



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"

D8.2– Report on Dissemination and Communication Activities version 1

Due date of deliverable: 31.05.2022

Actual submission date: 31.05.2022

Grant agreement number: 883273

Start date of project: 01/10/2020

Revision 1

Lead contractor: CNR

Duration: 36 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	

D8.2 – Report on Dissemination and Communication Activities version 1

Editor

Argyro Chatzopoulou (TUV)

Contributors

Karras Apostolos (TUV)
Stylianos Karagiannis (PDMFC)
Djordje Djokic (PN)
Dmitry Amelin (FHG-IBMT)
Georgios Chatzivasilis (STS)
Jihane Najar (AEGIS)
Thaise M Quiterio, Anca Bucur (PHILIPS)
Mario Ciampi, Stefano Silvestri (CNR)
Shareeful Islam (FP)
Efsthios Karanastasis (ICCS)
Eftychia Lakka (FORTH)
Kitty Kioskli (UOE)
Haris Mouratidis (UOE)
Lena Griebel (KLINIK)

Reviewers

Eftychia Lakka (FORTH)
Thaise M Quiterio (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	23.03.2022	Argyro Chatzopoulou	Initial Draft Version
0.2	02.05.2022	Argyro Chatzopoulou	Comments by project partners
0.3	18.05.2022	Argyro Chatzopoulou	Updated version until 18.05.2022
0.4	24.05.2022	Thaise M Quiterio	Review
0.5	25.05.2022	Eftychia Lakka	Review
1.0	27.05.2022	Argyro Chatzopoulou	1 st 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 first report on the communication and dissemination of the AI4HEALTHSEC project results to the general public, other organizations and 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 during the first 18 months 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 is the first report that provides an overview of all propagation efforts of the AI4HEALTHSEC project through traditional communication channels such as event attendance (conferences, workshops, etc.), project publications (brochures, 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.

Contents

Executive Summary	4
List of acronyms	6
List of tables	7
List of figures	8
1 Introduction	9
2 Dissemination and Communication activities	10
2.1 Dissemination and Communication Plan (D8.1)[1]	10
2.2 Dissemination and Communication planning for the 2 nd year	10
2.3 Traditional communication channels	13
2.3.1 Events	13
2.3.2 Conferences	14
2.3.3 Workshops	20
2.3.4 Collaboration with other projects	25
2.4 Project publications	29
2.4.1 Brochures	29
2.4.2 Publications in professional journals & Conferences	31
2.5 Social Media	34
2.5.1 Facebook	35
2.5.2 LinkedIn	39
2.5.3 Twitter	42
2.6 Website	43
2.7 Newsletters	45
2.8 Monitoring of objectives and related KPIs	49
3 References.....	51

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

TABLE 2-1. DISSEMINATION AND COMMUNICATION PLAN – 2ND YEAR OF THE PROJECT	12
TABLE 2-2. FACEBOOK STATISTICS	38
TABLE 2-3. LINKEDIN STATISTICS.....	41
TABLE 2-4. TWITTER STATISTICS	43
TABLE 2-5. KPIS UP TO M20 (LAST UPDATED ON 18.05.2022).....	50

List of figures

FIGURE 2-1. AN OVERVIEW OF THE TOOLS, MEANS AND AUDIENCE OF THE DISSEMINATION PLAN OF AI4HEALTHSEC PROJECT	11
FIGURE 2-2. PHOTOS FROM THE POSTER PRESENTATION OF THE AI4HEALTHSEC PROJECT AS PART OF THE CYBERHOT SUMMER SCHOOL	14
FIGURE 2-3. EXTRACT FROM THE AGENDA AND TIMELINE OF THE NMOTC 5TH CYBER SECURITY CONFERENCE.....	15
FIGURE 2-4. EXTRACT FROM THE 25TH PAN-HELLENIC CONFERENCE PROGRAM	16
FIGURE 2-5. EXTRACT FROM THE E-POSTERS OUTLINE OF THE 32ND ANNUAL CONGRESS OF THE HELLENIC SOCIETY OF HAEMATOLOGY	17
FIGURE 2-6. AI4HEALTHSEC / DEFEND STAND VISUAL	18
FIGURE 2-7. ANNOUNCEMENT OF THE CANCELLATION OF THE SRE 2022	18
FIGURE 2-8: SEVERAL CYBERCRIME-RELATED EU-FUNDED PROJECTS PRESENTED AT THE UNITED NATIONS	20
FIGURE 2-9. EXTRACT FROM THE AGENDA OF THE 2ND JOINT WORKSHOP - DYNAMIC COUNTERING OF CYBER-ATTACKS.....	21
FIGURE 2-10. SCREENSHOTS FROM THE PRESENTATIONS DURING THE CONCORDIA EHEALTH WORKSHOP	24
FIGURE 2-11. EXTRACT OF THE AGENDA OF THE 2 ND ECSCI WORKSHOP.....	25
FIGURE 2-12. SCREENSHOTS FROM THE PRESENTATION DURING THE 2 ND ECSCI WORKSHOP.....	25
FIGURE 2-13. ARES – IOSEC 2022 WORKSHOP.....	28
FIGURE 2-14. SCREENSHOTS FROM THE AI4HEALTHSEC – HEIR WORKSHOP	29
FIGURE 2-15. SCREENSHOT FROM AI4HEALTHSEC POSTERS.....	30
FIGURE 2-16. SCREENSHOTS FROM AI4HEALTHSEC BROCHURE	31
FIGURE 2-17. FACEBOOK GENERAL RESULTS.....	36
FIGURE 2-18. FACEBOOK HOME PAGE	37
FIGURE 2-19. FACEBOOK POSTS.....	38
FIGURE 2-20. LINKEDIN “COMPANY” HOME PAGE.....	40
FIGURE 2-21. LINKEDIN POSTS	41
FIGURE 2-22. TWITTER ACCOUNT HOME PAGE.....	42
FIGURE 2-23. TWITTER POSTS	43
FIGURE 2-24. THE AI4HEALTHSEC WEBSITE.....	44
FIGURE 2-25. EXTRACT FROM THE WEBSITE (HTTPS://WWW.AI4HEALTHSEC.EU/NEWSLETTERS/)	45
FIGURE 2-26. SCREENSHOT OF THE 1 ST PROJECT NEWSLETTER.....	46
FIGURE 2-27. SCREENSHOT OF THE 2 ND PROJECT NEWSLETTER	47
FIGURE 2-28. SCREENSHOT OF THE 3 RD PROJECT NEWSLETTER	48

1 Introduction

The purpose of this report is to present the main efforts performed by the consortium partners during the first 20 [Note] months of the project for the communication and dissemination of the AI4HEALTHSEC project to the general public.

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, web articles). In both cases, partners of the AI4HEALTHSEC consortium are actively involved. The deliverable is based on the deliverable Dissemination and Communication Plan (D8.1), 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. The deliverable D8.2 complements the information on the D8.1 and it is part of task T8.1. of WP8.

[Note] It should be noted that the information contained within this document covers the activities implemented until the 18th of May 2022 and not the entire month (M20). This was done to facilitate the internal review process. The remaining and future activities will be described in the deliverable Report on Dissemination and Communication Activities version 2 (D8.3) on M36.

2 Dissemination and Communication activities

Within this section, it is presented the planning, implementation and results of activities regarding dissemination and communication of the project. In the subsection 2.1, it is described an overview of the deliverable D8.1, Dissemination and Communication Plan, issued on M6 of the project, as the first initiative to share the project overview with the general public, during the first six months. After the completion of the first efforts reported, 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 subsection 2.2.

The overview and results of the dissemination and communication activities through various traditional (Events, Conferences, Workshops, Collaboration with other projects, Brochures, Publications in professional journals and Conferences) and non-traditional (social media, Website, Newsletters) communication channels is provided in the subsections 2.3. – 2.7.

2.1 *Dissemination and Communication Plan (D8.1)[1]*

The report D8.1 presents the description of the initial proposal and endeavours about how to spread the AI4HEALTHSEC outcomes to the external public. The purpose of this deliverable is to present the general Communication and Dissemination strategy that guides the development of activities envisaged for the whole project, to maximize the impact of the project on the target audiences (e.g. Market Stakeholders, research community, EU projects, etc), and to present the KPIs defined for the project which will allow to monitor and evaluate the success of the work performed in T8.1.

This document contains information on:

- The objectives to be fulfilled by the project and in particular by the dissemination and communication activities;
- The dissemination and communication strategy for the entire three-year duration of the project, at a high level;
- The dissemination and communication activities of the first year at a more detailed level.
- The different channels and means of communication and dissemination to be used by the AI4HEALTHSEC project;
- Details about the decisions that have been taken regarding the components of the AI4HEALTHSEC “brand” (e.g. Logo, colors, fonts, etc.);
- The KPIs that will be used for the monitoring, measurement, analysis and evaluation of the performance of Task 8.1 against the set objectives.

2.2 *Dissemination and Communication planning for the 2nd year*

The consortium continued to refine the planning described in the subsection 2.1, based on investigations, initial actions implemented, and feedback from the reviewers. **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 is more focused in the strength the awareness of the project existence to the general public. For the second year, the activities are toward the communication of the project initiatives and outcomes. In

the third, the consortium will focus in the dissemination of the implementation outcomes, demonstrators and publications.

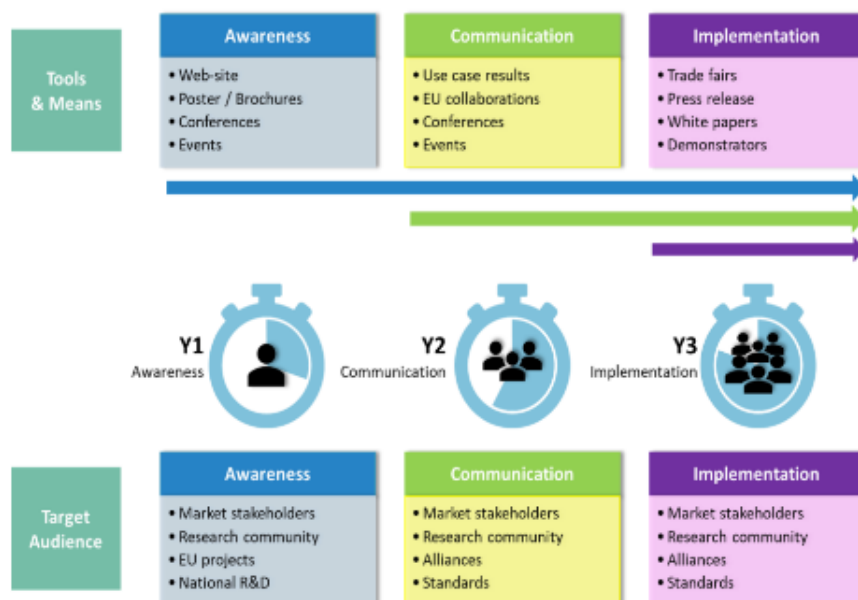


Figure 2-1. An overview of the Tools, means and audience of the dissemination plan of AI4HEALTHSEC project

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

In this planning the comments and recommendations of the reviewers during the first Technical Review were taken into consideration. The details on the issues raised during the first Technical Review, have already been reported in detail within D1.4, Periodic activity report version 2, submitted on M18.

Objective		Methods
Communication Year 2	<ul style="list-style-type: none"> • Communication of on-going progress, results and key achievements • Increase the reach of the project (collaborations, networking, etc.) • Special focus on digital security, health technology and ICT industry and target potential users 	<ul style="list-style-type: none"> • Elaboration of a business whitepaper / videos 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 second year. • Organization of a workshop within a scientific event. • Publication of at least two articles related to the subject of the project. • Publication of the results in the website and the social media of the project and that of the project partners. • Establishment of liaison with interested parties (e.g. authorities, special interest groups, SDO's etc.).

Table 2-1. Dissemination and Communication Plan – 2nd 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.
- Conduct a workshop to increase the awareness on the project to various stakeholders.

The following sections provide an overview of the results of the Communication and Dissemination activities until month 20 [Note] It should be noted that the information contained in all sections (with the exception of social media) refers to outcomes produced from the entire duration of the project so far.

[Note] It should be noted that the information contained within this document covers the activities implemented until the 18th of May 2022 and not the entire month (M20). This was done to facilitate the internal review process. The remaining and future activities will be described in the deliverable Report on Dissemination and Communication Activities version 2 (D8.3) on M36.

2.3 Traditional communication channels

2.3.1 Events

AI4HEALTHSEC participation in the CyberHOT Summer School

AI4HEALTHSEC was very proud to support and participate in the CyberHOT Summer School¹. The Cybersecurity Hands-On Training (CyberHOT) Summer School took place on Monday 27th and Tuesday 28th of September 2021 under the auspices of NMIOTC².

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

- Threat and Attack Monitoring;
- Risk Assessment;
- Security Management;
- Technical Vulnerability Assessments;
- Digital Forensics.

The partners FORTH and FP participated in the CyberHOT Summer School and a poster depicting the main information of the project was presented, as illustrated on **Figure 2-2**.

¹ <https://sites.google.com/cyberhot.eu/cyberhot2021/home>

² <https://nmiotc.nato.int/wp-content/uploads/2021/09/NMIOTC-5th-Cyber-Security-Conference-Agenda-28-Sep-21.pdf>



Figure 2-2. Photos from the poster presentation of the AI4HEALTHSEC project as part of the CyberHOT Summer School

2.3.2 Conferences

International Conference on Availability, Reliability and Security (ARES)

The International Conference on Availability, Reliability and Security (ARES)³ brings together researchers and practitioners in the field of IT security & privacy. Since 2005, ARES serves as an important platform to exchange, discuss and transfer knowledge and is hosted every year in another European city. The conference was held on line between August 17 to August 20, 2021.

As representative of the AI4HEALTHSEC project, Ms. Kitty Kioskli, from University of Brighton (UoB), presented some of the outcomes of the work carried out in collaboration with Theo Fotis and Haralambos Mouratidis (University of Brighton, Centre for Secure, Intelligent and Usable Systems (CSIUS), and Gruppo Maggioli, Research and Development Lab) on the subject of **“The landscape of cybersecurity vulnerabilities and challenges in healthcare: Security standards and paradigm shift recommendations”**.

³ <https://2021.ares-conference.eu/>

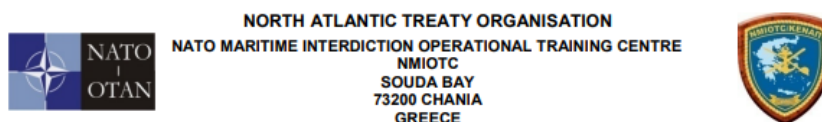
The presentation is available on YouTube in **ARES & CD-MAKE Conference** channel⁴ and has been uploaded also in project's website ([Presentation on Security standards and paradigm shift recommendations – AI4HEALTHSEC](#)).

NMIOTC 5th CYBER SECURITY Conference

The aim of the 5th NMIOTC Cyber Security Conference⁵ was to promote collaborative scientific, industrial, naval, maritime, and academic inter-workings among a wide variety of stakeholders regarding Cyber Security and Cyber Defense Operations in the maritime domain, in order to tackle Cyber Security issues in a holistic, comprehensive, and effective way and also increase awareness and expand the individual perception of the maritime community.

The Conference took place in Souda Bay, Chania, Greece on the 29th and 30th of September 2021.

As part of the proceedings of the second day of the conference, the AI4HEALTHSEC project and its current developments were presented by Ms. Eleni Maria Kalogeraki PhDc and Dr. Spyridon Papastergiou of the partner Focal Point.



NMIOTC 5th CYBER SECURITY CONFERENCE AGENDA AND TIMELINE **(Last Updated 28-09-2021)**

1110-1220	SESSION 5: Secure Maritime Value and Supply Chains, Infrastructures & Services	
	AI4HEALTHSEC - A Dynamic and Self-Organized Artificial Swarm Intelligence Solution for Security and Privacy Threats in Healthcare ICT Infrastructures	Eleni Maria Kalogeraki PhDc, Focal Point Dr. Spyridon Papastergiou Focal Point

Figure 2-3. Extract from the Agenda and Timeline of the NMIOTC 5th Cyber Security Conference

⁴ https://www.youtube.com/watch?v=mQenUFGTd_A%20

⁵ <https://nmiotc.nato.int/wp-content/uploads/2021/09/NMIOTC-5th-Cyber-Security-Conference-Agenda-28-Sep-21.pdf>

25th Pan-Hellenic Conference on Informatics (PCI2021)

The Greek Computer Society (GCS/ΕΠΥ), the University of Thessaly (UTH), the Hellenic Open University (HOU) and the University of West Attica (UniWA) organize the 25th Pan-Hellenic Conference on Informatics (PCI 2021) in Volos, Greece, from 26 to 28 November, 2021⁶.

PCI 2021 was a hybrid conference. The ability to present a paper and/or attend the conference both physically and remotely was provided. The conference took place at the new building of the Department of Electrical and Computer Engineering of the University of Thessaly, Sekeri & Cheiden st., Pedion Areos, 383 34, Volos, Greece.

The AI4HEALTHSEC project was represented by the partners FP and UoB who participated with a presentation entitled “A Dynamic Cyber Security Situational Awareness Framework for Healthcare ICT Infrastructures”.



Saturday Nov. 27th, 2021	
Eastern European Time	
11:50 – 14:00	<div>ROOM A</div> <p>SESSION 5A (Special Session) Cyber Security of Critical Infrastructures (part 2)</p> <ul style="list-style-type: none"> • Vasileios Dimitriadis, Leandros Maglaras, Nineta Polemi, Ioanna Kantzavelou and Nick Ayres. <i>Uncuffed: A Blockchain-based Secure Messaging System</i> • Konstantinos Charmanas, Nikolaos Mittas and Lefteris Angelis. <i>Predicting the existence of exploitation concepts linked to software vulnerabilities using text mining</i> • Stylianos Karagiannis, Alexandros Tokatlis, Sotiris Pelekis, Michael Kontoulis, George Doukas, Christos Ntanos and Emmanouil Magkos. <i>A-DEMO: ATT&CK Documentation, Emulation and Mitigation Operations</i> • Céilia Martinie, Christos Grigoriadis, Eleni-Maria Kalogeraki and Panayiotis Kotzanikolaou. <i>Modelling Human Tasks to Enhance Threat Identification in Critical Maritime Systems</i> • Shareeful Islam, Spyridon Papastergiou and Haralambos Mouratidis. <i>A Dynamic Cyber Security Situational Awareness Framework for Healthcare ICT Infrastructures</i>
	<div>ROOM B</div> <p>SESSION 5B (Special Session) Quantum Computing: Current state and future trends</p> <ul style="list-style-type: none"> • Sergey Gushanskiy, Viktor Potapov and Alexey Samoylov. <i>Research of Quantum Neural Networks and Development of a Single-qubit Model of Neuron</i> • Valery Pukhovskiy, Sergey Gushanskiy and Viktor Potapov. <i>Developing a Hardware Approach to Simulating Quantum Computing Using an Optimization Algorithm</i> • Maria Sabani, Ilias Galanis, Ilias Savvas and Georgia Garani. <i>Implementation of Shor's Algorithm and Some Reliability Issues of Quantum Computing Devices</i> • Maria Avramouli, Ilias Savvas, Georgia Garani and Anna Vasilaki. <i>Quantum Machine Learning: Current State and Challenges</i> • Dimitrios Ntalaperas, Konstantinos Prousalis and Nikos Konofaos. <i>A model for encoding multiple logical qubit states into the energy eigenstates of a transmon system</i>

Figure 2-4. Extract from the 25th Pan-Hellenic Conference Program

32nd Annual Congress of the Hellenic Society of Haematology

The Panhellenic Hematology Conference⁷ is the largest event in the field of Hematology in Greece and in this context, the Scientific Committee has formed, the Scientific Program to cover current developments in all fields of the specialty.

⁶ <https://pci2021.uth.gr/>

⁷ <https://www.eae.gr/el/information/video-gallery/item/984-32o-panellinio-aimatologiko-synedrio-programma>

The Educational Program of the 32nd PHC includes educational symposia, special lectures, scientific debates, oral and posted announcements and special sessions for Nurses, Biologists and Technologists. There will also be an opportunity to discuss with experts on issues of particular interest. For the first time in our Conference, in collaboration with the Hellenic Society of Medical Students of Greece, three sessions are included in the program.

The AI4HEALTHSEC project was represented by the partners FORTH and STS who participated through an e-POSTER contribution on the subject of the validation of a specific model using Machine Learning algorithms.



Figure 2-5. Extract from the e-POSTERS outline of the 32nd Annual Congress of the Hellenic Society of Haematology

Security Research Event 2022 (SRE2022)

In December 2021, the project Coordinator informed the project partners about the Security Research Event⁸ (SRE), which would take place on 1st and 2nd March 2022, at the Cité des Sciences et de l'Industrie in Paris.

The project partners reviewed the event and decided that it was a great opportunity to showcase the developments of the project, to increase awareness and introduce the project to wider audience.

The necessary arrangements were made and the AI4HEALTHSEC project was planned to participate with a stand along with the DEFEND project⁹.

⁸ <https://www.sre2022.eu/>

⁹ <https://www.defendproject.eu/>

CS CYBER-SECURITY

S1 - STAND 07 - DEFEND - AI4HEALTHSEC

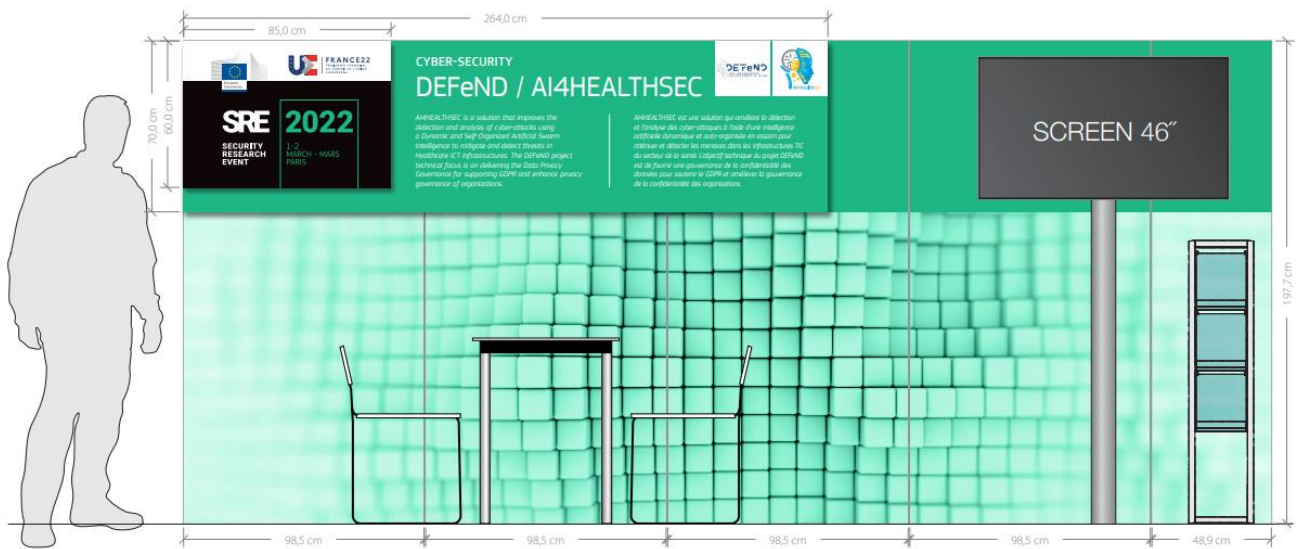


Figure 2-6. AI4HEALTHSEC / DEFEND stand visual

To further support AI4HEALTHSEC's presence developments of the project in the Security Research Event 2022 (SRE2022), a flyer and two presentations were created. The visual of the flyer can be found in section 2.4.1. Brochures.

On February 25th, 2022, the Coordinator of the project was informed that the SRE2022 was canceled due to FORCE MAJEURE.



ANNOUNCEMENT

Cancellation of the event

Due to the ongoing international crisis and its latest developments, the French Presidency of the Council of the European Union is obliged, by *FORCE MAJEURE*, to cancel the SRE 2022 scheduled for 1st and 2nd March at the *Cité des Sciences et de l'Industrie* in Paris. Further information will be provided at a later date.

Figure 2-7. Announcement of the Cancellation of the SRE 2022

International Cybersecurity Forum (FIC)

In January 2022, the project Coordinator informed the project partners about the International Cybersecurity Forum (FIC)¹⁰, which this year will take place from 7-9 June 2022 in Lille, France. The FIC is Europe's flagship cybersecurity event, and will this year be part of the official program of the French Presidency of the EU.

The project partners reviewed the event and decided that it was a great opportunity to showcase the developments of the project, to increase awareness and introduce the project to wider audience.

The necessary arrangements have started and the AI4HEALTHSEC project is planned to participate in the pitch sessions.

ISF Francophone chapter meeting

This meeting was held by the Information Security Forum in Paris on the 29th of March. The francophone ISF chapter is a regularly held meeting where information security actors have exchanges around ongoing projects and opportunities related to cybersecurity and risk management.

During this event, AI4HEALTHSEC has been presented by Privanova to a number of cybersecurity professionals and other industry experts.

United Nations: Countering the use of ICT for criminal purposes

AI4HEALTHSEC was presented, among other cybersecurity-related projects, during the first intersessional consultation of the Ad Hoc Committee established by the UN General Assembly¹¹ (on the 24th and 25th of March 2022). The project partner Privanova is a member of this Committee and was able to deliver this presentation. Figure2-8 is a screenshot from the presentation. The committee aims to elaborate a comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.

The project was thus introduced to representatives from 193 member states and other international organizations including the European Union's delegation that highlighted the importance of disseminating EU projects and efforts in cybersecurity capacity-building on a universal level.

¹⁰ <https://www.forum-fic.com/en/home/>

¹¹ <https://www.un.org/en/ga/>



Figure 2-8: Several cybercrime-related EU-funded projects presented at the United Nations

2.3.3 Workshops

2nd Joint Workshop - Dynamic Countering of Cyber-attacks

The Joint Standardisation Workshop¹² aims at gathering the projects from the SU-ICT-01-2018 H2020 call, whose main topic is Dynamic countering of cyber-attacks, to share the main progress of the project, create synergies and set a common ground for standardization activities.

Moreover, experts representing each project will discuss the different approaches to the common problem of attack detection and situational awareness in different environments.

The AI4HEALTHSEC project was represented by TUV who participated with a presentation on the subject “Standards in the HORIZON” (Figure 2-9).

¹² <https://www.cybersane-project.eu/standardisation-workshop-2022/>



15:00 – 15:20 Invited talk: "Standards in the HORIZON", Argyro Chatzopoulou - Lead Auditor and Trainer, Standardization leader of CONCORDIA & AI4HEALTHSEC, Member of ISO, CEN and CENELEC

15:20 – 15:30 Q&A Session

Figure 2-9. Extract from the agenda of the 2nd Joint Workshop - Dynamic Countering of Cyber-attacks

CONCORDIA e-health workshop

Introduction to the CONCORDIA project:

(The following text has been extracted from the project description page in Cordis¹³)

It is in the EU's strategic interest to develop and hold on to its security capacities. This, however, is a challenging task due to lack of alignment of cybersecurity competences across the sector in Europe with little alignment. CONCORDIA¹⁴, 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.

Objective 7 of the CONCORDIA project is to "Develop sector-specific (vertical) and cross-sector (horizontal) industrial pilots with building incubators". For this reason, there is dedicated e-Health

¹³ <https://cordis.europa.eu/project/id/830927>

¹⁴ <https://www.concordia-h2020.eu/>

pilot and specific activities have taken place on the subjects of Risk Management, Incident response and information sharing.

The CONCORDIA ecosystem

The CONCORDIA project has an extended ecosystem, with more than 50 partners and has created the following:

- A. The National Cybersecurity Coordination Centres and Agencies Stakeholders Group (NSG);
- B. The Liaison Stakeholders Group (LSG), and C. The Observer Stakeholders Group (OSG).

Specifically, the OSG concerns current, upcoming and future stakeholders of the Cybersecurity Competence Community, not being national governmental bodies (who generally will be part of the NSG) or European institutions (who generally will be part of the LSG).

The purpose of the OSG is to support the development of the proposed network (including both the National Cybersecurity Coordination Centers ('NCCCs') and Cybersecurity Competence Community), including without limitation interconnecting existing, developing or to be developed ecosystem in and across the member states with the other stakeholders of this evolving network. The OSG will focus on the Cybersecurity Competence Community.

The workshop

The partners of the AI4HEALTHSEC project, identified these common subjects and the existence of this extended ecosystem and proposed to implement a common workshop between the members of the two projects and the OSG, on the subject of eHealth, with a focus on Risk Management and Information Sharing.

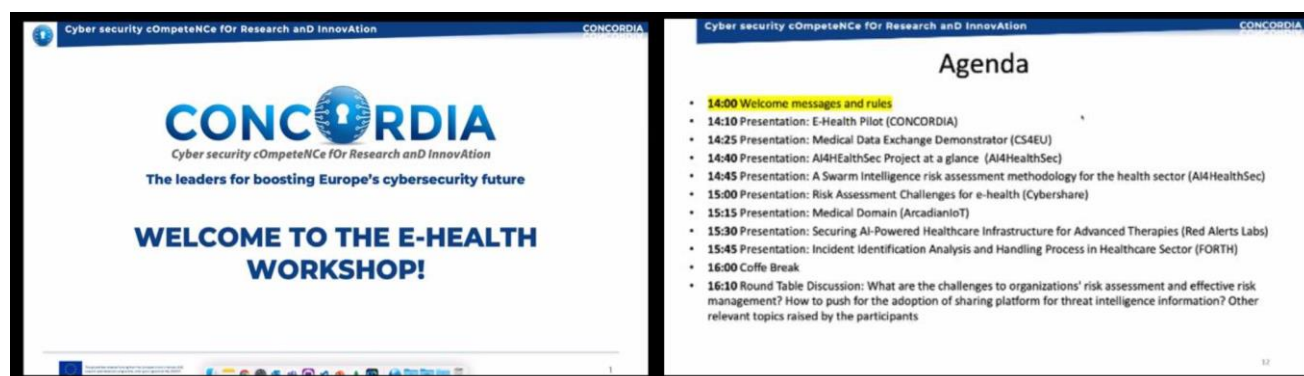
The eHealth workshop happened remotely on March 16th 2022. **Figure 2-10** shares some screenshots of the presentations. The workshop had also the purpose of rising awareness for the AI4HEALTHSEC project (raising awareness workshop).

The structure of the workshop was the following:

Part 1: presentation by each project on:

- i. The Project and its objectives;
- ii. Risk Management methodology and approach;
- iii. Incident response and Information Sharing.

Part 2: Open discussion open to all attendees of the workshop.



Cyber security cOmpeNeNce fOr Research aNd INNOVAtION

CONCORDIA
Cyber security cOmpeNeNce fOr Research aNd INNOVAtION

T2.4 eHealth pilot

Detlef Houdeau, IFAG, Munich, Germany
Anja Majstorovic, eesy-innovation, Germany

Cyber Security for Europe

CS4EU - Medical Data Exchange Demonstrator

Juan Carlos Pérez Bañ
Miryam Villegas Jimenez

CONCORDIA Workshop 16th March 2022

CyberSec4Europe is funded by the European Commission under the H2020 Programme Grant Agreement No. 830929

Ai4HealthSec H2020 Project

- A Dynamic and Self-Organized Artificial Swarm Intelligence Solution for Security and Privacy Threats in Healthcare ICT Infrastructures (AI4HealthSec)
- Call: H2020-SU-DS-2019 (Digital Security)
- Topic: SU-DS05-2018-2019
- Type of Action: RIA
- Project duration: 36 Months
 - Started: 1/10/2020
 - End: 30/09/2023
- Proposal overall cost: 4,998,948.75 €
- Project Coordinator: CNR
- Website: <https://www.ai4healthsec.eu/>

Open Call

- The project has the objective to design and develop a framework for the **healthcare sector**
- It also aims at validating its solution to **different domains**, like energy, finance and water supply sectors
- Ai4HealthSec will launch an **Open Call** to invite external partners coming from different domains to join Ai4HealthSec

A Swarm Intelligence Risk Assessment Methodology for the health sector

Ai4HealthSec

Dr. Shareef Islam
Dr. Spyridon Papastergiou
Focal Point
Date : 16/03/2022

CONCORDIA E-HEALTH WORKSHOP

RA/RM E-HEALTH WORKSHOP

Risk Assessment Challenges

ITSRM2 – IT Security Risk Management methodology developed by the European Commission in 2018

EC wanted:

- RM methodology customized for their environment
- One methodology for all projects
- Be able to compare results and reuse information

RED ALERT LABS
IoT Security

Securing AI Powered HealthCare Infrastructure for Advanced Therapies

Presentation to CONCORDIA

16/03/2022

AIDPATH

ARCADIAN-IOT MEDICAL DOMAIN C PRESENTATION TO CONCORDIA

RICARDO RUIZ
RGB MEDICAL DEVICES
RRUIZ@RGB-MEDICAL.COM

16th March 2022



Figure 2-10. Screenshots from the presentations during the CONCORDIA ehealth workshop

The participants included organizations in the following categories: European Projects in health domain, Medical Devices Manufacturers, Consulting companies, IT Companies, Laboratories, Ministries, Hospitals, Research institutions, Universities and others. The aim of this workshop was to acquaint a varied ecosystem regarding the project and approach, to introduce the open call and to exchange opinions regarding Risk Assessment and Threat Intelligence Information Exchange within the health domain. This workshop represents one of the actions implemented by the project in order to raise awareness for the project to an extended ecosystem.

The 2nd ECSCI Workshop on Critical Infrastructure Protection

The main objective of the ECSCI¹⁵ cluster is to create synergies and foster emerging disruptive solutions to security issues via cross-projects collaboration and innovation. Research activities focus on how to protect critical infrastructures and services, highlighting the different approaches between the clustered projects and establishing tight and productive connections with closely related and complementary H2020 projects. To promote the activities of the cluster, ECSCI will organize international conferences, and national or international workshops, involving both policy makers, industry and academic, practitioners, and representatives from the European Commission.

This 2nd workshop of the ECSCI cluster¹⁶, workshop presented the different approaches to integrated cyber and physical security in different industrial sectors, such as energy, transport, drinking and wastewater, health, digital infrastructure, banking and financial market, space and public administration. The peculiarities of critical infrastructure protection in each one of these sectors will be discussed and addressed by the different projects of the ECSCI cluster that will present their outcomes, discussing the technical, ethical, and societal aspects as well as the underlying technologies.

Specifically, novel techniques were presented for integrated security modelling, IoT security, artificial intelligence for securing critical infrastructures, distributed ledger technologies for security information sharing and increased automation for detection, prevention and mitigation measures.

¹⁵ <https://www.finsec-project.eu/ecsci>

¹⁶ <https://www.finsec-project.eu/second-ecsci-virtual-workshop>

The AI4HEALTHSEC project was represented by TUV who participated with a presentation on the subject “Standards and NIS compliance”, in the Session 2 (29.04.2022), Standards and regulations.

Day 3: Friday, April 29th 2022 (9:00-17:00)

Invited Talk & Common Thematic Presentations

Welcome and Session 1	
<i>Chair: Habtamu Abie, Norsk Regnesentral</i>	
09:00 – 09:10	Welcome and opening remarks - Giannis Skiadaresis from DG Migration and Home Affairs, Unit B4 - Innovation and Security Research
09:10 – 10:00	Invited talk: The evolution of security and resilience of critical infrastructures in a challenging environment by Georgios Giannopoulos, JRC
Session 2: Standards and regulations	
<i>Chair: Loredana Mancini, Inlecom Systems</i>	
10:00 – 11:20	Standards and Regulations for the Protection of Critical Infrastructures <ul style="list-style-type: none"> • PHOENIX – Industrial Cybersecurity Testing Methodology on LSPs by Ganesh Sauba, DNV • Emerging Cybersecurity Standards for Critical Infrastructure – Lessons from Recent Goals Released by CISA and NIST in the United States by Ilesh Dattani, Assentian • Standards and NIS compliance by Argyro Chatzopoulou, TÜV TRUST IT GmbH • InfraStress: New DIN 91461 standard SPEC document on stress-testing resilience of critical infrastructures by A. Jovanović, Steinbeis EU-VRI, G. Giunta, Ch. Grunewald

Figure 2-11. Extract of the agenda of the 2nd ECSCI workshop

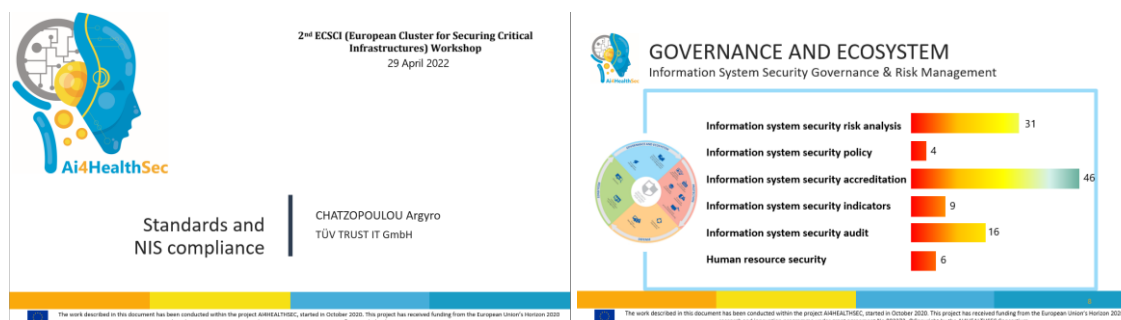


Figure 2-12. Screenshots from the presentation during the 2nd ECSCI workshop

2.3.4 Collaboration with other projects

The project partners actively review other projects’ descriptions in order to identify opportunities for possible collaborations, review and exchange of information. As such discussions have already started with the projects CyberKit4SME¹⁷, HEIR¹⁸, SENTINEL¹⁹ and SMARTBEAR²⁰.

CyberKit4SME

The overall aim of CyberKit4SME is to democratize advanced cyber security methods for SMEs and MEs, in order to:

- Enable SMEs and MEs to monitor and forecast cybersecurity risks by equipping them with advanced, but low-cost and easy-to-use tools that will allow them to both assess

¹⁷ <https://cyberkit4sme.eu/>

¹⁸ <https://heir2020.eu/>

¹⁹ <https://sentinel-project.eu/>

²⁰ <https://www.smart-bear.eu/>

the cybersecurity risks of their business's IT infrastructure at design-time (following an asset-based risk assessment approach aligned with ISO 27005) and to monitor and update risk level assessments in real-time to detect potential threats without frequent recourse to expensive cybersecurity experts including consultants.

- Raise SMEs and MEs' awareness of cybersecurity risks, vulnerabilities and attacks through training in the use of these tools, and by analysing organisational and human factors that affect risk levels in their business, making educational material available for their employees to promote safe behaviour, facilitating their participation to cyber ranges as part of the training experience, and fostering a resilient community of SMEs and MEs by promoting information exchange with CERT/CSIRTs and other SMEs and MEs on cybersecurity incidents.
- Support SMEs and MEs to manage their security, privacy and personal data protection risks by providing a wide-ranging set of tools that will allow them to implement risk mitigation measures based on a sophisticated risk analyses for their information networks, including end-to-end data protection using advanced encryption techniques to ensure confidentiality and integrity for data stored, transferred and processed onsite or in the cloud, and SIEM technology to help them prevent, detect and recover from cyber-attacks.
- Equip SMEs and MEs with an online collaborative, security information sharing and incident reporting system by providing a blockchain platform through which SMEs and MEs will be able to securely share cybersecurity information in supply chains and with CERTS to improve risk monitoring and facilitate preparedness and responses to cyber-attacks, engage in a collective response to cyber security risks, and implement mandatory cybersecurity incident reporting.

The CyberKit4SME project aims to demonstrate these tools working in an operational environment based on SME partners' existing product and service testing environments, and with users fulfilling their normal business roles. It will also take the necessary actions to ensure the tools provided will be commercially sustainable and can be made available to a wide range of SMEs and MEs following the project.

A preliminary meeting has already taken place on the 7th of March 2022, with the following agenda:

- Presentations / Introductions;
- CyberKit4SME short presentation;
- AI4HEALTHSEC short presentation
- Collaboration discussion.

Meeting minutes have been taken and collaboration potential identified. Further meeting was already scheduled for the 11th of April 2022.

HEIR and SENTINEL

The EU funded projects HEIR²¹ (GA 883275) and SENTINEL²² (GA 101021659) are also performing dedicated research and innovation activities for the healthcare sector.

HEIR is to provide thorough threat identification and cybersecurity knowledge base system addressing both local, in the hospital or medical centre, and global (including different stakeholders) levels, that comprises the following pillars:

- i. Real time threat hunting services, facilitated by advanced machine learning technologies, supporting the identification of the most common threats in electronic medical systems based on widely accepted methodologies such as the OWASP Top 10 Security Risks²³ and the ENISA Top 15 Threats²⁴;
- ii. Sensitive data trustworthiness sharing facilitated by the HEIR privacy aware framework;
- iii. Innovative Benchmarking based on the calculation of the Risk Assessment of Medical Applications (RAMA) score, that will measure the security status of every medical device and provide thorough vulnerability assessment of hospitals and medical centres;
- iv. The delivery of an Observatory for the Security of Electronic Medical Devices, an intelligent knowledge base accessible by different stakeholders, providing advanced visualisations for each threat identified in RAMA and facilitating global awareness on EMD-related threats.

SENTINEL aspires to bridge this gap by boosting SMEs/MEs capabilities in this domain through innovation, at a cost-effective level. SENTINEL will integrate tried-and-tested modular cybersecurity technologies with fresh, ambitious ones, such as a novel Identity Management System for human-centric data portability, enabling a unified “European Data Space” and an end-to-end digital personal data protection compliance self-assessment framework for SMEs, into a unified digital architecture. The data from these modules will then undergo disruptive Intelligence for Compliance through SENTINEL’s digital core, featuring machine learning-powered recommendations, policy drafting & enforcement for compliance, and a ‘one-stop-shop incident response centre. Combined with a well-researched methodology for application, an open knowledge sharing hub, and a wide-reaching plan for experimentation, SENTINEL will catalyze the adoption of market-leading security tech among SMEs/MEs and help safeguard their and their customers’ assets.

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)” 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,

²¹ <https://heir2020.eu/>

²² <https://sentinel-project.eu/>

²³ <https://owasp.org/www-project-top-ten/>

²⁴ <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-list-of-top-15-threats>

where further face-to-face interaction and collaboration is expected between the projects' partners.



Figure 2-13. ARES – IOSec 2022 workshop

SMARTBEAR

The aim of the SMART-BEAR²⁵ platform is to integrate heterogeneous sensors, assistive medical and mobile devices to enable the continuous data collection from the everyday life of the elderly, which will be analysed to obtain the evidence needed in order to offer personalised interventions promoting their healthy and independent living. The platform will also be connected to hospital and other health care service systems to obtain data of the end users (e.g., medical history) that will need to be considered in making decisions for interventions.

SMART-BEAR will leverage big data analytics and learning capabilities, allowing for large scale analysis of the above mentioned collected data, to generate the evidence required for making decisions about personalised interventions. Privacy-preserving and secure by design data handling capabilities, covering data at rest, in processing, and in transit, will cover comprehensively all the components and connections utilized by the SMART-BEAR platform.

The SMART-BEAR platform will be tested and validated through six large scale pilots, spanning six different countries and 5.100 individuals: France, Greece, Italy, Spain, Romania and Portugal. The pilots will enable the evaluation of the platform in the context of healthcare service delivery by private and public providers at regional, state and EU level, and demonstrate its efficacy, extensibility, sustainability, and cost effectiveness for the individual and the healthcare system.

²⁵ <https://www.smart-bear.eu/>

Meetings have already been implemented between the two projects and further meetings are planned to take place during the FIC – International Cybersecurity Forum.

AI4HEALTHSEC – HEIR workshop

As mentioned above, the AI4HEALTHSEC and the HEIR projects are trying to identify potential collaboration. To further investigate this potential, a workshop took place on the 29th of March 2022 with the following agenda (Figure 2-14):

- Presentations/ Introductions
- HEIR short presentation
- AI4HEALTHSEC short presentation
- Collaboration discussion

Meeting minutes have been taken and collaboration potential identified. The partners decided to meet in person and further discuss collaboration potential in France, along with the FIC (both projects plan to participate).

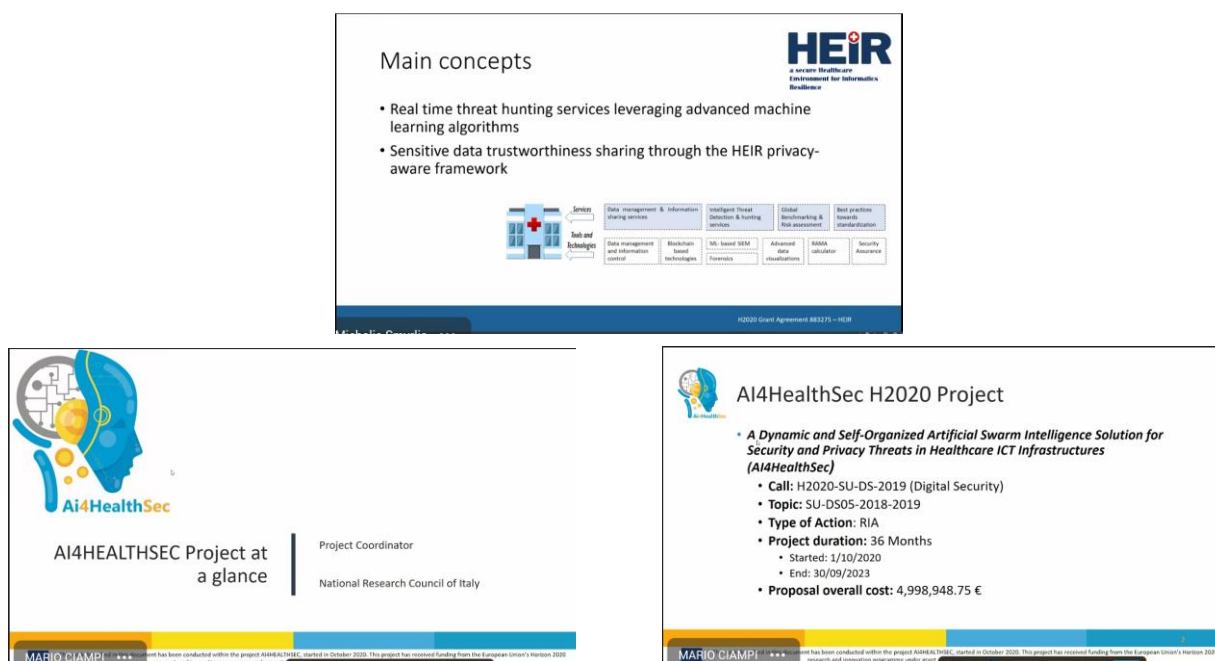



Figure 2-14. Screenshots from the AI4HEALTHSEC – HEIR workshop

2.4 Project publications

2.4.1 Brochures

For the needs of CyberHOT Summer School, AI4HEALTHSEC project created two posters (Figure 2-15) with the main objectives of the project.




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

AI4HEALTHSEC will deliver an Artificial Intelligence Dynamic Situational Awareness Framework (DSAF) able to:

- improve, intensify and coordinate the overall security efforts for the effective and efficient identification, evaluation, investigation and mitigation of realistic risks, threats and multi-dimensional attacks within the cyber assets
- support, prepare and help the Interdependent HCIs participating in different types of Health Care Supply Chain Services.

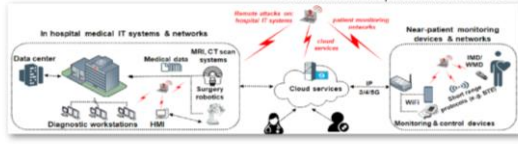
The DSAF will support:

- the HCIs and the other stakeholders comprising the Health Care ecosystem to recognize, identify, model, and dynamically analyse cyber risks
- forecasting, treatment and response to advanced persistent threats and handle daily cyber-security and privacy risks, incidents and data breaches.



Objectives:

- Self-organized Swarm Intelligence (SI) model
- Distributed data management and reasoning capabilities
- Dynamic Situational Awareness Approach for HCIs
- Validation in real operational environments



Partners: ICAR, AEGIS, @bit, focal point, FORTH, Fraunhofer, PDM, PHILIPS, Privanov, TÜV, University of Brighton.

Project Coordinator: Giuseppe De Pietro (CNR)
Project Technical Manager: Spyridon Papadimitriou (FP)

Website: www.ai4healthsec.eu
Twitter: @ai4healthsec
LinkedIn: ai4healthsec
Facebook: ai4healthsec

This project has received funding from the European Union's Horizon 2020 research and innovation programme, under Grant Agreement 883273. **Project Duration:** 3 years



WHAT

The objectives of the AI4HealthSec project are:

- 1 Self-organized Swarm Intelligence (SI) model
- 2 Distributed data management and reasoning capabilities
- 3 Dynamic Situational Awareness Approach for HCIs
- 4 Validation in real operational environments

HOW

To achieve these objectives the AI4HealthSec project:

- proposes a state of the art solution that improves the detection and analysis of cyber-attacks and threats on HCIs, and increases the knowledge on the current cyber security and privacy risks.
- will build risk awareness, within the digital Healthcare ecosystem and among the involved Health operators, to enhance their insight into their Healthcare ICT infrastructures and provide them with capability to react in case of security and privacy breaches.
- fosters the exchange of reliable and trusted incident.

FOLLOW & SUBSCRIBE TO OUR NEWSLETTER
<https://www.ai4healthsec.eu/newsletter/>
www.ai4healthsec.eu

Twitter **Facebook** **LinkedIn**

This project has received funding from the European Union's Horizon 2020 research and innovation programme, under Grant Agreement 883273

Figure 2-15. Screenshot from AI4HEALTHSEC posters

Figure 2-16 illustrates the AI4HEALTHSEC brochure for Security Research Event 2022 (SRE2022).



Figure 2-16. Screenshots from AI4HEALTHSEC brochure

2.4.2 Publications in professional journals & Conferences

This subsection presents an overview of the paper publication by the consortium partners.

A Dynamic Cyber Security Situational Awareness Framework for Healthcare ICT Infrastructures

PCI 2021: 25th Pan-Hellenic Conference on Informatics | November 2021 | Pages 334–339 | <https://doi.org/10.1145/3503823.3503885>

Authors: Shareeful Islam, Spyridon Papastergiou, Haralambos Mouratidis

The healthcare sectors have experienced a massive technical evolution over the past decade by integration of medical devices with IT at both physical and cyber level for a critical Health Care Information Infrastructure (HCII). HCII provides huge benefits for the health care service delivery but evolving digital interconnectivity among medical and IT devices has also changed the threat landscape. In particular, systems are now more exposed to the cyber-attacks due to sensitivity and

criticality of patient health care information and accessibility of medical devices and this pose any potential disruption of healthcare service delivery. There is a need to enhance security and resilience of HCII. In this paper, we present a Cyber Security Situational Awareness Framework that aims to improve the security and resilience of the overall HCII. The framework aims to develop a novel dynamic Situational Awareness approach on the health care ecosystem. We consider bio inspired Swarm Intelligence and its inherent features with the main principles of the Risk and Privacy assessment and management and Incident handling to ensure security and resilience of healthcare service delivery.

The landscape of cybersecurity vulnerabilities and challenges in healthcare: Security standards and paradigm shift recommendations

ARES 2021: The 16th International Conference on Availability, Reliability and Security | August 2021 | Article No.: 136 | Pages 1–9 | <https://doi.org/10.1145/3465481.3470033>

Authors: Kitty Kioskli, Theo Fotis, Haralambos Mouratidis

Digital technology provides unique opportunities to revolutionize the healthcare ecosystem and health research. However, this comes with serious security, safety, and privacy threats. The healthcare sector has been proven unequipped and unready to face cyberattacks while its vulnerabilities are being systematically exploited by attackers. The growing need and use of medical devices and smart equipment, the complexity of operations and the incompatible systems are leaving healthcare organizations exposed to various malware, including ransomware, which result in compromised healthcare access, quality, safety and care. To fully benefit from the advantages of technology, cybersecurity issues need to be resolved. Cybersecurity measures are being suggested via a number of healthcare standards which are often contradicting and confusing, making these measures ineffective and difficult to implement. To place a solid foundation for the healthcare sector, in improving the understanding of complex cybersecurity issues, this paper explores the existing vulnerabilities in the health care critical information infrastructures which are used in cyberattacks and discusses the reasons why this sector is under attack. Furthermore, the existing security standards in healthcare are presented alongside with their implementation challenges. The paper also discusses the use of living labs as a novel way to discover how to practically implement cybersecurity measures and also provides a set of recommendations as future steps. Finally, to our knowledge this is the first paper that analyses security in the context of living labs and provides suggestions relevant to this context.

A Privacy-Preserving and Standard-Based Architecture for Secondary Use of Clinical Data

Information 2022, 13(2), 87 | February 2022 | <https://doi.org/10.3390/info13020087>

Authors: Mario Ciampi, Mario Sicuranza, Stefano Silvestri

The heterogeneity of the formats and standards of clinical data, which includes both structured, semi-structured, and unstructured data, in addition to the sensitive information contained in them, require the definition of specific approaches that are able to implement methodologies that can permit the extraction of valuable information buried under such data. Although many challenges and issues that have not been fully addressed still exist when this information must be processed and used for further purposes, the most recent techniques based on machine learning and big data analytics can support the information extraction process for the secondary use of clinical data. In particular, these techniques can facilitate the transformation of heterogeneous data into a common standard format. Moreover, they can also be exploited to define anonymization or pseudonymization approaches, respecting the privacy requirements stated in the General Data Protection Regulation, Health Insurance Portability and Accountability Act and other national and regional laws. In fact, compliance with these laws requires that only de-identified clinical and personal data can be processed for secondary analyses, in particular when data is shared or exchanged across different institutions. This work proposes a modular architecture capable of collecting clinical data from heterogeneous sources and transforming them into useful data for secondary uses, such as research, governance, and medical education purposes. The proposed architecture is able to exploit appropriate modules and algorithms, carry out transformations (pseudonymization and standardization) required to use data for the second purposes, as well as provide efficient tools to facilitate the retrieval and analysis processes. Preliminary experimental tests show good accuracy in terms of quantitative evaluations.

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

NEURAL COMPUTING AND APPLICATIONS SPECIAL ISSUE ON LARGE SCALE NEURAL COMPUTING & CYBERSECURITY OPPORTUNITIES USING ARTIFICIAL INTELLIGENCE | February 2022 | <https://doi.org/10.1007/s00521-022-06959-2>

Authors: Halima Ibrahim Kure, Shareeful Islam, Haralambos Mouratidis

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-CSRМ) 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.

Cyberattack Path Generation and Prioritisation for Securing Healthcare Systems

Applied Sciences 12(9), 4443 | April 2022 | <https://doi.org/10.3390/app12094443>

Authors: Shareeful Islam, Spyridon Papastergiou, Eleni-Maria Kalogeraki, Kitty Kioskli

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.

2.5 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.

The *AI4HEALTHSEC social media accounts* are mainly used to disseminate news that are related to:

- The AI4HEALTHSEC project;
- Cybersecurity, Artificial Intelligence, Privacy;
- New trends or new solutions in relation to the project scope;
- Promote and share the Newsletters.

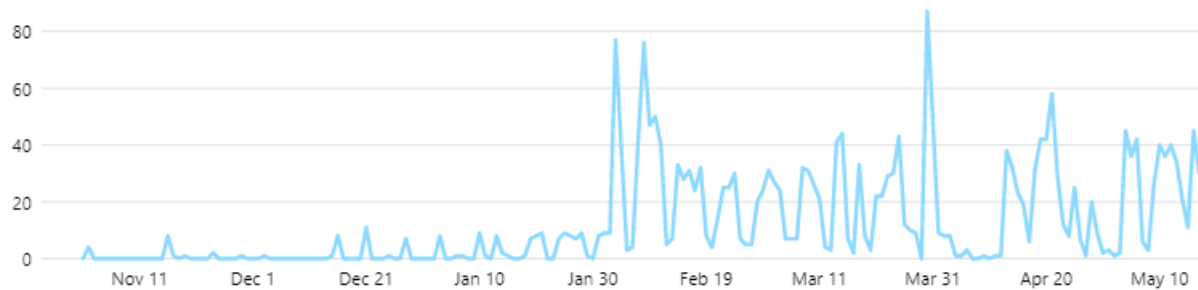
2.5.1 Facebook

The *Facebook*²⁶ account (up to 18th of May 2022) counts 149 followers. **Figure 2-17** depicts the results, in general, of the account for the period November 2021 - May 2022.

²⁶ <https://www.facebook.com/Ai4HealthSec>

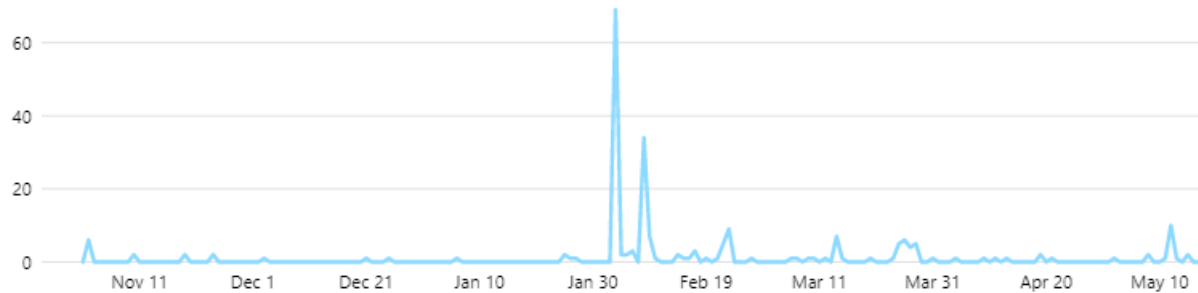
Facebook Page reach ⓘ

276 ↑ 1.9K%



Facebook Page visits ⓘ

223 ↑ 869.6%



Facebook Page new likes ⓘ

119 ↑ 981.8%

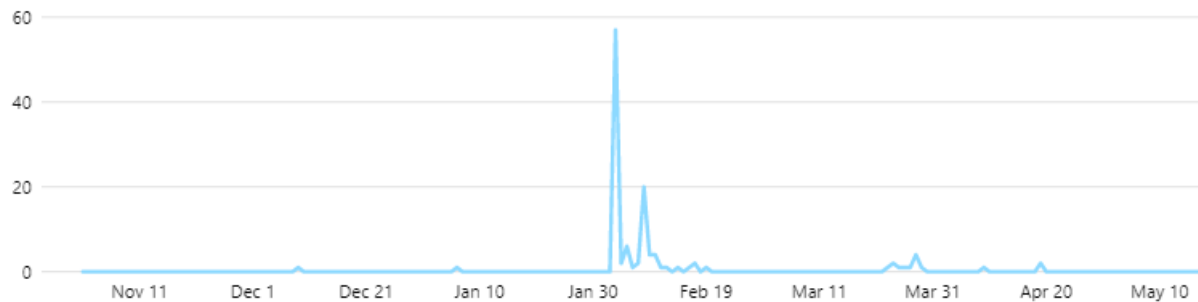
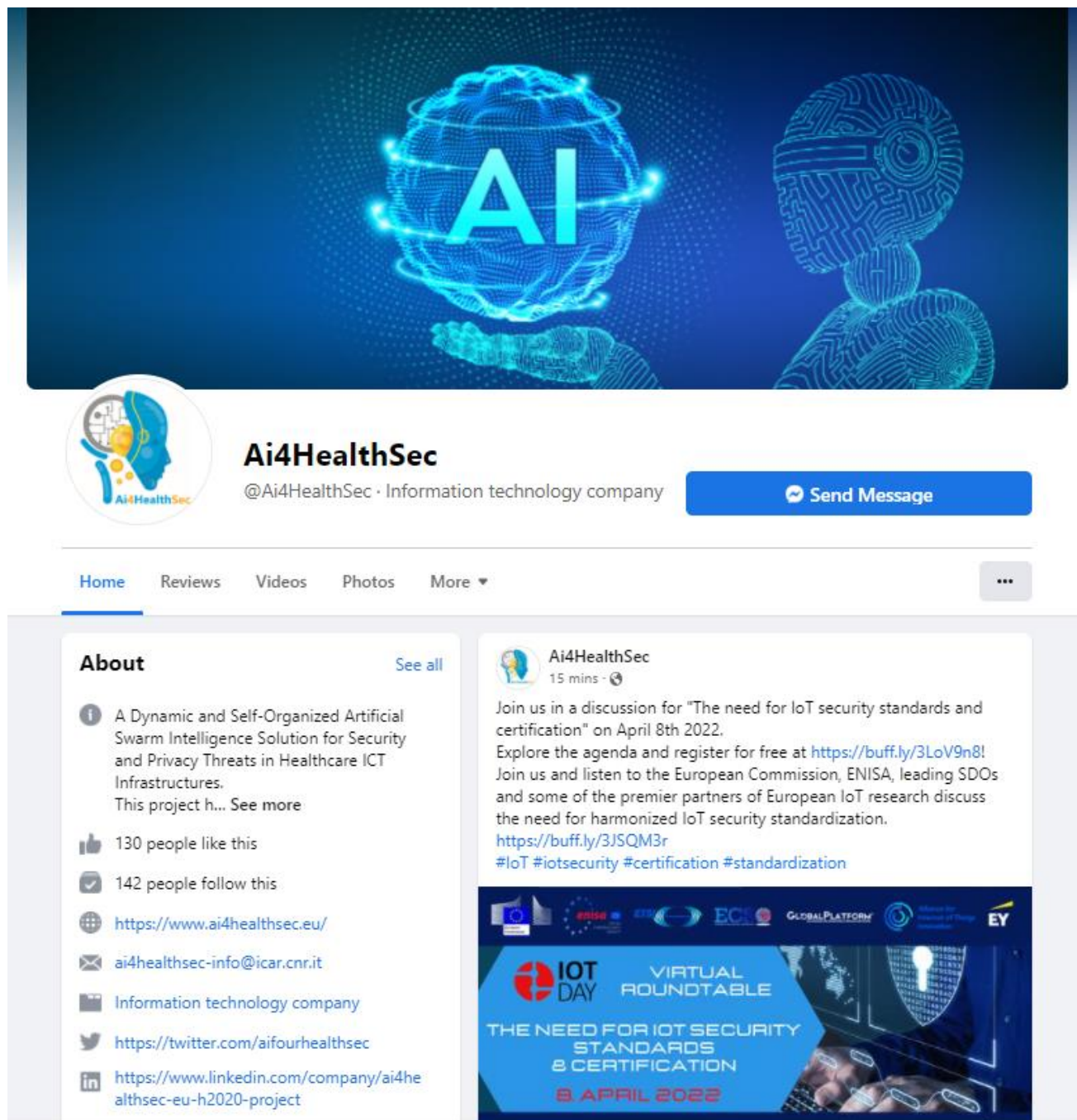


Figure 2-17. Facebook general results



The image shows a screenshot of the Facebook profile page for Ai4HealthSec. The profile picture is a circular logo featuring a stylized head with a brain and circuitry. The cover photo is a blue-themed graphic with a glowing 'AI' in the center, surrounded by a network of dots and lines, and a robotic head silhouette on the right. The profile name is 'Ai4HealthSec' with the tagline '@Ai4HealthSec · Information technology company'. A 'Send Message' button is visible. Below the profile information, there are tabs for 'Home', 'Reviews', 'Videos', 'Photos', and 'More'. The 'About' section is expanded, showing a description of the project as a 'Dynamic and Self-Organized Artificial Swarm Intelligence Solution for Security and Privacy Threats in Healthcare ICT Infrastructures'. It also lists 130 likes and 142 followers, along with the website 'https://www.ai4healthsec.eu/' and email 'ai4healthsec-info@icar.cnr.it'. A recent post from 15 minutes ago discusses a discussion on 'The need for IoT security standards and certification' on April 8th 2022, with a link to a Buffer post and hashtags #IoT, #iotsecurity, #certification, and #standardization. The post includes a banner for 'IOT DAY VIRTUAL ROUNDTABLE' with the text 'THE NEED FOR IOT SECURITY STANDARDS & CERTIFICATION' and the date '8 APRIL 2022'.

Figure 2-18. Facebook home page

Facebook Statistics from November 2021 – May 2022

Posts	76
Reach	3157
Clicks	82
Likes and Reactions	400

Table 2-2. Facebook statistics

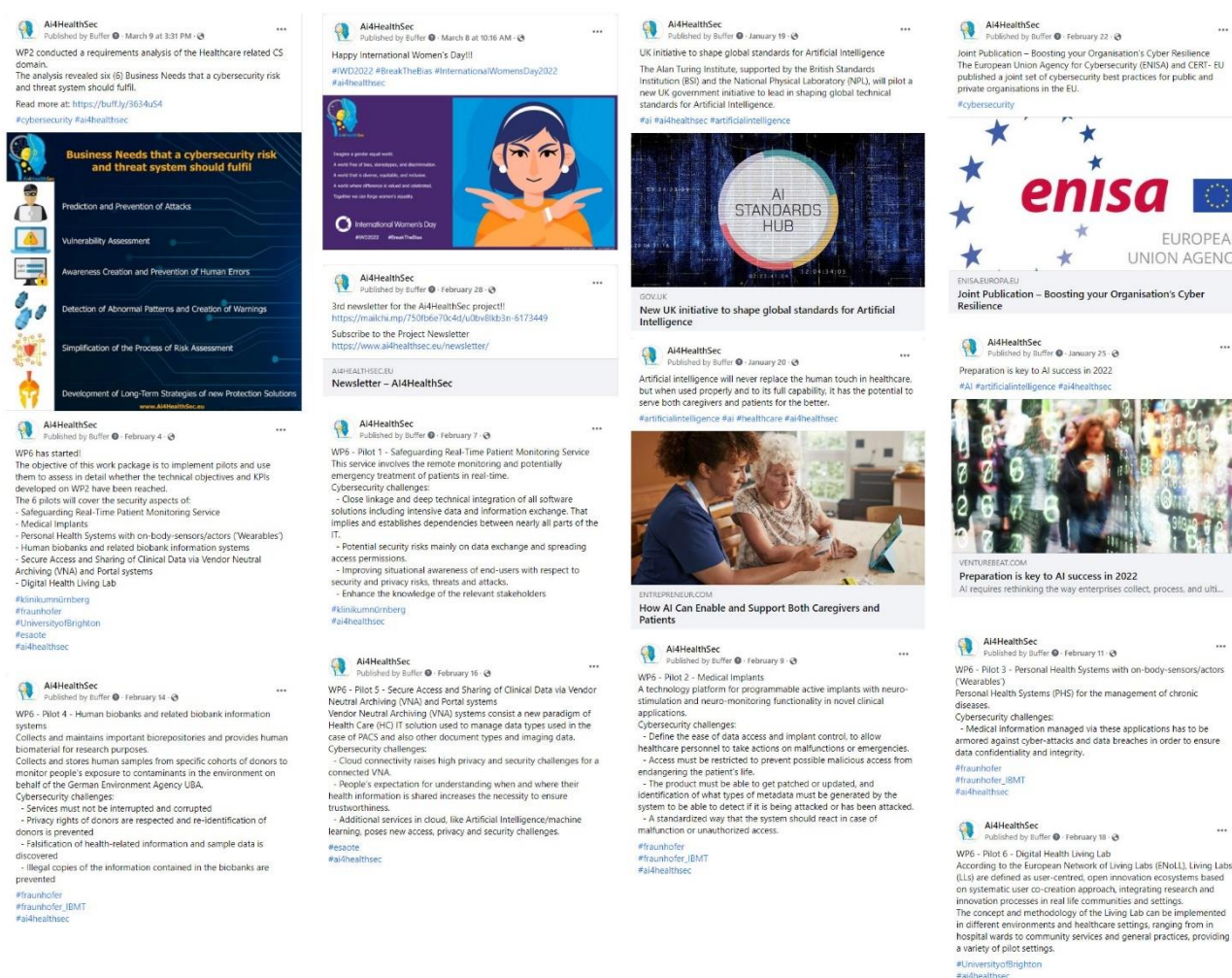


Figure 2-19. Facebook posts

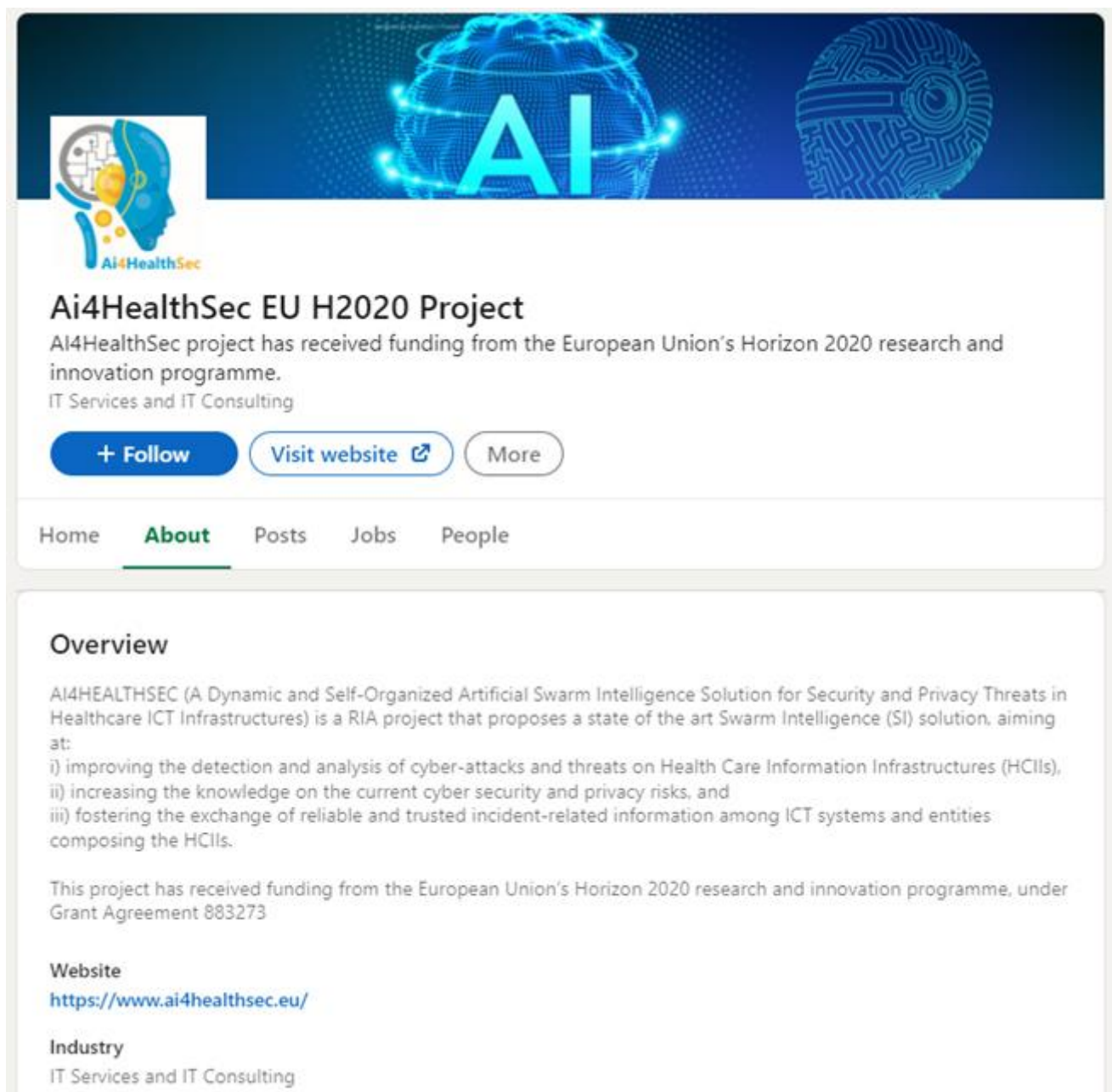
2.5.2 LinkedIn

The [LinkedIn²⁷](#) account for the AI4HEALTHSEC project was also created in 2021 but during the communication meeting that we had on the 16th of December, some of the partners they suggest us to create a company page for better management and easier connection. Specifically, in this way people can just follow the project page instead of becoming connected first. In the Communication meeting on the 3rd of February 2022, it was decided that a corporative account should be activated and the previous content should be reposted by the end of February 2022.

The AI4HEALTHSEC LinkedIn corporative account is entitled **AI4HEALTHSEC EU H2020 Project**.

(<https://www.linkedin.com/company/AI4HEALTHSEC-eu-h2020-project/>)

²⁷ <https://www.linkedin.com/company/ai4healthsec-eu-h2020-project>



Ai4HealthSec EU H2020 Project

Ai4HealthSec project has received funding from the European Union's Horizon 2020 research and innovation programme.

IT Services and IT Consulting

[+ Follow](#) [Visit website](#) [More](#)

Home **About** Posts Jobs People

Overview

AI4HEALTHSEC (A Dynamic and Self-Organized Artificial Swarm Intelligence Solution for Security and Privacy Threats in Healthcare ICT Infrastructures) is a RIA project that proposes a state of the art Swarm Intelligence (SI) solution, aiming at:

- i) improving the detection and analysis of cyber-attacks and threats on Health Care Information Infrastructures (HCIIIs),
- ii) increasing the knowledge on the current cyber security and privacy risks, and
- iii) fostering the exchange of reliable and trusted incident-related information among ICT systems and entities composing the HCIIIs.

This project has received funding from the European Union's Horizon 2020 research and innovation programme, under Grant Agreement 883273

Website
<https://www.ai4healthsec.eu/>

Industry
 IT Services and IT Consulting

Figure 2-20. LinkedIn “company” Home Page

LinkedIn Statistics from February 2022 – May 2022	
Followers	70
Unique visitors	109
Overview page views	243
Total page views	300

Table 2-3. LinkedIn statistics

2.5.3 Twitter

AI4HEALTHSEC [Twitter](https://twitter.com/aifourhealthsec)²⁸ account is mainly used for smaller posts that relate to the project, due to the character limitation. The account has earned 60 followers.



Figure 2-22. Twitter account home page

Twitter Statistics from November 2021 – March 2022							
	NOV 2021	DEC 2021	JAN 2022	FEB 2022	MAR 2022	APR 2022	MAY 2022
Tweets	2	3	12	20	16	10	17
Tweet impressions	406	262	1,442	2,149	2,468	1,431	1,654
Profile visits	540	300	986	1,545	1,771	1,099	1,134
Mentions	3	-	2	5	5	2	1

²⁸ <https://twitter.com/aifourhealthsec>

New followers	2	3	3	9	5	10	3
---------------	---	---	---	---	---	----	---

Table 2-4. Twitter statistics



Figure 2-23. Twitter posts

2.6 Website

The [AI4HEALTHSEC website](https://www.AI4HEALTHSEC.eu/) 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.

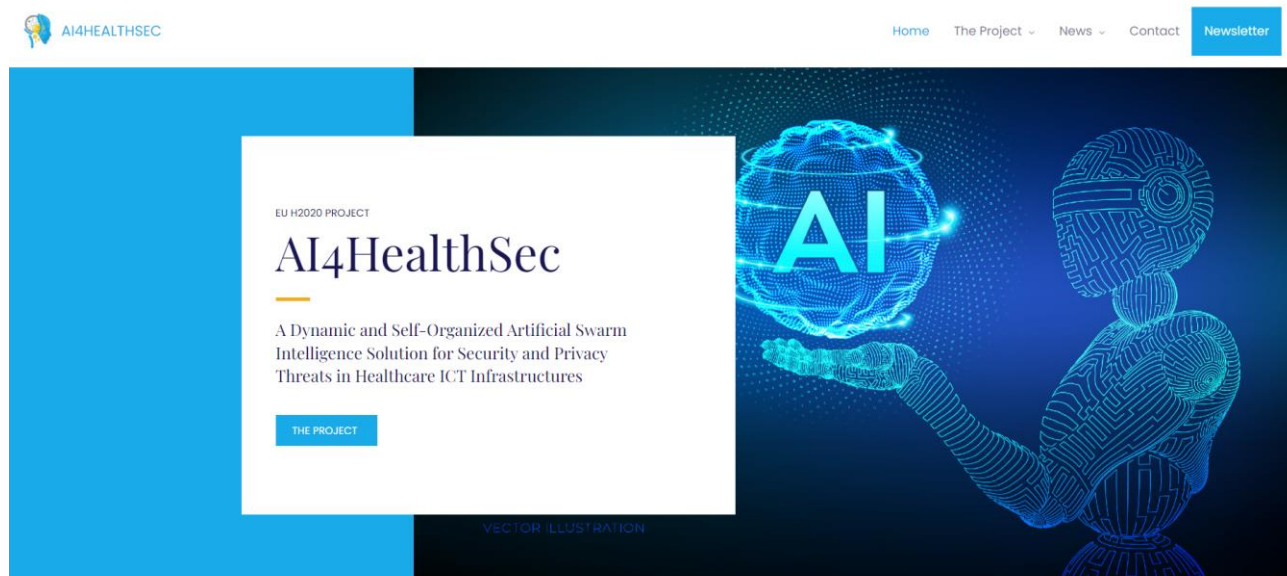


Figure 2-24. The AI4HEALTHSEC website

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 Workpackages are depicted in a roadmap in this page.

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 2.3. of this document.
- **Deliverables:** contains the published deliverables of the project. Deliverables classified as public can be directly accessed through this webpage. The entries until M18 have been updated on the website.
- **Publications:** displays the published articles and presentations in Scientific Journals and conferences. Currently there are four such publications displayed in the page.

- **Newsletters:** contains the links to the published newsletters of the AI4HEALTHSEC project. To this time 3 newsletters have been issued by the project (till the point that this report is being drafted).
- **Articles:** presents articles written by the project partners on the subjects of the project. Currently 4 articles have been published.

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 (subsection 2.7) .

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.

2.7 Newsletters

The newsletter subscription²⁹ 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. Until now 3 newsletters have been published as shown in **Figure 2-25**.

Project Newsletters

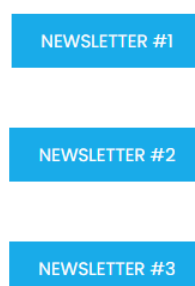


Figure 2-25. Extract from the website (<https://www.AI4HEALTHSEC.eu/newsletters/>)

²⁹ <https://www.ai4healthsec.eu/newsletter/>

Newsletter 1, May 2021



May 2021



About the Ai4HealthSec project

A Dynamic and Self-Organized Artificial Swarm Intelligence Solution for Security and Privacy Threats in Healthcare ICT Infrastructures (AI4HealthSec) is a European funded project under H2020-EU.3.7.6 & H2020 EU.3.7.4. The project was submitted as a proposal for the H2020-SU-DS-2019 call on the topic of Digital Security, privacy, data protection and accountability in critical sectors. [Grant Agreement ID: 883273]. Learn more on the project objectives, structure, partners and deliverables by pressing more.

More

Figure 2-26. Screenshot of the 1st project Newsletter

The first Newsletter of the AI4HEALTHSEC project, introduced the project and the partners. The newsletter was complimented by a brief message from the Coordinator of the project and commented on the progress of the project to that point of time.

Newsletter 2, September 2021



September 2021

The **1st Periodic activity report** of the **Ai4HealthSec** project has been issued and **successfully** dispatched!



Hand photo created by jcomp - www.freepik.com

The deliverable D1.3 – "Periodic activity report version 1" has been created and submitted.

This deliverable provides a summary of the progress and results achieved during the first year (M1-M12) of the AI4HEALTHSEC project.

In detail, the first part of this deliverable describes:

Figure 2-27. Screenshot of the 2nd project Newsletter

The second Newsletter of the AI4HEALTHSEC project, focused on the project developments until M11. Specifically, an overview of the 1st Periodic activity report was provided as well as an overview of the developments on the subjects:

- Swarm-inspired Dynamic Situational Awareness Framework;
- Risk and Privacy assessment methodology for the Healthcare ecosystem.

Newsletter 3, February 2022

[View this email in your browser](#)



WP6 has started!

The objective of this work package is to implement pilots and use them to assess in detail whether the technical objectives and KPIs developed on WP2 have been reached.

The 6 pilots will cover the security aspects of:

- Safeguarding Real-Time Patient Monitoring Service
- Medical Implants
- Personal Health Systems with on-body-sensors/actors ('Wearables')
- Human biobanks and related biobank information systems
- Secure Access and Sharing of Clinical Data via VNA and Portal systems
- Digital Health Living Lab



Cybersecurity challenges:

- Close linkage and deep technical integration of all

Figure 2-28. Screenshot of the 3rd project Newsletter

The third Newsletter of the AI4HEALTHSEC project was dedicated to the commencement of activities of WP6.

The objective of this work package is to implement pilots and use them to assess in detail whether the technical objectives and KPIs developed on WP2 have been reached.

The 6 pilots and the involved partners in them were presented:

- Safeguarding Real-Time Patient Monitoring Service;
- Medical Implants;
- Personal Health Systems with on-body-sensors/actors ('Wearables');
- Human biobanks and related biobank information systems;
- Secure Access and Sharing of Clinical Data via VNA and Portal systems;

- Digital Health Living Lab

Note: The commencement of WP6 was also promoted through the social media of the project at the same period.

2.8 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 HCIs.
- **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 performance and operation 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 Description	KPI Goal	Performance at M18
The % of tasks, etc. completed on time according to the action plan.	$\geq 95\%$	100%
The existence of a well-established and functioning community	≥ 10 members (at least)	4
Number of periodic meetings	≥ 6 general meeting	3
Number of workshops	≥ 3	3
Number of contributions to roadmaps, discussion papers	≥ 2	-
Number of contributions to policy-makers	≥ 2	1
Number of external workshops, seminars, etc. attended	≥ 10	7
Number of press releases issued	≥ 4	4
Number of registered members of the project's website	≥ 60	69

KPI Description	KPI Goal	Performance at M18
Number of journal publications	≥ 8	<i>3 published 1 accepted and in press 2 in preparation</i>
Number of conference papers and presentations	≥ 10	<i>2 published 3 accepted and in press 3 in preparation</i>
Number of events attended	≥ 15	9

Table 2-5. KPIs up to M20 (last updated on 18.05.2022)

3 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>