe1002211

Digitalization is moving at an increasing speed in all sectors of the economy. Along with it the cybersecurity threats and attacks continue to rise rapidly. Enterprises in all economic sectors are imposed to constantly assess the vulnerabilities (weaknesses) of their Information and Communication Systems (ICT) and further estimate their severity, to avoid exploitability by targeted cyber-attacks. Attacks may have catastrophic consequences (impacts), including the disruption or termination of operations, economic damages, long-term damaged reputation, customer loss, lawsuits, and fines. Organisations need to undertake mitigating actions and technical controls to lower the severity of the vulnerabilities and protect their ICT assets. However, security measures are expensive, especially for small companies. Cybersecurity is considered a burden to the Small-Medium Enterprises (SMEs) and not a marketing advantage, while cost is their biggest challenge. We need to be as realistic as possible in the vulnerability severity scoring, to decrease the security costs for smaller companies and simultaneously prevent potential attackers to exploit their assets. Identifying the potential attacker for each sector and company is the first step in building resilience. The classifications for attackers are usually based on whether they are internal, or by their means and capabilities, such as knowledge of the organization's resources, including personnel, facilities, information, equipment, networks, and systems. In 2021, ENISA published a sector-specific taxonomy based on opportunities, means, motives and sectors or products they wish to attack. In all existing classifications, psychological, behavioural, and social traits of the attackers are neither measured nor considered. The existing security scoring systems concentrate on technical severity, not considering the human factors with practical methods such as via the external or internal attackers' profile in their calculations. The Common Vulnerability Scoring System (CVSS) is a standard and widely adopted measure for vulnerabilities' severity. CVSS assumes that the potential attacker will be highly skilled, but it does not consider any other human factors which may be involved. Our work, in the latest years, targets to bridge psychosocial advancements, including human, behavioural, and psychosocial factors, with cybersecurity efforts to improve and reach a realistic cyber-resilient state within the information systems. The overarching objective of the present paper is to further contribute to providing realistic vulnerability severity scoring. Our main aim is to show that the CVSS scores are not unique for every vulnerability but vary depending on the potential attacker. Based on the organisations' cyber threat intelligence (CTI) level, the sectoral threats can be identified, and the profiles of their potential attackers can be predicted. In this paper, we measure the attackers' profiles and use these values in the CVSS calculator to score the vulnerabilities' severity more accurately. Considering practical implications, multiple interventions and suggestions at various levels are presented to tackle the ongoing cybersecurity internal and external threats and also enhance the CVSS to provide more realistic and accurate results.

5.1.3.3 2nd Edition of the IEEE Conference on ICT SOLUTIONS for EHEALTH

Cyber Threat Analysis Using Natural Language Processing for a Secure Healthcare System

Islam, S., Papastergiou, S., & Silvestri, S. (2022, June). Cyber Threat Analysis Using Natural Language Processing for a Secure Healthcare System. In 2022 IEEE Symposium on Computers and Communications (ISCC) (pp. 1-7). IEEE. http://doi.org/10.1109/ISCC55528.2022.9912768

Cyber threats in the healthcare sector have increased significantly in recent years. Attackers are now using sophisticated techniques to launch multi-phase cyber attacks to compromise the system and leak patient healthcare data. Healthcare organisations need to protect IT infrastructures and understand the threats and possible attack surface for a secure healthcare service delivery. Hence, threat analysis is one of the key activities for tackling the potential risks and ensuring security of a system context. This work presents a threat analysis approach that allows to identify and assess the possible threats within healthcare information infrastructure. The approach considers the existing threat data from widely used repositories and uses Natural Language Processing to identify threats among cyber security news, also evaluating their corresponding level. The preliminary experimental assessment shows promising results, providing a realistic manner to assess the threats, allowing to adopt the proposed approach in real-world contexts.

Incident Handling for Healthcare Organizations and Supply-Chains

Lakka, E., Hatzivasilis, G., Karagiannis, S., Alexopoulos, A., Athanatos, M., Ioannidis, S., … & Spanoudakis, G. (2022, June). Incident Handling for Healthcare Organizations and Supply-Chains. In 2022 IEEE Symposium on Computers and Communications (ISCC) (pp. 1-7). IEEE. http://doi.org/10.1109/ISCC55528.2022.9912965

Healthcare ecosystems form a critical type of infrastructures that provide valuable services in today societies. However, the underlying sensitive information is also of interest of malicious entities around the globe, with the attack volume being continuously increasing. Safeguarding this complex computerized setting constitutes a major challenge for the involved organizations. This paper presents an incident handling system for healthcare organizations and their supply-chain. The proposed approach utilizes swarm intelligence in order to assess the current security posture in a continuous basis and respond to attacks in real-time. The overall solution is based on the related NIST 800.61 standard and implements the operations of i) preparation, ii) detection and analysis, iii) containment, eradication, and recovery, and iv) post-incident activity. The system is developed under the EU funded project AI4HEALTHSEC and is applied in the relevant healthcare pilots.

5.1.3.4 The 2022 International Conference On Innovations In Computing Research (ICR’22)

A Conceptual Model for Data-Driven Threat Analysis for Enhancing Cyber Security

Alwaheidi, M. K., Islam, S., & Papastergiou, S. (2022, August). A Conceptual Model for Data-Driven Threat Analysis for Enhancing Cyber Security. In Proceedings of the ICR’22 International Conference on Innovations in Computing Research (pp. 365-374). Cham: Springer International Publishing. http://doi.org/10.1007/978-3-031-14054-9_34

Technology has become increasingly adopted by businesses for achieving overall objectives. Systems within these technologies generate a huge amount of data. It is necessary to identify the data and undertake appropriate controls to protect the data from any potential threats. Data, in general, is different types, such as operational and business which have different costs and impact on the overall business continuity. Threat analysis needs to consider various data types and associated weaknesses related to an organisational context’s systems and applications. There are numerous threat models available, but there is a lack of focus on analysing and prioritizing threats relating to the data. This paper presents a data-driven approach for threat analysis and a conceptual model. The model includes several concepts, i.e., actor, infrastructure, data and weakness, to analyse the data and threats from three phases management, control and business. Finally, a running example is used to demonstrate the applicability of the work.

5.1.3.5 The 12th International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH 2022)

Swarm intelligence model for securing healthcare ecosystem

Ribino, P., Ciampi, M., Islam, S., & Papastergiou, S. (2022). Swarm intelligence model for securing healthcare ecosystem. Procedia Computer Science, 210, 149-156. *http://doi.org/10.1016/j.procs.2022.10.131*

The healthcare sector is constantly facing challenges in ensuring security due to the sophisticated attacks by the threat actor for acquiring sensitive patient data. An attack on the system can pose any potential risk to the business continuity. The increased use of information technology in the modern healthcare system makes medical devices and systems more vulnerable to exploitation and possible cyber-security attacks. This paper proposes a flexible and decentralized cyber-security model based on the integration of multi-agent systems and swarm intelligence for tackling the propagation of attacks inside interconnected healthcare organizations and ensuring the whole healthcare ecosystem’s security and resilience. The proposed model is based on the collaboration between the agents with different functions and cognitive capabilities, named primary and supervisor agents. Primary agents are lightweight BDI (Belief-Desire-Intention) agents implementing a minimum set of capabilities for monitoring a specific area of the healthcare system; supervisor agents incorporate an extended version of the BDI reasoning to provide advanced capabilities for securing the overall healthcare system by enabling collective intelligence and overall cyber-security awareness. The preliminary experimental results show that the model is robust and responsive for securing the ecosystem.

5.1.3.6 14th International Conference on Ubiquitous Computing and Ambient Intelligence (UCAmI 2022)

Swarm Intelligence Based Multi-Agent Communication Model for Securing Healthcare Ecosystem

Ribino, P., Islam, S., Ciampi, M., & Papastergiou, S. (2022, November). Swarm Intelligence Based Multi-Agent Communication Model for Securing Healthcare Ecosystem. In Proceedings of the International Conference on Ubiquitous Computing & Ambient Intelligence (UCAmI 2022) (pp. 50-61). Cham: Springer International Publishing. http://doi.org/10.1007/978-3-031-21333-5_5

The healthcare ecosystem is complex by its inherent nature, which consists of a heterogeneous set of actors, entities, and sub-systems to deliver multidisciplinary and collaborative health services. The increased use of connected medical devices makes such an ecosystem more vulnerable and increases the cyber-attack surface. Traditional security methods are insufficient to deal with such a high degree of interconnected medical and IoT devices. There is a need for security approaches based on concepts of collaboration, cooperation, autonomy and dynamism to ensure timely security of the whole healthcare ecosystem. This work adopts swarm-based principles with multi-agent systems to meet collaboration, distribution and robustness requirements, thus improving the healthcare ecosystem's security. The paper presents a swarm-based agent-to-agent communication model founded on the collaboration among primary and supervisor agents to acquire new knowledge related to the healthcare ecosystem. The proposed model is based on the direct collaboration between primary agents that provides supervisor agents with local security-related information and the indirect collaboration between supervisor agents that exchange stigmergic information through the environment to make a collectively informed decision. The communication model is implemented using the BDI (Belief-Desire-Intention) approach. The preliminary results show the communication model's robustness, scalability and responsiveness for securing the healthcare ecosystem.

5.1.3.7 14th International Conference on Applied Human factors and Ergonomics (AHFE2023)

Bringing humans at the core of cybersecurity: challenges and future research directions

Kioskli, K., Mouratidis, H., Polemi, N. (2023). Bringing humans at the core of cybersecurity: Challenges and future research directions. In: Abbas Moallem (eds) Human Factors in Cybersecurity. AHFE (2023)

International Conference. AHFE Open Access, vol 91. AHFE International, USA. http://doi.org/10.54941/ahfe1003722

The prompt response to successfully adopt good cybersecurity practices from protecting passwords to security incidents' responding to activating a disaster recovery or a business continuity plan depends upon the level of operators' ability in problem solving, resilience, readiness, maturity, observation, and perception. New technologies, such as Artificial Intelligence (AI) can also be helpful to more effectively forecast or respond to serious incidents, especially to massive attacks. However, the cybersecurity operators need to alter their mindsets, adopt new behavioural patterns, and work attitudes to embrace and interact with AI-assistance during cyber defence activities. in addition, when the operators need to assess or mitigate AI socio-technical risks related to bias, transparency and equality, they will base their decisions for estimating or mitigating these risks on their behavioural, social, cultural, and ethical characteristics. In this paper, we are presenting challenges related to human and psychosocial factors of the cybersecurity operators. We also discuss the motives and drivers that impact the cognitive aspects (e.g., focus on operational tasks, attention, objectivity) of the cyber operations. We further identify how the cybersecurity operators' personality traits impact the success of the cybersecurity practices and estimations and analyse research challenges, regarding the impact of operators' profiles on their perceptions and interactions, with AI cyber defending tools and management of AI risks. Finally, we consider the impact these human factors may have on successful cybersecurity operations and practices and provide proposals for interdisciplinary research directions requiring the collaboration of cybersecurity experts, psychologists, and behavioural scientists.

Enhancing practical cybersecurity skills: The ECSF and the CyberSecPro European efforts

Polemi, N., Kioskli, K. (2023). Enhancing practical cybersecurity skills: The ECSF and the CyberSecPro European efforts. In: Abbas Moallem (eds) Human Factors in Cybersecurity. AHFE (2023) International Conference. AHFE Open Access, vol 91. AHFE International, USA.
http://doi.org/10.54941/ahfe1003723

The accelerated digitalization of all business and industrial sectors (transport, government, health, finance manufacturing) will increase the number, complexity and scale of cybersecurity incidents and their impact on the economy and society. The digital transformation imposes Higher Education Institutions and training providers to enhance their role in preparing the new generation of workforce that will have the capabilities and skills to address the upcoming digital challenges. Training providers need to become the enablers of the digital transformation with the capacity to accommodate different skills needed by the market, to a variety of training specializations. Fostering collaboration with the private sector can be effective in attracting the necessary funding, state-of-the-art technological training tools needed and real-life based training material. In this paper, we describe two recent efforts coming from the European Union targeting to close the gap between the available cybersecurity training and cybersecurity marketing demands, and further analyse the human factors involved in these efforts.

5.1.3.8 19th International Conference on the Design of Reliable Communication Networks (DRCN2023)

A Swarm Artificial Intelligence Approach for Effective Treatment of Chronic Conditions

K. Kioskli and S. Papastergiou, "A Swarm Artificial Intelligence Approach for Effective Treatment of Chronic Conditions," 2023 19th International Conference on the Design of Reliable Communication Networks (DRCN), Vilanova i la Geltru, Spain, 2023, pp. 1-5, doi: 10.1109/DRCN57075.2023.10108128.

Long-term conditions or chronic diseases are multifaceted and challenging. Current treatment options, for patients with long-term conditions, are mainly pharmacological, causing numerous adverse drug events and pressing for alternative management strategies such as personalized interventions. Areas of machine learning, such as deep learning, would enable researchers to develop predictive modelling algorithms, using continuous monitoring and allowing assessing the medical risk for long-term conditions and their related complications. In this paper, we claim that harmonization of data, novel machine learning algorithms, swarm-based technologies, and the involvement of the entire healthcare community will lead to acceptable and effective personalized healthcare. Our proposed approach aims to amplify the intelligence of the healthcare community. Based upon the patients' characteristics empowers better decisions, personalised medical risk prediction and recommendations of acceptable and effective interventions. Our future work includes the validation of the SwarmAI framework by actively engaging relevant stakeholders.

Information Sharing for Creating Awareness for Securing Healthcare Ecosystem

S. Islam, C. Grigoriadis and S. Papastergiou, "Information Sharing for Creating Awareness for Securing Healthcare Ecosystem," 2023 19th International Conference on the Design of Reliable Communication Networks (DRCN), Vilanova i la Geltru, Spain, 2023, pp. 1-5, doi: 10.1109/DRCN57075.2023.10108266

The increased usage of information technology makes the healthcare ecosystem more vulnerable to the activities of hackers and other perpetrators of cyber-related crime. Information sharing is an essential for creating awareness and increasing collaborative response capabilities for overall security improvements. Such sharing capabilities can significantly contribute to the healthcare sector in the aspect of raising awareness towards current threats and risks for, with the purpose of performing informed decision making. This paper proposes a flexible approach to share risk related information among the healthcare entities. Our approach includes a business process model and cyber attack forecasting system in order to present information sharing among different entities of the healthcare system. To achieve this we adopt STIX as a standard protocol to map the business processes and services of the healthcare organisations with risk related information including vulnerability, threat and control information. Finally, a demonstrator is added to present the information sharing and applicability of the work.

5.1.3.9 The 2023 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining

Russo-Ukrainian War: Prediction and explanation of Twitter suspension

Alexander Shevtsov, Despoina Antonakaki, Ioannis Lamprou, Ioannis Kontogiorgakis, Polyvios Pratikakis, Sotiris Ioannidis. (2023, June). Russo-Ukrainian War: Prediction and explanation of Twitter suspension. https://arxiv.org/abs/2306.03502

On 24 February 2022, Russia invaded Ukraine, starting what is now known as the Russo-Ukrainian War, initiating an online discourse on social media. Twitter as one of the most popular SNs, with an open and democratic character, enables a transparent discussion among its large user base. Unfortunately, this often leads to Twitter's policy violations, propaganda, abusive actions, civil integrity violation, and consequently to user accounts' suspension and deletion. This study focuses on the Twitter suspension mechanism and the analysis of shared content and features of the user accounts that may lead to this. Toward this goal, we have obtained a dataset containing 107.7M tweets, originating from 9.8 million users, using Twitter API. We extract the categories of shared content of the suspended accounts and explain their characteristics, through the extraction of text embeddings in junction with cosine similarity clustering. Our results reveal scam campaigns taking advantage of trending topics regarding the Russia-Ukrainian conflict for Bitcoin and Ethereum fraud, spam, and advertisement campaigns. Additionally, we apply a machine learning methodology including a SHapley Additive explainability model to understand and explain how user accounts get suspended.

5.1.3.10 2023 IEEE Symposium on Computers and Communications (ISCC)

Pump Up the JARM: Studying the Evolution of Botnets Using Active TLS Fingerprinting

Eva Papadogiannaki, Sotiris Ioannidis. (2023, July). Pump Up the JARM: Studying the Evolution of Botnets Using Active TLS Fingerprinting. In Proceedings of the 2023 IEEE Symposium on Computers and Communications (ISCC 2023). http://doi.org/10.1109/ISCC58397.2023.10218210

The growing adoption of network encryption protocols, like TLS, has altered the scene of monitoring network traffic. With the advent increase in network encryption, typical DPI systems that monitor network packet payload contents are becoming obsolete, while in the meantime, adversaries abuse the utilization of the TLS protocol to bypass them. In this paper, aiming to understand the botnet ecosystem in the wild, we contact IP addresses known to participate in malicious activities using the JARM tool for active probing. Based on packets acquired from TLS handshakes, server fingerprints are constructed during a time period of 7 months. We investigate if it is feasible to detect suspicious servers and re-identify other similar within blocklists with no prior knowledge of their activities. We show that it is important to update fingerprints often or follow a more effective fingerprinting approach, since the overlapping ratio with legitimate servers rises over time.

5.1.4 Press Releases

Various partners of the Ai4HealthSec project, created, published and communicated information about their participation in the project or the extraction of related results.

Due to the number of the press releases, in this section, an indicative number of links to these press releases are presented. It should be also noted that there is an allocated space within the webpage of the Ai4HealthSec project which contains also articles and other documents (i.e., the position paper – see section 5.1.5.) by the project partners.

https://www.essex.ac.uk/research-projects/ai4healthsec
https://aegisresearch.eu/research/projects/ai4healthsec/
https://www.ahci.icar.cnr.it/ai4healthsec/
https://www.privanova.com/eu-projects/ai4healthsec
https://www.icar.cnr.it/en/progetti/ai4healthsec/
https://research.brighton.ac.uk/en/projects/a-dynamic-and-self-organized-artificial-swarm-intelligence-soluti
https://www.privanova.com/resources/ai4healthsec-ensuring-privacy-in-healthcare-ict-infrastructure
https://aegisresearch.eu/ai4healthsec-kickoff-news/
https://www.ibmt.fraunhofer.de/en/ibmt-press-releases/presse-ibmt-AI4HealthSec-10072023.html
http://grid.ece.ntua.gr/dkmgsite/index.php/category/news/
https://www.sphynx.ch/randd/
https://focalpoint-sprl.be/research-and-innovation/
https://uniparthenope.it/Portale-Ateneo/articolo/Innovative_Cybersecurity_solutiof23db5827ade4e95aeb233fecf7aeca6

5.1.5 Position Paper

In March 2022 the European Commission published a proposal for a regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union.

The Council subsequently, in November 2022, adopted its position on a draft regulation aimed at ensuring a high common level of cybersecurity across the EU institutions, bodies, offices and agencies, In June 2023, a political agreement was reached between the European Parliament and the Council of the EU on the Regulation proposed by the Commission.

Once the text is finalised, the European Parliament and the Council will have to formally adopt the new Regulation before it can enter into force. Union entities will then be required to comply with the obligations and meet the deadlines specified in the text.

A Position Paper[39] of the AI4HealthSec and HEIR projects was created, published and communicated on the Regulation of the European Parliament and of the Council laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union.

This document provides comments from the AI4HEALTHSEC and HEIR projects and their partners with regards to the importance of the proposal, the feasibility of the envisioned measures and possible improvement points.

The AI4HEALTHSEC and HEIR projects and their partners welcome this initiative, as it addresses crucial subjects of the protection of the information and abilities of institutions, bodies, offices and agencies of the Union.

The AI4HEALTHSEC and HEIR projects and their partners especially, welcome the introduction of the cybersecurity risk management, governance and control framework ('the framework') in support of each entity's mission and exercising its institutional autonomy.

It is a belief shared also by the AI4HEALTHSEC and HEIR projects that Risk Management should be at the core of any design and implementation of a system and measures to achieve the information security objectives of an organization.

The new processes that will consider big data must ensure full compliance with the underlying data protection EU regulations, have a clear legal basis, be proportionate and ensure accountability for those processing them. As such, synergies when data is been managed within the context of cybersecurity and personal data protection are necessary so that citizens' rights to the protection of personal data and privacy do not slip and ensuring that mechanisms to be imposed must be clear, traceable, homogeneous, transparent, effective and correctly complement the existing legislation on personal data protection.

Finally, although each entity may implement the controls, mechanisms and processes mentioned above, it is of paramount importance that incident response should be structured, planned and well supported.

[39] https://www.ai4healthsec.eu/wp-content/uploads/Position-Paper_Reg_EU_institutions.pdf

6 Monitoring of objectives and related KPIs

Based on the project call and as stated in the GA, the following objectives have been set:

- **Objective 1:** Conceptualize and establish a self-organized Swarm Intelligence (SI) model.
- **Objective 2:** Provide distributed data management and reasoning capabilities for threats, risks and vulnerabilities identification.
- **Objective 3:** Develop an advanced cyber incident handling approach for the health care ecosystem.
- **Objective 4:** Develop a novel Dynamic Situational Awareness Approach (AI4HEALTHSEC framework) for HCIIs.
- **Objective 5:** To develop the AI4HEALTHSEC system based on the AI4HEALTHSEC framework.
- **Objective 6:** To deploy and validate the AI4HEALTHSEC Framework and System in real operational environments.
- **Objective 7:** To disseminate knowledge developed during the project to different areas of the health care ecosystem and transfer knowledge to other critical sectors.

For each of these objectives, specific measures of success (KPIs) have been identified and monitored by the project team.

Additionally, some more specific KPIs regarding the dissemination and communication activities of the project have been set and are shown in the following table (it should be noted that goals of these KPIs relate to the entire duration of the project).

KPI:	**The % of tasks, etc. completed on time according to the action plan.**
KPI Goal:	>=95%
Performance:	100%
Status:	Achieved
Comments:	All tasks have been completed on time according to the revised action plan. 92% of the deliverables were submitted on time and 8% were submitted with one day delay.

KPI:	**The existence of a well-established and functioning community.**
KPI Goal:	>= 10 members (at least)
Performance:	27
Status:	Achieved
Comments:	The project has created a community of organizations through the cooperation with other projects, the pilot operations, the operation of the open call and the existence of the project partners. If all these organizations are taken into account, the community is comprised at least of 27 entities.

KPI:	**Number of periodic meetings.**
KPI Goal:	>=6
Performance:	11
Status:	Achieved

Comments:	Many meetings have taken place at different levels within the project. For his KPI only the PSC meetings are reported (11).

KPI:	**Number of workshops.**
KPI Goal:	>=3
Performance:	6
Status:	**Achieved**
Comments:	The project has participated in 6 workshops (4 from this reporting period and 2 from the previous). Moreover, as part of the WP7 activities, workshops have been carried out with internal and external stakeholders for the validation of the Ai4healthSec solution.

KPI:	**Number of contributions to roadmaps, discussion papers.**
KPI Goal:	>= 2
Performance:	5
Status:	**Achieved**
Comments:	Ai4HealthSec has: provided a contribution to the chapter Standardization and Certification of the Cybersecurity Roadmap for Europe by CONCORDIA, produced a position paper on the measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union, created a discussion paper on Standards and NIS compliance, provided feedback on the European Cyber Resilience Act during the open consultation procedure (May 2022) and provided feedback on the EU CSA during the open consultation procedure (July 2023). More information can be found in deliverable 7.11

KPI:	**Number of contributions to policy makers.**
KPI Goal:	>= 2
Performance:	4
Status:	**Achieved**
Comments:	Ai4HealthSec has: produced a position paper on the measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union, created a discussion paper on Standards and NIS compliance, provided feedback on the European Cyber Resilience Act during the open consultation procedure (May 2022) and provided feedback on the EU CSA during the open consultation procedure (July 2023). More information can be found in deliverable 7.11.

KPI:	**Number of external workshops, seminars, etc. attended.**
KPI Goal:	>= 10
Performance:	29
Status:	**Achieved**
Comments:	The project partners have participated in workshops, webinars, conferences, summer schools, informational days and other types of events. This participation is depicted in the various sections of this document. Specifically, for this reporting period, the project partners participated in 8 events, 4 workshops and 10 conferences. For the first reporting period, the number for this KPI was 7, bringing the total to 28.

KPI:	**Number of press releases issued.**
KPI Goal:	>= 4
Performance:	13
Status:	**Achieved**

Comments:	Various partners of the Ai4HealthSec project, created, published and communicated information about their participation in the project or the extraction of related results. Section 5.1.4. of this document provides links to an indicative number of press releases of the project partners. It should be also noted that there is an allocated space within the webpage of the Ai4HealthSec project which contains also articles and other documents (i.e., the position paper – see section 5.1.5.) by the project partners.

KPI:	**Number of registered members of the project's website.**
KPI Goal:	>= 60
Performance:	75
Status:	**Achieved**
Comments:	The project website does not have a user functionality. The measurement here reflects the number of people subscribed to the project newsletter.

KPI:	**Number of journal publications.**
KPI Goal:	>= 8
Performance:	15
Status:	**Achieved**
Comments:	12 journal publications have been issued within the second reporting period and 3 in the first reporting period.

KPI:	**Number of conference papers and presentations.**
KPI Goal:	>= 10
Performance:	14
Status:	**Achieved**
Comments:	The project partners presented in 3 conferences and produced 14 conference papers during the project duration.

17

KPI:	**Number of events attended.**
KPI Goal:	>= 15
Performance:	23
Status:	**Achieved**
Comments:	The project partners have participated in various events, summer schools, etc. The number reported results from the aggregation of the various types of events.

7 References

[1] D8.1 – Dissemination and Communication Plan, Date of deliverable: 31.03.2021 https://www.AI4HEALTHSEC.eu/wp-content/uploads/deliverables/AI4HEALTHSEC-D8.1-v1.0.pdf