



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"

### **D7.11 – Best Practices and Policy Development Guidelines for Replicability and Wider Use**

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	✓
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	

## **D7.11 – Best Practices and Policy Development Guidelines for Replicability and Wider Use**

### **Editor**

Dmitry Amelin

### **Contributors**

Gabriele Weiler

Kossay Talmoudi

Stylianos Karagiannis

Apostolis Karras

Argyro Chartzopoulou

Spyros Papastergiou

### **Reviewers**

Andreas Alexopoulos

Manos Athanatos



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	06.09.2023	IBMT – Dmitry Amelin	ToC and assignment of tasks to partners
0.2	25.09.2023	TUV – Apostolos Karras, Argyro Chatzopoulou	Contribution to 3. Policy Recommendations
0.3	05.10.2023	IBMT – Gabriele Weiler, Dmitry Amelin	Introduction section and merging contribution to Policy Recommendations section
0.5	21.11.2023	IBMT – Gabriele Weiler PDM - Stylianos Karagiannis PN - Kossay Talmoudi	Contribution to 2. Assessment of Legal and Ethical Considerations Contribution to 5. Lessons Learned and Best Practices/Guidelines
0.6	12.12.2023	IBMT – Dmitry Amelin, Gabriele Weiler PDM – Stylianos Karagiannis CNR - Stefano Silvestri Spyros Papastergiou	Contribution to sections 3.4.5.1, 3.4.5.2, 3.4.5.3 Fix formatting Re-work of Executive Summary and Conclusion based on the received contributions
1.0	22.12.2023	FORTH – Manos Athanatos AEGIS – Andreas Alexopoulos IBMT – Dmitry Amelin PN – Kossay Talmoudi TUV – Argyro Chatzopoulou	Changes according to the reviewers comment.



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**

In the AI4HEALTHSEC project, we've developed an Artificial Intelligence Dynamic Situational Awareness Framework, enhancing the identification and examination of cyber-attacks and threats targeting healthcare infrastructures. Although initially designed for the healthcare sector, the AI4HEALTHSEC platform exhibits broad adaptability, making it viable for application in other domains. Within the project, we executed an open call specifically targeting companies across diverse sectors, such as transportation. This initiative addressed challenges in customizing the platform for non-healthcare domains, providing tailored solutions.

Recognizing the significance of incorporating legal and ethical considerations from the outset in developing such a framework, this deliverable encapsulates evaluations of these considerations. Additionally, it outlines policy recommendations, shares insights on lessons learned during internal pilot operation, and presents best practices and guidelines for AI4HEALTHSEC integration.

## Contents

<b>Executive Summary</b>	<b>4</b>
<b>List of acronyms</b>	<b>6</b>
<b>List of tables</b>	<b>8</b>
<b>List of figures</b>	<b>9</b>
<b>1 Introduction</b>	<b>10</b>
1.1 Scope	10
1.2 Document structure	10
<b>2 Assessment of Legal and Ethical Considerations</b>	<b>12</b>
2.1 Context	12
2.2 Validation against the Legal and Ethical Framework	12
<b>3 Policy Recommendations</b>	<b>14</b>
3.1 Introduction to Policy Recommendations	14
3.2 European Policy Outlook	15
3.3 Identification of Key Topics	19
3.4 Policy Recommendations	25
3.4.1 European Cyber Resilience Act	25
3.4.2 EU CSA	25
3.4.3 Measures for a High Common Level of Cybersecurity at the Institutions, Bodies, Offices and Agencies of the Union	26
3.4.4 Standardization Coverage of the NIS (1)	27
3.4.5 Project Conclusions in the Area of Risk Assessment, AI and Cybersecurity, and Incident Response	29
<b>4 Wider Applicability and Use</b>	<b>33</b>
<b>5 Lessons Learned and Best Practices</b>	<b>36</b>
5.1 Integration Plan	39
<b>6 Conclusion</b>	<b>43</b>
<b>7 Appendix</b>	<b>44</b>
7.1 Feedback on the consultation to the European Cyber Resilience Act	44
7.2 Feedback on the consultation to the amendment of the Cybersecurity Act	61

## List of acronyms

Abbreviation	Definition
AI	Artificial Intelligence
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CER	Critical Entities Resilience Directive
CERT	Computer Emergency Response Team
CG	Cooperation Group
COVID	Coronavirus disease
CS	Cyber Security
CSA	CyberSecurity Act
DNS	Domain Name System
DORA	Digital Operational resilience Act
DSAF	Dynamic Situational Awareness Framework
EC	European Commission
ECSCI	European Cluster for Securing Critical Infrastructures
EEAS	European External Action Service
EMPACT	European Multidisciplinary Platform Against Criminal Threats
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunication Standards Institute
EU	European Union
FAICP	Framework for AI Cybersecurity Practices
GDPR	General Data Protection Regulation
HCII	Health Care Information Infrastructure
ICT	Information and Communication Technology
ID	Identifier
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
KB	Knowledge Base
LLM	Large Language Model
ML	Machine Learning
MSP	Managed Service Provider
NIST	National Institute of Standards and Technology
NL	Natural Language
NLP	Natural Language Processing
OASIS	Organization for the Advancement of Structured Information Standards
SDO	Standard Developing Organizations
SEPIA	Security Enforcement of in Child Psychology sensitive data

Abbreviation	Definition
SME	Small and Medium-sized Enterprise
SOC	Security Operations Centres
UEBA	User and Entity Behavior Analytics
UI	User Interface

## List of tables

TABLE 1 IDENTIFICATION OF RELEVANT TOPICS TO AI4HEALTHSEC PROJECT .....	25
---	----



## List of figures

FIGURE 5-1. SCENARIO RESULTS FROM BIOBANK ON FAILED PASSWORD LOGINS .....	36
FIGURE 5-2. DNS SPOOFING ON TETHYS (PILOT FROM THE OPEN CALL).....	36
FIGURE 5-3. RANSOMWARE ATTACK ON KLINIK .....	37
FIGURE 5-4. PRIVILEGE ESCALATION OR ADMINISTRATIVE COMMAND EXECUTION ON BIOBANK.....	38
FIGURE 5-5. SURVEILLANCE FROM UNAUTHORIZED USAGE OF CAMERA ON SMART GLASSES (LIVINGLABS PILOT).....	38
FIGURE 5-6. DOS ATTACK EXECUTION ON KLINIK.....	39
FIGURE 5-7 INTEGRATION PLAN OF AI4HEALTHSEC PLATFORM. ....	40

## 1 Introduction

### 1.1 Scope

In the AI4HEALTHSEC project an Artificial Intelligence Dynamic Situational Awareness Framework (DSAF) has been developed, which improves the detection and analysis of cyber-attacks and threats on healthcare ICT infrastructures.

The AI4HEALTHSEC platform has been originally designed for the healthcare domain, but due to its broad applicability, we believe it can be adapted for use in other domains with minor modifications. Within the project we conducted an open-call targeting companies in various sectors, such as transportation, to tailor the AI4HEALTHSEC platform to their specific requirements. This open-call aimed to address the challenges encountered when customizing the AI4HEALTHSEC platform for domains different from healthcare and provide solutions to their challenges.

For the development of such a framework it is important that legal and ethical requirements are considered from the beginning. This deliverable summarizes the assessments of the considerations, and additionally reports on policy recommendations, wider applicability, lessons learned, best practices, and guidelines.

This document is the main outcome of the following tasks:

- **Task 7.5** “Legal and Ethical Implementation, Oversight and Evaluation”. Through close collaboration with partners defining system requirements, this task ensures that legal and ethical specifications are integrated into the system design, building upon the outcomes of Task 2.2. Furthermore, it clarifies how the legal framework applies to specific system aspects not addressed earlier. This task conducts a comprehensive assessment of project progress and evaluates developed technologies against the ethical and legal criteria from Task 2.2. Insights gained from technical solutions for compliance with identified requirements will inform Task 7.6 (see below) policy recommendations and guidelines for broader application.
- **Task 7.6** “Policy Recommendations and Guidelines for Wider Applicability and Use”. This task focuses on formulating policy recommendations for public authorities overseeing cybersecurity in healthcare systems, considering both cyber threats and risks. Drawing from earlier legal investigations, it pinpoints legal obstacles hindering the implementation of cyber incident handling systems. Additionally, this task compiles and documents broader operational best practices related to dynamic models for swarm intelligence, incident handling, and healthcare systems. These guidelines will facilitate the successful expansion and application of AI4HEALTHSEC outcomes in other critical information infrastructures, as exemplified by mini-projects within the open-call initiative in WP8. These best practices will also encompass instructions for implementing the AI4HEALTHSEC approach across diverse types of critical information infrastructures, irrespective of size or business activities.

### 1.2 Document structure

The deliverable is structured as following:

- Section “Assessment of Legal and Ethical Considerations” presents the assessment of legal and ethical considerations. It is described how the legal and ethical specifications are duly taken into account in the design of the AI4HEALTHSEC platform.

- Section “Policy Recommendations” describes how the project adopts and uses different standards and provides the reader with a list of the policies.
- Section “Wider Applicability and Use” depicts a wider applicability and use beyond the healthcare domain and especially outlines the open call.
- Section “Lessons Learned and Best Practices” specifies lessons learned, best practice, and guidelines based on internal pilot operation and the open-call.

At the end of the deliverable we summarize and conclude in the “Conclusion” section.

## 2 Assessment of Legal and Ethical Considerations

### 2.1 Context

Throughout its lifecycle, the project is monitored closely from ethical and legal point of view. This is later reflected in a validation process that is elaborated in this section.

In this sense, the task T7.5, “Legal and ethical implementation, oversight, and evaluation”, overarches the progress of WP7 and accompanies the consortium in the implementation of solutions developed in AI4HEALTHSEC in regards to legal and ethical considerations. The lessons learned from T7.5 feed into the T7.6 related to this deliverable.

The assessment of legal and ethical considerations operates in accordance with an already provided deliverable, which is D2.2, titled Legal and Ethical Requirements and which was submitted at M6 of the project’s span.

### 2.2 Validation against the Legal and Ethical Framework

The report on Legal and Ethical Requirements previously referenced, encompasses an array of legal texts as well as standards that the AI4HEALTHSEC project needs to abide by. WP7 underscored, during the project’s deployment phase, the importance accorded to articulating the technologies developed with the legal framework. This legal and ethical compliance is sought after in all new technologies as it renders it more exploitable and sustainable.

Considering the nature of the solutions developed in AI4HEALTHSEC, the report referenced binding and non-binding texts and mechanisms that mainly focused on data protection and data security which the project followed in the development of its technologies. This resulted in an AI4HEALTHSEC solution that is deemed compliant with the essence of the mentioned legal and ethical framework.

The principles of the GDPR were respected in the development and deployment of the AI4HEALTHSEC solutions, this is mirrored, per instance, in the attention accorded to types of data that can be identified in the context of health care infrastructure. In this sense, the utilisation of the AI4HEALTHSEC solution calls for a data mapping that would point out the personal data of patients and its possible processing. The identification of special category data, covered by article 9 of the GDPR is also important in the process of accompaniment of the deployment of the solutions. Data relating to health data of patients should thus be protected robustly in accordance with the GDPR. Data deemed as having a more sensitive nature should then be segregated, as much as technically possible, from the rest of the data contained in the infrastructure. Rights of access to different data sets is, in this sense, conditioned by the presence or not of personal data pertaining to patients. This is manifested in the AI4HEALTHSEC solution through the possibility of tailoring the AI4HEALTHSEC solution to address specific security challenges; this means that specific profiles can be created within the organization putting in place the AI4HEALTHSEC solution allowing limitation of access to data bases based on the organization’s need.

The proper application of cybersecurity policies is also a corner stone in the deployment of the AI4HEALTHSEC solution, with what this entails in terms of reporting of cyber incidences, retention of incident detection repositories, and overall high standards of cybersecurity in the organization. This aligns with the strategic cybersecurity framework of the European Union which presents more and more incentives for an efficient reporting and pooling of resources.

The legal framework also references principles guiding legislation and standards such as the Ethics Guidelines for Trustworthy Artificial Intelligence or the upcoming AI act, this is manifested in the solution through the continuous oversight that is set to accompany deployment of the AI4HEALTHSEC solution in various organization, this oversight thus covers the AI component and coincides with an explainable AI solution.

Overall, the legal and ethical framework previously detailed has been taken rigorously into consideration while developing and implementing the AI4HEALTHSEC solutions. This resulted in a set of lessons learned that also feed into the policy recommendations detailed hereafter.

## 3 Policy Recommendations

### 3.1 Introduction to Policy Recommendations

The European Commission has articulated and set the priorities for the years 2019-2024. These priorities<sup>1</sup> are the following:

- A European Green Deal
- A Europe fit for the digital age
- An economy that works for people
- A stronger Europe in the world
- A new push for European democracy

As part of the activities related to the priority “Shaping Europe’s digital future”, the European Commission underlines the need for digital solutions<sup>2</sup> that:

- open up new opportunities for businesses;
- encourage the development of trustworthy technology;
- foster an open and democratic society;
- enable a vibrant and sustainable economy;
- help to fight climate change and achieve the green transition.

The protection of people from cyber threats (e.g., hacking, ransomware, identity theft), is one of the three pillars to support this approach.

The EU is working on various fronts to promote cyber resilience, fight cybercrime, and boost cyber diplomacy and defence<sup>3</sup>.

In an effort to provide feedback to relevant policies and authorities within the EU on the subjects related to those of the project, a four step methodology has been devised and followed by the AI4HEALTHSEC project.

**Step 1: Identification of policy instruments.**

During this step, the project reviewed the policy instruments and activities related to cybersecurity at EU level.

**Step 2: Selection of the most related policy instruments.**

A number of policy instruments identified within step 1 are selected based on their relevance to cybersecurity.

**Step 3: Identification of topics.**

For each one of the policy instruments, the main topics are identified (mostly in the form of keywords).

**Step 4: Identification of relevance and provision of recommendations, comments and feedback.**

---

<sup>1</sup> [https://commission.europa.eu/strategy-and-policy/priorities-2019-2024\\_en](https://commission.europa.eu/strategy-and-policy/priorities-2019-2024_en)

<sup>2</sup> [https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/shaping-europes-digital-future\\_en](https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/shaping-europes-digital-future_en)

<sup>3</sup> <https://www.consilium.europa.eu/en/policies/cybersecurity/>

The relevance of the policy instruments (based on the topics covered) to the outcomes and experiences of the AI4HEALTHSEC project is identified and relevant opportunities for interaction are monitored by the project.

Where possible, the AI4HEALTHSEC project, shall provide feedback following the above selection methodology or ad-hoc should an opportunity arise.

The following sub-sections provide an overview of the results of the implementation of the above stepped methodology.

### 3.2 *European Policy Outlook*

As mentioned above, the EU is working on various fronts to promote cyber resilience, fight cybercrime, and boost cyber diplomacy and defence.

From all the activities and initiatives, the AI4HEALTHSEC project has singled out the following 17 instruments and activities at a European level:

1. In December 2020, the European Commission and the European External Action Service (EEAS) presented a new *EU cybersecurity strategy*<sup>4</sup>. The aim of this strategy is to strengthen Europe's resilience against cyber threats and ensure that all citizens and businesses can fully benefit from trustworthy and reliable services and digital tools. On 22 March 2021, the Council adopted conclusions on the cybersecurity strategy, underlining that cybersecurity is essential for building a resilient, green and digital Europe.
2. The *EU cybersecurity act*<sup>5</sup> entered into force in June 2019 and introduced: an EU-wide certification scheme and a new and stronger mandate for the EU agency for cybersecurity (ENISA).
3. Certification plays a critical role in ensuring high cybersecurity standards for ICT products, services and processes. The fact that different security certification schemes are currently used by different EU countries generates market fragmentation and regulatory barriers. With the cybersecurity act, the EU has introduced a single *EU-wide certification framework*<sup>6</sup> that: build trust, increase the cybersecurity market's growth, ease trade across the EU. The framework provides a comprehensive set of rules, technical requirements, standards and procedures.
4. The *new EU agency for cybersecurity*<sup>7</sup> builds on the structures of its predecessor, the European Union agency for network and information security, but with a strengthened role and a permanent mandate. It has also adopted the same acronym (ENISA). It supports member states, EU institutions and other stakeholders in dealing with cyberattacks.
5. The directive on the security of network and information systems (NIS) was introduced in 2016 as the first ever EU-wide legislative measure with the purpose of increasing cooperation between member states on the vital issue of cybersecurity. It laid down security obligations for operators of essential services (in critical sectors such as energy, transport, health and

<sup>4</sup> <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy>

<sup>5</sup> <https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act>

<sup>6</sup> <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework>

<sup>7</sup> <https://www.enisa.europa.eu/>

finance) and for digital service providers (online marketplaces, search engines and cloud services). The EU adopted in 2022 a *revised NIS directive (NIS2)*<sup>8</sup> to replace the 2016 directive. The new rules ensure a high common level of cybersecurity across the Union, responding to the evolving threat landscape and taking into account the digital transformation, which has been accelerated by the COVID-19 pandemic. The new EU law: sets new minimum rules for a regulatory framework, lays down mechanisms for effective cooperation among relevant authorities in each EU country and updates the list of sectors and activities subject to cybersecurity obligations.

6. The EU wants to introduce mandatory cybersecurity requirements for hardware and software products with a connected digital element (such as smart TVs or other home appliances, baby monitors, toys). The proposed regulation (*Cyber resilience act*) ensures that businesses and consumers are effectively protected against cyber threats.<sup>9</sup> In July 2023, Member states' representatives (COREPER) reached a common position on the proposed legislation regarding horizontal cybersecurity requirements for products with digital elements (cyber resilience act).<sup>10</sup> The proposed new rules want to ensure that products with digital components, such as connected home cameras, smart fridges, TVs, and toys, are safe before entering the EU single market.
7. A specialised *European cybercrime center* has been created within Europol<sup>11</sup> to help EU countries investigate online crimes and dismantle criminal networks. The European multidisciplinary platform against criminal threats (EMPACT) is a security initiative driven by member states to identify, prioritise and address threats posed by organised international crime. Countering cyberattacks is one of its priorities.
8. Fraud and counterfeiting involving non-cash means of payment pose a serious threat to the EU's security and provide a significant income for organised crime. Moreover, this kind of fraud affects the trust of consumers in the security of digital technologies. In April 2019, the EU adopted *new rules to fight non-cash payment fraud*. Member states should implement the new rules in 2021.<sup>12</sup>
9. In May 2019, the Council established a *framework* which allows the EU to impose targeted *sanctions to deter and respond to cyberattacks* which constitute an external threat to the EU or its member states. More specifically, this framework allows the EU for the first time to impose sanctions on persons or entities that are responsible for cyberattacks or attempted cyberattacks, who provide financial, technical or material support for such attacks or who

---

<sup>8</sup> <https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/eu-decides-to-strengthen-cybersecurity-and-resilience-across-the-union-council-adopts-new-legislation/>

<sup>9</sup> <https://www.consilium.europa.eu/en/press/press-releases/2023/07/19/cyber-resilience-act-member-states-agree-common-position-on-security-requirements-for-digital-products/>

<sup>10</sup> <https://www.consilium.europa.eu/en/press/press-releases/2023/07/19/cyber-resilience-act-member-states-agree-common-position-on-security-requirements-for-digital-products/>

<sup>11</sup> <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3>

<sup>12</sup> <https://www.consilium.europa.eu/en/press/press-releases/2019/04/09/eu-puts-in-place-tighter-rules-to-fight-non-cash-payment-fraud/>



are involved in other ways. Sanctions may also be imposed on other persons or entities associated with them.<sup>13</sup>

10. Connected devices, including machines, sensors and networks that make up the Internet of Things (IoT), will play a key role in further shaping Europe's digital future, and so will their security. In December 2020, the Council adopted conclusions acknowledging the increased use of *consumer products and industrial devices connected to the internet* and the related *new risks for privacy, information security and cybersecurity*. The conclusions set out priorities to address this crucial issue and to boost the global competitiveness of the EU's IoT industry by ensuring the highest standards of resilience, safety and security.<sup>14</sup>
11. The Council and the European Parliament reached a provisional agreement on the *Digital Operational Resilience Act (DORA)*<sup>15</sup>, which will make sure the financial sector in Europe is able to maintain resilient operations through a severe operational disruption. DORA creates a regulatory framework on digital operational resilience whereby all firms need to make sure they can withstand, respond to and recover from all types of ICT-related disruptions and threats. The EU is strengthening the IT security of financial entities such as banks, insurance companies and investment firms, given the ever-increasing risks of cyber-attacks.
12. The Council adopted conclusions calling for *stronger security of the EU's information and communication technologies (ICT) supply chains*. The conclusions also address dependencies in ICT supply chains. The call for action is even more urgent in the context of Russia's aggression to Ukraine. In the conclusions, the Council calls for adjustments to public procurement or foreign direct investment screening frameworks, including cybersecurity-related selection criteria. Member states invited the Commission to issue methodological guidelines to encourage contracting authorities to put appropriate focus on the cybersecurity practices of tenderers and their subcontractors.<sup>16</sup>
13. The Council has adopted its position on a *common framework for cybersecurity at EU institutions, bodies, offices and agencies*. Against the backdrop of increased numbers of sophisticated cyberattacks against the EU public administration, in March 2022 the European Commission proposed measures aimed at ensuring a high common level of cybersecurity. By creating a common framework, these measures set out to improve the resilience and incident response capacities of all EU entities and to address differences in their approach.<sup>17</sup> In June 2023, the Council of the EU and the European Parliament have struck a provisional deal on a common framework for cybersecurity at the EU institutions, bodies, offices and agencies. The

<sup>13</sup> <https://www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/>

<sup>14</sup> <https://www.consilium.europa.eu/en/press/press-releases/2020/12/02/cybersecurity-of-connected-devices-council-adopts-conclusions/>

<sup>15</sup> <https://www.consilium.europa.eu/en/press/press-releases/2022/05/11/digital-finance-provisional-agreement-reached-on-dora/>

<sup>16</sup> <https://www.consilium.europa.eu/en/press/press-releases/2022/10/17/the-council-agrees-to-strengthen-the-security-of-ict-supply-chains/>

<sup>17</sup> <https://www.consilium.europa.eu/en/press/press-releases/2022/11/18/cybersecurity-at-the-eu-institutions-bodies-offices-and-agencies-council-adopts-its-position-on-common-rules/>

deal will help improve their resilience and incident-response capacities, and ensure common standards and cooperation. Next, the deal will be finalised at technical level and then sent to EU ambassadors for confirmation. Once confirmed in both the Council and the Parliament, both institutions will formally adopt it.

14. In April 2021, the European Commission proposed the first EU regulatory framework for AI. It says that AI systems that can be used in different applications are analysed and classified according to the risk they pose to users. The different risk levels will mean more or less regulation. In June 2023, the European Parliament has approved its negotiating position on the proposed [Artificial Intelligence Act](#).<sup>18</sup>
15. The proposed [FAICP framework](#)<sup>19</sup> is the response from the European Union Agency for Cybersecurity (ENISA) to the EU Artificial Intelligence Act ("AI Act"), that lays down harmonised rules for the placing on the market, the putting into service, and the use of artificial intelligence systems in the European Union. The FAICP is a framework for AI good cybersecurity practices necessary for securing the ICT infrastructures and the hosted AI, taking into account the AI life cycle (from system concept to decommissioning), and all elements of the AI supply chain, associated actors, processes and technologies.
16. In 2020 the Commission proposed a significant upgrade to the EU's rules on the resilience of critical entities and the security of network and information systems. On 16 January, two key directives on critical and digital infrastructure entered into force with the purpose of strengthening the EU's resilience against online and offline threats, from cyberattacks to crime, risks to public health or natural disasters – the Directive on the resilience of critical entities (CER Directive) and the Directive on measures for a high common level of cybersecurity across the Union (NIS 2 Directive)<sup>20</sup>. In July 2023, the Commission has adopted a list of essential services in the eleven sectors covered by the [Critical Entities Resilience Directive \(CER\)](#)<sup>21</sup>, which entered into force on 16 January 2023. Critical entities provide essential services in upholding key societal functions, supporting the economy, ensuring public health and safety, and preserving the environment.
17. In April 2023, the European Commission introduced a proposal for a [Cyber Solidarity Act](#), in an effort to improve the preparedness, detection and response to cybersecurity incidents across the EU. The EU framework comprises several legislations already in place or proposed at Union level to reduce vulnerabilities, increase the resilience of critical entities against cybersecurity risks and support the coordinated management of large-scale cybersecurity incidents and crises, notably: the Directive on measures for a high common level of security of network and information systems across the Union (NIS 2), the Cybersecurity Act (Regulation (EU) 2019/881), the Directive on attacks against information systems (Directive 2013/40/EU), the Commission Recommendation (EU) 2017/1584 on coordinated response to large-scale cybersecurity incidents and crises. The actions proposed under the Cyber Solidarity Act cover situational awareness, information sharing, as well as support for preparedness and

<sup>18</sup> <https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence>

<sup>19</sup> <https://www.enisa.europa.eu/publications/multilayer-framework-for-good-cybersecurity-practices-for-ai>

<sup>20</sup> [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_23\\_3992](https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3992)

<sup>21</sup> <https://eur-lex.europa.eu/eli/dir/2022/2557/oj>

response to cyber incidents. The Cyber Solidarity Act will especially build on and support the existing cybersecurity operational cooperation and crisis management frameworks, in particular the European Cyber Crisis Liaison Organisation Network (EU-CyCLONe) and the Computer Security Incident Response Teams (CSIRTs) network. The cross-border Security Operations Centres (SOC) will constitute a new capability that is complementary to the CSIRTs network, by pooling and sharing data on cybersecurity threats from public and private entities, enhancing the value of such data through expert analysis and state of the art tools, and contributing to the development of Union capabilities and technological sovereignty<sup>22</sup>.

### 3.3 Identification of Key Topics

During the 3rd step of the methodology described in Section 3.1, the project team identified the main topics of each one of selected instruments, as well as the relevant of these topics to the outcomes and experiences of the AI4HEALTHSEC project (Table 1).

European Policy Instrument	Topics covered	Topics relevant to the AI4HEALTHSEC project
EU cybersecurity strategy	<ul style="list-style-type: none"> <li>• Resilient infrastructure and critical services.</li> <li>• Security operations centres.</li> <li>• Ultra-secure communication infrastructure.</li> <li>• Securing the next generation of broadband mobile networks.</li> <li>• An Internet of Secure Things.</li> <li>• Greater global Internet security.</li> <li>• A reinforced presence on the technology supply chain.</li> <li>• A Cyber-skilled EU workforce.</li> <li>• operational and technical</li> <li>• Coordination against major cross border cyber incidents and threats.</li> <li>• Tackling cybercrime.</li> <li>• EU cyber diplomacy toolbox.</li> <li>• Boosting cyber defence capabilities.</li> <li>• EU leadership on standards, norms and frameworks in cyberspace.</li> <li>• Cooperation with partners and the multi-stakeholder community.</li> </ul>	<ul style="list-style-type: none"> <li>• Resilient infrastructure and critical services.</li> <li>• A Cyber-skilled EU workforce.</li> <li>• Coordination against major cross border cyber incidents and threats.</li> <li>• EU leadership on standards, norms and frameworks in cyberspace.</li> <li>• Common binding rules on information security and for common binding rules on cybersecurity for all EU institutions, bodies and agencies.</li> <li>• Increase CERT-EUs ability to help EU institutions, bodies and agencies to apply the new cybersecurity rules, improve their cyber resilience</li> </ul>

<sup>22</sup> <https://www.eu-cyber-solidarity-act.com/>

European Policy Instrument	Topics covered	Topics relevant to the AI4HEALTHSEC project
	<ul style="list-style-type: none"> <li>Strengthening global capacities to increase global resilience.</li> <li>Rules for the protection of EU classified information as well as sensitive non-classified information.</li> <li>Common binding rules on information security and for common binding rules on cybersecurity for all EU institutions, bodies and agencies.</li> <li>Increase CERT-EUs ability to help EU institutions, bodies and agencies to apply the new cybersecurity rules, improve their cyber resilience</li> </ul>	
EU cybersecurity act	EU-wide certification scheme and a new and stronger mandate for the EU agency for cybersecurity (ENISA).	Workings of the Cybersecurity Certification Framework for ICT products and services
EU-wide certification framework	<ul style="list-style-type: none"> <li>Build trust, increase the cybersecurity market's growth, ease trade across the EU.</li> <li>Provides a comprehensive set of rules, technical requirements, standards and procedures</li> </ul>	Workings of the Cybersecurity Certification Framework for ICT products and services
New EU agency for cybersecurity	Supports member states, EU institutions and other stakeholders in dealing with cyberattacks.	Incident response / cyberattacks
Revised NIS directive (NIS2)	<ul style="list-style-type: none"> <li>Ensure a high common level of cybersecurity across the Union.</li> <li>Responding to the evolving threat landscape.</li> <li>Taking into account the digital transformation.</li> <li>Sets new minimum rules for a regulatory framework.</li> <li>Lays down mechanisms for effective cooperation among relevant authorities in each EU country.</li> </ul>	<ul style="list-style-type: none"> <li>Measures related to incident preparedness and response</li> <li>Risk assessment</li> </ul>

European Policy Instrument	Topics covered	Topics relevant to the AI4HEALTHSEC project
	<ul style="list-style-type: none"> <li>Updates the list of sectors and activities subject to cybersecurity obligations.</li> </ul>	
Cyber Resilience Act	<ul style="list-style-type: none"> <li>Cybersecurity requirements for hardware and software products with a connected digital element.</li> <li>Ensures that businesses and consumers are effectively protected against cyber threats.</li> </ul>	<ul style="list-style-type: none"> <li>Risk assessment</li> <li>Certification of hardware and software products with a connected digital element</li> </ul>
European Cybercrime Centre	Identify, prioritise and address threats posed by organised international crime. Countering cyberattacks is one of its priorities.	-
New rules to fight non-cash payment fraud	<ul style="list-style-type: none"> <li>Harmonised definitions of some online crime offences, such as hacking a victim's computer or phishing.</li> <li>Harmonised rules on penalties for natural persons: five, four or three years of prison, depending on the offence, as the minimum penalty in cases where a judge imposes the national "maximum" custodial sentence for non-cash payment fraud.</li> <li>Assistance and support to ensure victims are sufficiently informed of their rights and citizens are advised on how to protect themselves from such frauds.</li> <li>Clarification of the scope of jurisdiction to ensure cross border fraud is tackled more effectively.</li> </ul>	-
Sanctions to deter and respond to cyberattacks	Impose targeted restrictive measures to deter and respond to cyber-attacks which constitute an external threat to the EU or its member states.	-

European Policy Instrument	Topics covered	Topics relevant to the AI4HEALTHSEC project
Internet of Things (IoT)	The Council adopted conclusions acknowledging the increased use of consumer products and industrial devices connected to the internet and the related new risks for privacy, information security and cybersecurity. The conclusions set out priorities to address this crucial issue and to boost the global competitiveness of the EU's IoT industry by ensuring the highest standards of resilience, safety and security.	-
Digital Operational Resilience Act (DORA)	<ul style="list-style-type: none"> <li>• DORA sets uniform requirements for the security of network and information systems of companies and organisations operating in the financial sector as well as critical third parties which provide ICT (Information Communication Technologies)-related services to them, such as cloud platforms or data analytics services.</li> <li>• DORA creates a regulatory framework on digital operational resilience whereby all firms need to make sure they can withstand, respond to and recover from all types of ICT-related disruptions and threats.</li> <li>• Prevent and mitigate cyber threats.</li> <li>• Develop technical standards for all financial services institutions to abide by, from banking to insurance to asset management.</li> </ul>	-
ICT supply chain security	<ul style="list-style-type: none"> <li>• Specific actions for strengthening ICT supply chain security aspects of existing instruments, such as public procurement or foreign direct investment screening frameworks.</li> </ul>	Risk assessment and supply chain risk assessment

European Policy Instrument	Topics covered	Topics relevant to the AI4HEALTHSEC project
	<ul style="list-style-type: none"> <li>• How existing and upcoming cyber-specific legislation can contribute to ICT supply chain security.</li> <li>• Use of supporting mechanisms for financing secure digital infrastructure building.</li> <li>• Enhance common understanding and awareness.</li> <li>• Increase ICT supply chain security in the EU and beyond.</li> <li>• Creation of an ICT Supply Chain Toolbox that would consist of generic measures for reducing critical ICT supply chain risks.</li> <li>• Facilitate the implementation of coordinated risk assessments of critical supply chains under the NIS2 Directive.</li> </ul>	
Common framework for cybersecurity at EU institutions, bodies, offices and agencies	<ul style="list-style-type: none"> <li>• Improve the resilience and incident response capacities of all the EU entities.</li> <li>• Address the disparities in their approach by creating a common framework.</li> <li>• Strengthening the mandate and funding of the Computer Emergency Response Team for the EU institutions, bodies, offices and agencies (CERT-EU).</li> <li>• Setting up an interinstitutional Cybersecurity Board to drive and oversee the implementation of the new regulation.</li> <li>• Strengthening incident-related information sharing with CERT-EU.</li> <li>• Promoting coordination and cooperation in response to cyber incidents.</li> </ul>	Risk assessment



European Policy Instrument	Topics covered	Topics relevant to the AI4HEALTHSEC project
Artificial Intelligence Act	<ul style="list-style-type: none"> <li>• Ensure the proper functioning of the single market by creating the conditions for the development and use of</li> <li>• Trustworthy AI systems in the Union.</li> <li>• Ensure that AI systems placed on the EU market are safe and respect existing EU law.</li> <li>• Ensure legal certainty to facilitate investment and innovation in AI.</li> <li>• Enhance governance and effective enforcement of EU law on fundamental rights and safety requirements applicable to AI systems.</li> <li>• Facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation.</li> </ul>	<ul style="list-style-type: none"> <li>• Risk assessment</li> <li>• Cybersecurity and AI</li> </ul>
FAICP framework	<p>The FAICP is a scalable 3-layered framework:</p> <p>The key elements of this layer are: security management of the ICT infrastructure hosting AI systems; security management; cybersecurity certification; cybersecurity legislation and policies that affect AI systems.</p> <p>The third layer of the FAICP framework provides additional recommendations and best practices available in order to address cybersecurity issues in the AI systems used in some of these sectors. (Energy, Health, Automotive, Telecommunications)</p>	<ul style="list-style-type: none"> <li>• Risk assessment</li> <li>• Cybersecurity and AI</li> </ul>
Critical Entities Resilience Directive (CER)	Strengthening the EU's resilience against online and offline threats, from cyberattacks to crime, risks to public health or natural disasters.	Risk assessment



European Policy Instrument	Topics covered	Topics relevant to the AI4HEALTHSEC project
Cyber Solidarity Act	<ul style="list-style-type: none"> <li>Preparedness, detection and response to cybersecurity incidents across the EU.</li> <li>Coordinated management of large-scale cybersecurity incidents and crises.</li> </ul>	Preparedness, detection and response to cybersecurity incidents across the EU.

Table 1 Identification of relevant topics to AI4HEALTHSEC project

### 3.4 Policy Recommendations

#### 3.4.1 European Cyber Resilience Act

In March 2022, the European Commission launched a public consultation to gather the views and experiences of all relevant parties on the forthcoming European Cyber Resilience Act.

Specifically, the consultation aimed to gather the views of a variety of stakeholders. These include:

- ICT industry representatives (e.g. hardware manufacturers, software developers, distributors, importers) and professional users;
- national competent authorities, including cybersecurity-relevant authorities;
- consumers and consumer associations;
- conformity assessment bodies;
- academic experts and the general public.

Through this consultation, the Commission would like to gather:

- stakeholders' views on current and emerging problems related to the cyber security of digital products and associated services, including non-embedded software;
- stakeholders' views on the possible policy approaches to address such problems, the available options and their potential impacts; and
- evidence and data underpinning the identified problems.

The AI4HEALTHSEC project comprises from ICT industry representatives, academic experts and professional users, focusing on a solution related to cybersecurity within the HealthCare domain. As such, the AI4HEALTHSEC project believes that it has useful feedback, opinions and experience on the specific subject and decided to participate in this consultation.

The response to the consultation was submitted on the 25<sup>th</sup> of May 2022 at 22:16:05, with Contribution ID: 16af12fb-e733-4117-8169-4d0d8ab511fc. The feedback provided is included in the Appendix of this document in Section: Feedback on the consultation to the European Cyber Resilience Act.

#### 3.4.2 EU CSA

In April 2023, the European Commission launched a public consultation to gather the views and experiences of all relevant parties on a proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2019/881 as regards managed security services.

Specifically, the consultation provided the proposal document COM(2023) 208 final and asked interested parties to comment on the changes imposed to the regulation 2019/881 by the addition of Managed Security Services.

The AI4HEALTHSEC project comprises from ICT industry representatives, academic experts and professional users, focusing on a solution related to cybersecurity within the HealthCare domain. Also, the solution proposed by the project can facilitate the provision of a managed security service, as such, the AI4HEALTHSEC project believes that it has useful feedback, opinions and experience on the specific subject and decided to participate in this consultation.

The response to the consultation was submitted on the 20<sup>th</sup> of July 2023 at 17:54, with Feedback reference: F3430725.

The feedback provided is included in the Appendix of this document in Section: Feedback on the consultation to the amendment of the Cybersecurity Act.

### **3.4.3 Measures for a High Common Level of Cybersecurity at the Institutions, Bodies, Offices and Agencies of the Union**

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<sup>23</sup>, provided their opinion on selected provisions of the regulation.

The position document contains comments of the AI4HEALTHSEC & HEIR projects on parts of the following Articles: 4,5,7,8,9,11,12,13,14 and Chapter V of the draft (at that time) 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.

The document<sup>24</sup> has been included in the articles section of the project and has been promoted through the relevant communication channels of the project.

Some of the key points of the position paper, as they relate also to the key topics of the project were the following:

1. On the subject of risk management, that guidance on the minimum components of the cybersecurity risk management, governance and control framework as well as information on the methodologies and standards related to this subject should be provided to the Institutions, Bodies, offices and Agencies of the Union.
2. On the subject of the Cybersecurity Baseline, that the domains covered by the baseline should also include Privacy by Design and extend the cybersecurity training to the top management of the organizations. The subject of privacy and the inclusion of GDPR compliance is also mentioned throughout the document.
3. On the subject of Maturity Assessments, that the text included in the proposal for regulation does not provide enough information for the cybersecurity maturity concept understanding

---

<sup>23</sup> <https://heir2020.eu/>

<sup>24</sup> [https://www.ai4healthsec.eu/wp-content/uploads/Position-Paper\\_Reg\\_EU\\_institutions.pdf](https://www.ai4healthsec.eu/wp-content/uploads/Position-Paper_Reg_EU_institutions.pdf)

and implementation and as such should be enriched and guidance should be provided to the Institutions, Bodies, offices and Agencies of the Union.

4. On the subject of Cybersecurity plans that an awareness and collaboration-based methodology and tool set designed to implement and operationalize the cooperation/collaboration-based cybersecurity framework defined by the European cybersecurity strategy and subsequent legislation like NIS/NIS2 and GDPR.
5. On the subject of CERT-EU mission and tasks, that minimum requirements that cyber threat intelligence, including situational awareness, methodologies should comply with should be provided.

The regulation 2023/2841 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, was published on the 13<sup>th</sup> of December 2023<sup>25</sup>.

A review of the published regulation was implemented and when compared to the positions and recommendations of the AI4HEALTHSEC project the following conclusions were extracted:

- **Article 4:** The previous article 4 has been replaced by provisions related to the processing of personal data. This has been stated in the position document of the Ai4HealthSec project, as discussed in point 2 above.
- **Article 5:** The previous article 5 has been replaced by provisions related to the implementation of measures. Specifically, this article mandates that “By 8 September 2024, the Interinstitutional Cybersecurity Board established pursuant to Article 10 shall, after consulting the European Union Agency for Cybersecurity (ENISA) and after receiving guidance from CERT-EU, issue guidelines to Union entities for the purpose of carrying out an initial cybersecurity review and establishing an internal cybersecurity risk-management, governance and control framework pursuant to Article 6, carrying out cybersecurity maturity assessments pursuant to Article 7, taking cybersecurity risk-management measures pursuant to Article 8, and adopting the cybersecurity plan pursuant to Article 9”. This has been stated in the position document of the AI4HEALTHSEC project, as discussed in points 1 and 3 above.
- **Article 8:** This article provides the domains of cybersecurity risk-management measures. Within the minimum measures prescribed, the following has been included “the establishment and adoption of training programs on cybersecurity commensurate to the prescribed tasks and expected capabilities for the highest level of management and members of staff of the Union entity tasked with ensuring the effective implementation of this Regulation, as stated in the position document of the Ai4HealthSec project, as discussed in point 2 above.

### 3.4.4 Standardization Coverage of the NIS (1)

In preparation of the implementation of the project work, the project team of the AI4HEALTHSEC, ran an analysis of existing and developing standards in the focus areas of the project. The objective of this analysis was to become acquainted with the state of the art, to collect valuable information, to build upon them and to identify possible shortcomings.

---

<sup>25</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R2841>

After the initial analysis that provided the foundation for the first deliverables of the project, the project team decided to enrich this analysis and map standards to all the proposed measures of the NIS Cooperation Group (Reference document on security measures for Operators of Essential Services, CG Publication 01/2018 [NIS 2018]).

The analysis was implemented according to the following parameters:

- The SDOs (Standard Developing Organizations) that were included in the analysis were at least the following: CEN and CENELEC, ETSI (CYBER), IEC, OASIS, ISO/IEC, IEEE, NIST. (Some exceptions of other SDO's were allowed in cases where a specific standard on the subject is well known or recognized.)
- To these SDOs, organizations like ENISA and specific Cybersecurity Authorities were added, since it was found that specific guidance documents were provided specifically on the subject of Network and Information Security.
- The standards identified are in their majority not sector specific.
- The standards identified are in their majority not technology specific.
- The standards identified are viewed from the perspective of the provision of guidance to the organizations (independent of size). This means that standards presenting the scientific basis of a security measure were not included. E.g., For the Cryptography security measure, standards like ISO/IEC 15946-1:2016 Cryptographic Techniques Based on Elliptic Curves -- Part 1: General [ISO-IEC 2016] (standard that describes the mathematical background and general techniques necessary for implementing the elliptic curve cryptography mechanisms) are not included. Whereas NIST, SP 800-57 Part 1 Revision 5 – General, cryptographic key management guidance [SP 800-57 2020] was included since it provides guidance on key management practices.

The analysis performed and described above, revealed that there is a variance in the number of standards that exist per security measure as proposed by the “Reference document on security measures for Operators of Essential Services, CG Publication 01/2018” [NIS 2018].

There are areas where a high number of standards were identified by the project team, e.g., information system security risk analysis, industrial control systems, and authentication and identification and other areas where a low number of standards were identified by the project team e.g. crisis management organization and disaster recovery management.

It is the opinion of the project team that the following should be carried out in support of the NIS compliance:

- Conduct further analysis on the reasons behind these fluctuations. This would allow for the implementation of solutions that would fit the cause of the problem and provide value to the entire market
- Conduct studies on the interoperability among standards that cover the same area (like INTEROPERABLE EU RISK MANAGEMENT FRAMEWORK). These studies will provide the market with a way to correlate between the different standards and provide also the policy makers and SDOs with information on existing gaps and opportunities for improvement.
- Especially for the areas where a limited number of standards have been identified, the SDOs and other interested parties should further investigate the situation and develop specific standards to fill these gaps if needed.

- Further research needed to promote the direct communication between the stakeholders, by facilitating security-related information sharing through standards and decentralized coordination and improving the overall cyber-situational awareness of the digital ecosystem.
- The digital SC ecosystems raise the need for advanced self-healing and self-repairing processes, which facilitate the automatic recovery and reconfiguration of their IT/OT components in order to guarantee the business continuity in the IT-interconnected networks. In this context, further research needed to improve the cybersecurity practices, enhance the business continuity and disaster recovery processes of the digital infrastructures by empowering them with new advanced self-healing capabilities.
- Finally, and in alignment to the rolling plan for ICT standardization, efforts should be invested in the identification, development and communication in an easy and straight forward way of standards for SMEs.

The analysis and results described above were presented during the second ECSCI Workshop on critical infrastructure protection and resilience, and the work was published within the relevant proceedings. The document can be accessible through the project website at: <https://www.ai4healthsec.eu/standards-and-nis-compliance-2/>.

### **3.4.5 Project Conclusions in the Area of Risk Assessment, AI and Cybersecurity, and Incident Response**

#### **3.4.5.1 Risk Assessment**

The healthcare sector is heavily relying on the digital technologies which provide significant benefits including more efficient and coordinated service delivery, higher degree of flexibility, scalability of the overall infrastructure. Despite of these benefits, healthcare information infrastructure is now more complex with growing interconnectivity among different sub-systems that creates possible attack surfaces for any potential risk. Cyber-attack from any part of the system can propagate to the other parts of the overall healthcare ecosystem that can pose disruption for the healthcare service delivery. There is a need for an effective risk management practice based on the actual observations of events within a specific context so that appropriate informed decision can be taken to tackle the risks and related threats and vulnerabilities.

The output of the EU AI4HEALTHSEC project proposes a novel cybersecurity risk management method based on the actual observation of the evidence from the healthcare information infrastructure for an effective risk management practice and common situational awareness. The actual observations of the security events within the healthcare ecosystem context considers occurrence of threats from the various published data sources, indicator of attack and compromise, vulnerability exploitation, incidents, existing controls, and others. There are following unique contributions beyond the existing risk assessment and management method.

- Evidence based cybersecurity risk management to assess and manage risk based on the observation of events taken in account possible assets and their dependencies within the healthcare ecosystem.
- Adoption of Natural Language Processing (NLP) techniques to identify and assess possible threats that are relevant within the healthcare context. The threat levels are used to quantify and prioritise the risk.

- Generation of attack path based on the dependencies among the assets and underlying vulnerabilities that are propagated within the dependent asset. This allows to calculate cascading risks besides individual risks within the healthcare eco system context.
- Evaluate the applicability of the work based on the real-world healthcare scenario offered by the consortium partner.

Healthcare sector needs resilience for delivering the critical services relating to patient treatment support and ensuring security is paramount important to achieve resilience. Evidence based approach supports improvement of the overall cybersecurity capability in terms of understanding risks and existing controls so that informed decision can be taken for the overall security improvement. However, for an effective risk management practice, it is necessary to consider dynamic behaviour of the collected evidence. In particular, the values of the several evidence such as log and threat feed data, control effectiveness, and vulnerability level can be constantly changing. Therefore, it is necessary to re-estimate the risk values considered the continuous evolution of the critical evidence. Additionally, a control taxonomy to link with the sector specific risks for the overall cyber security improvement would be effective to risk mitigation. Finally, we are also planning to deploy the proposed method into different sector context to evaluate the applicability of the evidence-based risk management method.

#### 3.4.5.2 AI and Cybersecurity

The massive digitization in the healthcare ecosystems provides many benefits, but it increases the cyber security issues and challenges related to the high number of systems, software, and assets, causing an increased attack surface where threat actors can exploit possible threats for any potential risk within the Health Care Information Infrastructure (HCII). Threats and vulnerabilities analysis in the healthcare sectors is a challenging task, due to the large number of published reports and databases. Moreover, also a huge amount of unstructured Natural Language (NL) Cyber Security (CS) data related to the healthcare domain is freely available on the Web, containing crucial and constantly updated data related to the assets of the HCII, including threats, vulnerabilities, attacks, and other important information, which could be very useful to improve the protection of the HCIIs. But, also in this case, it is difficult to identify and extract the relevant information from such kinds of texts, which are usually available on blog posts, CS news websites, social media, and other similar not-structured sources. Therefore, it is hard to define specific methodologies able to mine and extract the required information, namely updated CS threats and vulnerabilities, from this huge amount of information available buried under that huge amount of textual data. Therefore, even if NL documents on the Internet can support the establishment of situational awareness proactively monitoring and preventing CS issues, innovative and tailored approaches are required.

The results obtained during the development of the AI4HEALTHSEC project proposed innovative AI-based approaches for the CS domain. The main novelty of these methods is related to the use of Natural Language Processing (NLP) techniques applied to the cyber security domain. In detail, we developed the following AI-based methods and resources:

- A threat assessment NLP method, based on a Large Language Model (LLM) pre-trained on the cybersecurity domain and fine-tuned to the Named Entity Recognition task. This method is specifically tailored to extract the mentions of threats and assets from huge natural language documents available on the Internet (such as news, social media, forums, etc.), mapping them



to the HCII assets and calculating the threat's level exploiting the frequency of their mention within the considered dataset. The method is also capable to prioritize the corresponding risk and to identify possible mitigation actions.

- A constantly updated big dataset formed by NL CS news, periodically crawled from a web news platform that attracts over eight million readers monthly, which is daily updated with the latest CS news and provides in-depth reports on current and future CS trends. This dataset can be also very useful to support and promote new research activities in the CS domain.

The proposed AI-based approach provides an innovative threat assessment and management approach, increasing the security of the HCLs, and more in general, of the whole healthcare ecosystems and their supply chains. Moreover, it allows to leverage updated information available on the Internet, to assess threats of the assets of healthcare infrastructure, after a preliminary identification of the assets of the healthcare ecosystem context.

Although the proposed approach can be applied to any kind of natural language text, a limitation is related to the acquisition of large NL corpora, where reports of CS threats are described, requiring in many cases specific web crawlers and web scrapers, or tools provided by the owners of the websites. Another limit is related to the language of the NL corpus and the pre-training of the LLMs: in our knowledge, English is the main language where the resources are published on the Web. Concerning the applicability of our method to other businesses and contexts, there is also the need of domain-specific Knowledge Bases, allowing to correctly model and categorise the assets of the considered use case and domain.

In the future, we will firstly continue to improve and extend the proposed method. In detail, we are planning to include more NL CS datasets (from social, forums and other publicity available sources), to further enlarge the information source adopted to evaluate the threat level. We want also to test other NLMs, as well as to integrate into our pipeline an AI-based Relation Extraction method, to detect and classify the relations between the threat and the assets. Finally, to the end of further mitigating a possible contribution of false positives and negatives found by the NLP module, we are planning to integrate the threat prioritisation phase with information available in the CS knowledge bases (KBs), weighting in this way the obtained results

### 3.4.5.3 Incident Response

In the contemporary healthcare cybersecurity landscape, the escalating reliance on digital technologies introduces an imperative for robust incident handling and response strategies. Incident handling in healthcare refers to the systematic approach of identifying, containing, eradicating, and recovering from cybersecurity incidents. The interconnected nature of healthcare information infrastructure necessitates a proactive response to cyber threats to ensure the integrity and availability of critical healthcare services.

The EU AI4HEALTHSEC project improves the insights and enable incident handling and response in the following main topics:

- **Log Collection:** The project provides in significance the log collection mechanisms, that play critical role in incident detection by capturing a comprehensive set of data points necessary for understanding and responding to cybersecurity incidents. The agents actively monitor system activities and significantly contribute to incident detection. The incident detection phase ensures the timely identification of potential threats within the healthcare ecosystem.

- **Simulated Attack Validation:** A noteworthy aspect of the project involves the validation of incident handling procedures through simulated attacks. These controlled scenarios replicate real-world threats, offering a practical testbed to assess the efficacy of incident response mechanisms.
- **IoC Extraction:** Continuous monitoring of threat feeds involves the systematic and ongoing scrutiny of information provided by these intelligence sources. This active surveillance is essential for promptly identifying indicators of compromise (IoCs) that may signify potential security incidents within the healthcare ecosystem. IoCs encompass various elements, such as IP addresses, domain names, file hashes, and patterns of behaviour associated with known threats. Monitoring these indicators allows the healthcare system to detect anomalies and potential malicious activities in real-time.
- **Historical Records:** The insights garnered from historical incident analysis contribute directly to the improvement of the incident response strategy. By recognizing recurring patterns or identifying common vulnerabilities, incident responders can fine-tune their procedures to address specific challenges faced in the healthcare sector. This adaptive approach ensures that incident response efforts are tailored to the unique characteristics and risks associated with healthcare information systems.
- **Machine Learning:** ML algorithms in User and Entity Behavior Analytics (UEBA) analyse user and entity behaviours over time to establish baselines. Deviations from these baselines can indicate anomalies that might suggest a security incident. Continuous learning allows the system to adapt to changing patterns of normal behaviour and detect previously unseen threats. Furthermore, ML algorithms analyse network traffic patterns to identify unusual or suspicious behaviour. This includes identifying patterns associated with reconnaissance, lateral movement, or data exfiltration.

In conclusion, the integration of evidence-based cybersecurity risk management and advanced incident handling/response strategies within the healthcare sector, as exemplified by the EU AI4HEALTHSEC project, marks a significant advancement in safeguarding critical patient data and healthcare services. The evidence-based approach provides a clear understanding of cybersecurity risks and allows event-based detection and supports decision-making. The incorporation of machine learning algorithms enhances incident detection, enabling proactive responses to evolving cyber threats. The conducted simulated attacks validate the real-world applicability and underscore the practical effectiveness of the incident response.

Expanding the deployment of incident handling into different sectors represents a crucial avenue for future exploration. The results from the open call contributed to some initial results in this context. The cross-sector deployment is envisioned to offer valuable insights into the adaptability and effectiveness of the proposed methodologies across diverse environments. By testing the methodologies in varied contexts, the project aims to validate and refine its evidence-based approach for broader applicability. Furthermore, validating the isolation and mitigation steps becomes essential, while continuous improvement and adaptation coupled with robust validation procedures will ensure that incident response strategies remain effective and resilient in the face of evolving cyber threats.



## 4 Wider Applicability and Use

The AI4HEALTHSEC platform has been originally designed and developed specifically for healthcare domain. Also, the test cases proposed in the pilots executed during the WP6 activities considered several scenarios from the healthcare domain itself.

At the same time, the project foresees a wider applicability of the proposed solution, in other critical domains (such as transportation, banking, energy and others), as well as in healthcare scenarios different from the ones tested in our pilots. Therefore, the consortium organised an open call (the details of the open call organisation, application and selection procedures are reported in deliverable D8.6), with the following main purposes:

- To further test the AI4HEALTHSEC in the infrastructures of companies external to the consortium.
- To test it in critical environments different from the healthcare domain, also investigating on the usability and applicability of the platform outside the HCII.

The open call selected four external partners, who proposed additional pilots to test our platform. These external partners are listed below, including a brief overview of their proposed pilot use cases:

- *Clynxio LDA*<sup>26</sup> is a Digital Health Start-up based in Lisbon, Portugal, specialised in innovative technologies to support physiotherapy services. Clynxio deployed a project called TETHYS (TElemonitoring THreat-detection in a pHYSiotherapy platform) to validate the AI4HEALTHSEC platform via its integration to the Clynxio Platform, also *provisioning of a best practices roadmap inspired by this activity towards the wider applicability in telephysiotherapy and telemedicine* approaches. In detail, this pilot evaluated how secure Clynxio's solution is to cyber-attacks; and secondly, how helpful a solution like the AI4HEALTHSEC platform can be in detecting and providing information on these attacks.
- *IKE Ethos Hub*<sup>27</sup> is a child and family support centre based in Greece providing support for children and family in different sectors, including psychologists, special education teachers, speech, occupational therapists and play therapists. Ethos Hub proposed the SEPIA (Security Enforcement of in Child Psychology sensitive data) pilot to measure privacy and risks in the context of *conducting privacy-preserving linking in their own database containing sensitive medical and clinical data*, by identifying the different types of attacks that potentially can be applied on encoded or encrypted databases where the aim of an adversary is to learn about the sensitive information contained in such databases. In this way, they evaluated and validated the evidence-based risk management and assessment and the multi-level incident identification and management services of the AI4HEALTHSEC platform, enabling Ethos Hub to understand its cybersecurity posture and explore protective measures to increase the organisation's security, reducing the risk of harm to patients, staff, and infrastructure.
- *iLink New Technologies OE*<sup>28</sup> is a software company based in Greece, whose main products are devoted to the logistics and transportation domain. In this case, this external company proposed a pilot where AI4HEALTHSEC Dynamic Situational Awareness Framework (DSAF) is

---

<sup>26</sup> <https://www.Clynxio.io>

<sup>27</sup> <https://www.ethos-hub.eu>

<sup>28</sup> <https://ilink.gr>

used to gain a better understanding of their SME's cybersecurity posture and to study all the risks that might reside in their system for the *management and coordination of transportation fleets*, analysing the possibility that a vulnerability or a threat could lead to system failures and disruptions. They have also used the evidence-based risk management and assessment services provided by the DSAF to assess the vulnerabilities related to the cyber assets of their platform and forecast and evaluate the probability of cyber-attacks.

- *Dot Syntax Pliroforiki IKE*<sup>29</sup> is a Greek IT Solutions and Services Company. They proposed a pilot to validate and evaluate the evidence-based risk management and assessment services and the multi-level incident identification and management services of the DSAF in AI4HEALTHSEC, via a cross technology and cross domain perspective to explore important development issues like performance, flexibility, and reusability, to protect the *critical air transport infrastructure* in the Sofia Airport against cyber-threats.

Two of these companies (Clynxio and Ethos Hub) proposed a pilot study in the healthcare domain, while the other two ones (iLink New Technologies and Dot Syntax) developed and tested a scenario in a different domain (transportations and logistics). The details of the scenarios proposed by the open call partners, their development and implementation, as well as the results obtained by the application of the AI4HEALTHSEC platform to these test cases, are reported in the Deliverable D8.7.

After the exploitation of the pilots, the open call partners also filled a questionnaire (provided by the consortium), to provide a detailed evaluation report of the application, usage and results obtained by the AI4HEALTHSEC platform. Each questionnaire has been filled at least by three different persons of each external company directly involved in the pilot projects.

The results of the open call, including the evaluation questionnaires, allowed the consortium to highlight and understand the common challenges related to a wider applicability and usability of the AI4HEALTHSEC solution, as well as to identify the possible issues to be addressed in this perspective, obtaining in this way insights on the applicability of our platform in different scenarios and domains, which will be summarised below.

Firstly, it is worth noting that the deployment and implementation of the external pilots didn't report significant problems, barriers, or incidents, except for very few minor issues in a couple of cases, related to the connection between the assets involved in two of the proposed scenarios (Ethos Hub and Dot Syntax), that required some consultation with the technical partners of AI4HEALTHSEC.

Moreover, the AI4HEALTHSEC platform, in all tested cases (both healthcare and transportation domains), was able to provide useful information related to the attack, vulnerabilities, threats, and risks, as well as a detailed summary of reported events classified for security, highlighting the vulnerabilities of the external partners' systems, and suggesting the required mitigation actions.

The external partners affirmed that is very likely their organisation will be using the solution in the future, following relevant updates, evaluating AI4HEALTHSEC an important possible asset in their organisation, which is capable of providing useful information and mitigation techniques to make their systems more secure. Furthermore, they confirmed that they would recommend the solution to other companies, not only in their same domain.

---

<sup>29</sup> <https://www.dotsyntax.gr>

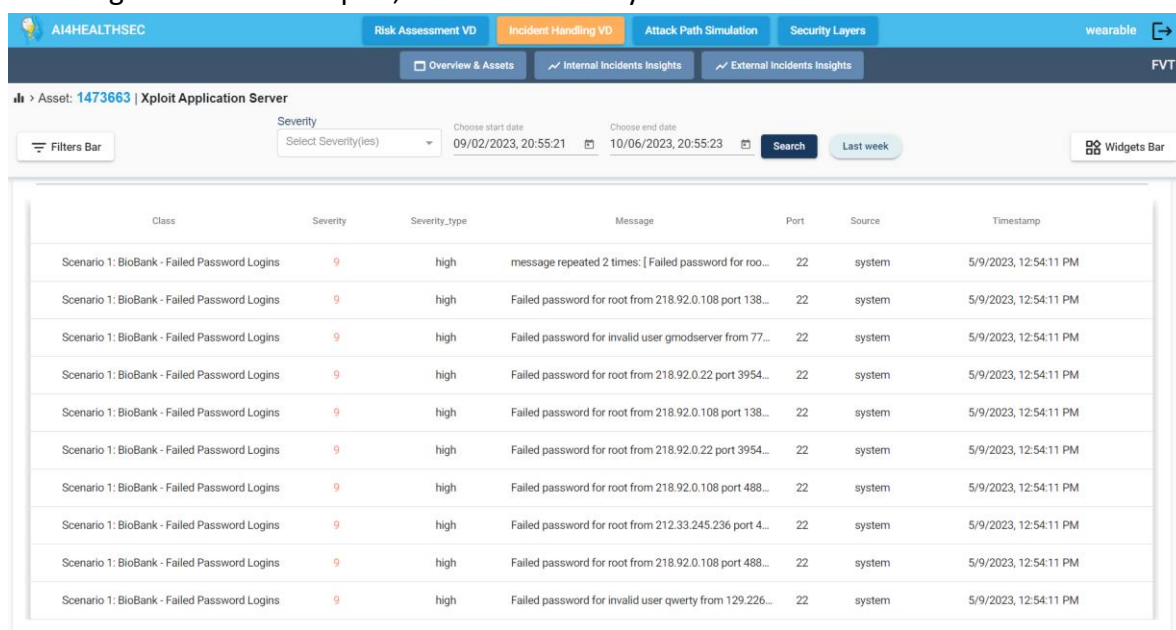
Regarding common challenges of the platform, applicable to any domain, the open call pilots' results suggested that there are still some difficulties for executing some actions using the AI4HEALTHSEC platform, in the case of not expert users. In detail, some open call partners reported that the platform's UI and, more in general, the operations that are required to perform some analyses, should be more user friendly. In particular, they highlighted that a person without any cybersecurity knowledge should not be able to navigate the platform and find immediately all the relevant information. This issue is related to the maturity of the implementation of the platform, as well as to a current usage of the dashboard and the UI by a small group of people, whose feedback is still not enough to improve these aspects. Nevertheless, this issues will be addressed in the next versions of the platform, following the suggestions from the users of the platform. A better support for non-expert users is expected to be offered in the future, e.g., during the commercialisation phase.

In summary, the exploitation of the open call pilots not only allowed to test more in deep the AI4HEALTHSEC platform, collecting more final users' feedbacks to improve some specific aspects, but, more important, demonstrated that some of the few issues encountered by the open call partners, such as the need of assistance to implement some of the assets' connections and to navigate the platform to obtain the required information, are not domain-specific, but they are common to different domains.

On the other hand, these additional pilots, confirmed that the AI4HEALTHSEC DSAF methodology and the implemented platform can be easily and effectively adopted, without specific adaptations, in domains different from the healthcare. It is important to underline that the solution can be deployed, with the assistance of the AI4HEALTHSEC technical team in several different assets' configurations without installing any kind of software within the IT systems that must be analysed, but it only requires the assets' lists and the details of their interconnection, in addition to the system logs. This feature can further facilitate a larger adoption of the proposed AI4HEALTHSEC solution.

## 5 Lessons Learned and Best Practices

In the various cybersecurity scenarios outlined within the AI4HEALTHSEC project, several lessons learned, and best practices can be applied to enhance security measures, detect threats, and respond effectively to incidents. In the case of biobank, understanding common attack methods was vital to safeguard sensitive biological data and maintain the integrity of their operations. Biobank encountered a scenario involving failed password logins, where an attacker attempted unauthorized access through various techniques, such as dictionary attacks.



Class	Severity	Severity_type	Message	Port	Source	Timestamp
Scenario 1: BioBank - Failed Password Logins	9	high	message repeated 2 times: [ Failed password for roo...	22	system	5/9/2023, 12:54:11 PM
Scenario 1: BioBank - Failed Password Logins	9	high	Failed password for root from 218.92.0.108 port 138...	22	system	5/9/2023, 12:54:11 PM
Scenario 1: BioBank - Failed Password Logins	9	high	Failed password for invalid user gmodserver from 77...	22	system	5/9/2023, 12:54:11 PM
Scenario 1: BioBank - Failed Password Logins	9	high	Failed password for root from 218.92.0.22 port 3954...	22	system	5/9/2023, 12:54:11 PM
Scenario 1: BioBank - Failed Password Logins	9	high	Failed password for root from 218.92.0.108 port 138...	22	system	5/9/2023, 12:54:11 PM
Scenario 1: BioBank - Failed Password Logins	9	high	Failed password for root from 218.92.0.22 port 3954...	22	system	5/9/2023, 12:54:11 PM
Scenario 1: BioBank - Failed Password Logins	9	high	Failed password for root from 218.92.0.108 port 488...	22	system	5/9/2023, 12:54:11 PM
Scenario 1: BioBank - Failed Password Logins	9	high	Failed password for root from 212.33.245.236 port 4...	22	system	5/9/2023, 12:54:11 PM
Scenario 1: BioBank - Failed Password Logins	9	high	Failed password for root from 218.92.0.108 port 488...	22	system	5/9/2023, 12:54:11 PM
Scenario 1: BioBank - Failed Password Logins	9	high	Failed password for invalid user qwerty from 129.226...	22	system	5/9/2023, 12:54:11 PM

Figure 5-1. Scenario results from biobank on Failed Password Logins

Implementing strong password policies, enforcing regular password changes, and integrating multi-factor authentication was crucial in fortifying their defenses against such threats. This lesson can be applied across all pilots, ensuring that a comprehensive approach to safeguarding access and data is adopted, regardless of the specific pilot's context. Tethys faced a different aspect of data collection with DNS spoofing. Understanding the manipulation of DNS responses and the importance of monitoring these responses is crucial to detect such attacks.

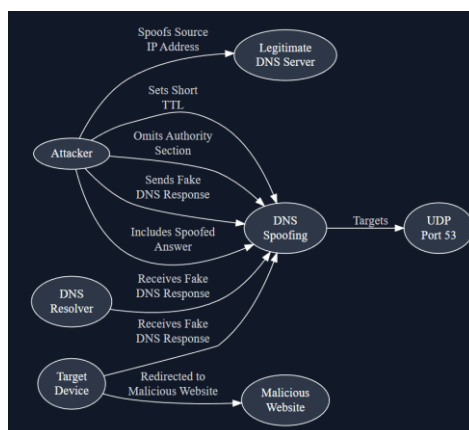


Figure 5-2. DNS Spoofing on Tethys (Pilot from the Open Call)

By recognizing the significance of these events, all pilots can better prepare to monitor DNS traffic and protect their systems from potential spoofing or cache poisoning attacks, thus maintaining the integrity of critical healthcare infrastructure.

Klinikum Nuremberg, in another instance, faced an external attack with cryptomining malware. To prevent such attacks, organizations like Klinikum Nuremberg need to employ measures that protect against malware infiltration, including security patches and robust endpoint security solutions.

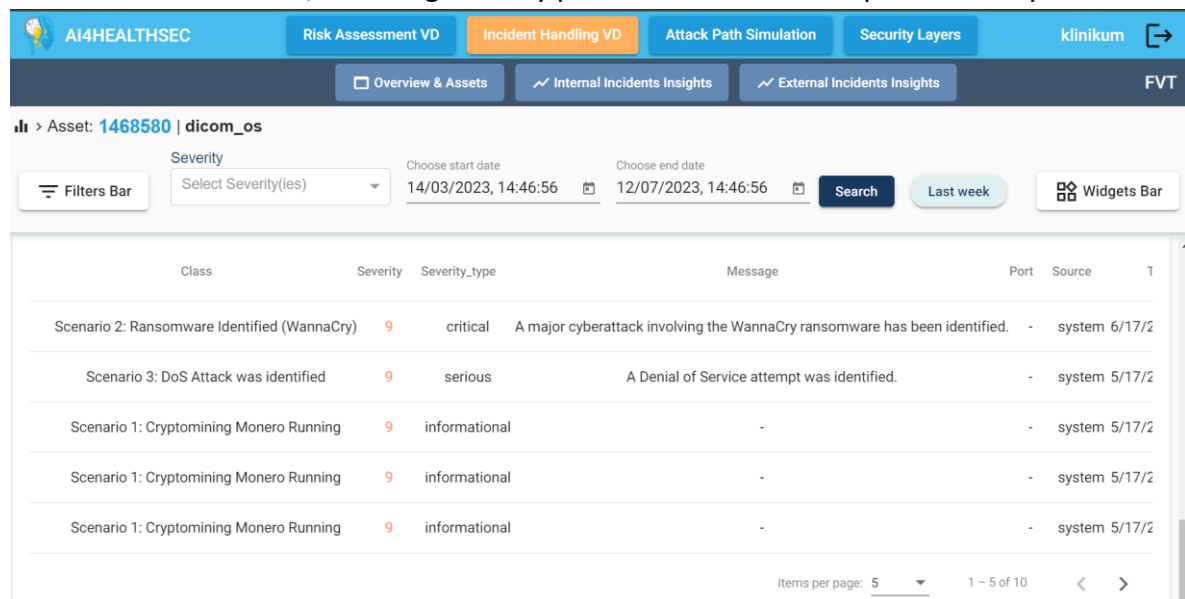


Figure 5-3. Ransomware attack on KLINIK

By adopting these practices, pilot cases can effectively anticipate and prepare for potential threats that might attempt to exploit their systems through various malicious means, thereby increasing the overall resilience of healthcare environments.

The need for continuous monitoring of network traffic patterns is exemplified in the scenario of ML-IDS discovering a network anomaly. In this context, ML-IDS identified unusual data transfer patterns, indicative of potential security breaches. By maintaining a baseline of normal network behavior, organizations like Living Labs can more accurately differentiate between benign fluctuations and true threats. This lesson underscores the importance of real-time monitoring and early threat detection, applicable to all pilots and use cases.

By recognizing the significance of these events, all pilots can better prepare to monitor DNS traffic and protect their systems from potential spoofing or cache poisoning attacks, thus maintaining the integrity of critical healthcare infrastructure.

Biobank's scenario (see Figure 5-4) involving a sudo command executed highlights the importance of data sanitization. Implementing filtering mechanisms in IDS solutions, such as in this case, can help reduce noise in alerts, allowing teams to focus on actionable information.

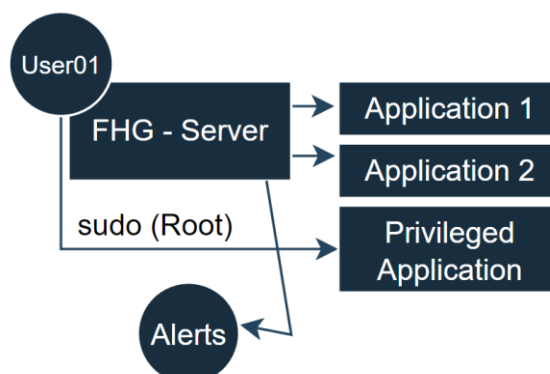


Figure 5-4. Privilege escalation or administrative command execution on biobank

This practice is pertinent to all pilot cases, as it emphasizes the need to streamline incident response processes by ensuring that alerts prioritize real threats over false positives. In the case of eBIT, attacks involving multiple failed password logins were addressed. Developing and refining detection rules is critical, and the establishment of specific rules for each scenario is essential for timely alerts and responses. By crafting and adapting these rules, all pilots can stay ahead of evolving threats and bolster their cybersecurity posture.

Living Labs dealt with unauthorized access and surveillance exploitation, which underscores the need for refined detection rules to identify such breaches and mitigate their consequences effectively.

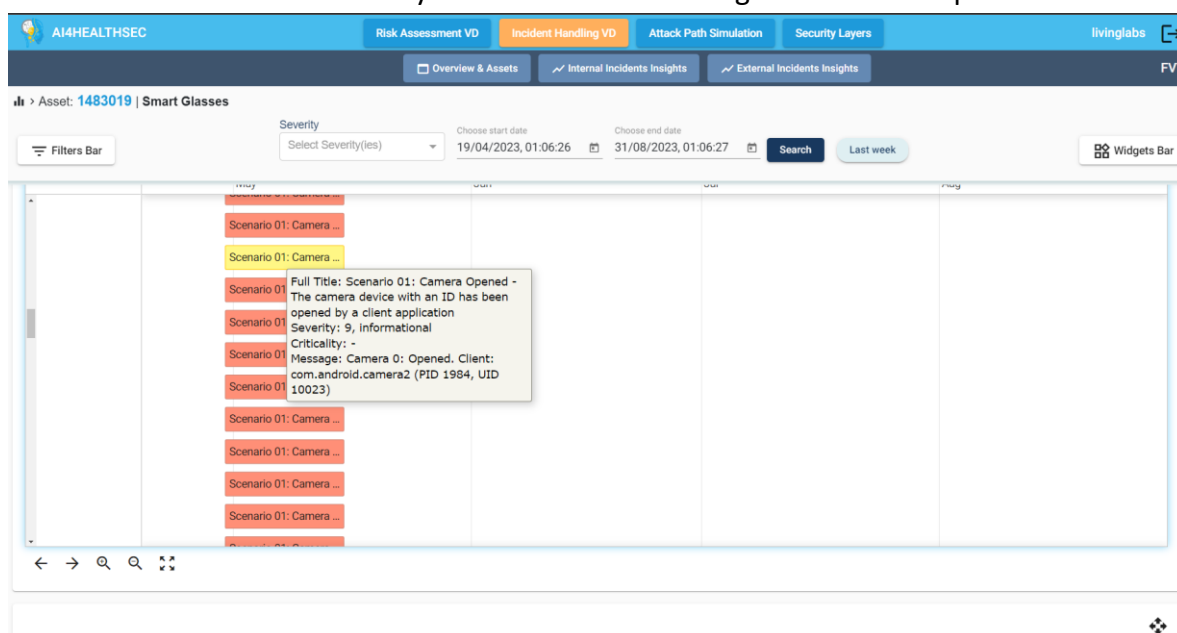
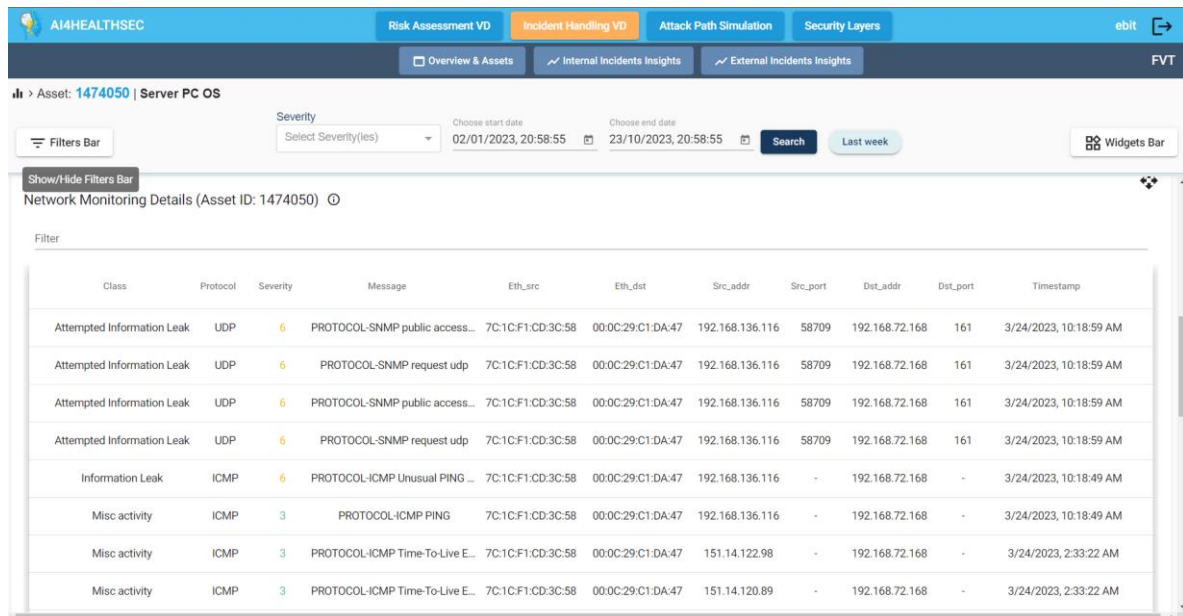


Figure 5-5. Surveillance from unauthorized usage of Camera on Smart Glasses (LivingLabs Pilot)

In this context, creating precise detection rules can prevent unauthorized access to sensitive patient data, ensuring patient safety and confidentiality. The emphasis on configuring alerts to trigger upon significant deviations from expected patterns, as shown in the case of Tethys, can be universally applied. Setting alert thresholds carefully ensures that alerts are both effective and efficient. This lesson is invaluable for prioritizing incident response actions across all pilot cases.



KLINIK's scenario of a DoS attack further accentuates the importance of alert triggering, as it disrupts normal operations.



Class	Protocol	Severity	Message	Eth_src	Eth_dst	Src_addr	Src_port	Dst_addr	Dst_port	Timestamp
Attempted Information Leak	UDP	6	PROTOCOL-SNMP public access...	7C:1C:F1:CD:3C:58	00:0C:29:C1:DA:47	192.168.136.116	58709	192.168.72.168	161	3/24/2023, 10:18:59 AM
Attempted Information Leak	UDP	6	PROTOCOL-SNMP request udp	7C:1C:F1:CD:3C:58	00:0C:29:C1:DA:47	192.168.136.116	58709	192.168.72.168	161	3/24/2023, 10:18:59 AM
Attempted Information Leak	UDP	6	PROTOCOL-SNMP public access...	7C:1C:F1:CD:3C:58	00:0C:29:C1:DA:47	192.168.136.116	58709	192.168.72.168	161	3/24/2023, 10:18:59 AM
Attempted Information Leak	UDP	6	PROTOCOL-SNMP request udp	7C:1C:F1:CD:3C:58	00:0C:29:C1:DA:47	192.168.136.116	58709	192.168.72.168	161	3/24/2023, 10:18:59 AM
Information Leak	ICMP	6	PROTOCOL-ICMP Unusual PING ...	7C:1C:F1:CD:3C:58	00:0C:29:C1:DA:47	192.168.136.116	-	192.168.72.168	-	3/24/2023, 10:18:49 AM
Misc activity	ICMP	3	PROTOCOL-ICMP PING	7C:1C:F1:CD:3C:58	00:0C:29:C1:DA:47	192.168.136.116	-	192.168.72.168	-	3/24/2023, 10:18:49 AM
Misc activity	ICMP	3	PROTOCOL-ICMP Time-To-Live E...	7C:1C:F1:CD:3C:58	00:0C:29:C1:DA:47	151.14.122.98	-	192.168.72.168	-	3/24/2023, 2:33:22 AM
Misc activity	ICMP	3	PROTOCOL-ICMP Time-To-Live E...	7C:1C:F1:CD:3C:58	00:0C:29:C1:DA:47	151.14.120.89	-	192.168.72.168	-	3/24/2023, 2:33:22 AM

Figure 5-6. DoS attack execution on KLINIK

Ensuring that alert thresholds are set based on potential impact can help all pilots prioritize responses effectively, minimizing the impact of such attacks on their healthcare systems.

Maintaining a repository of detection rules is essential for consistency and efficiency. These rules can be documented, version-controlled, and updated as needed. Regular updates and adaptations of rules are vital as threats evolve. Staying ahead of emerging threats requires continuous refinement of detection mechanisms. For instance, in the scenario involving password attacks, regularly updating password-related detection rules can help adapt to new attack patterns or emerging password vulnerabilities.

Collecting logs asynchronously ensures real-time access to data for analysis. Logs often contain critical information about security incidents. Robust log management systems centralize and store logs securely, allowing for easy access, analysis, and retention in compliance with data protection regulations. In cases like malware infections, asynchronous log collection can aid in analyzing patterns of infection and source identification.

## 5.1 Integration Plan

The integration plan for deploying AI4HEALTHSEC (Figure 5-7) to other use cases entails a series of well-defined steps to ensure its effective implementation within diverse healthcare scenarios. It begins with asynchronous manual log collection, a process that involves capturing log data in real-time, enabling prompt access for analysis and incident response. This approach is fundamental for early threat detection and enhanced cybersecurity. Subsequently, conducting test analyses using historical or simulated log data allows organizations to fine-tune the AI models and assess system performance under various conditions, ensuring readiness for real-world deployment.

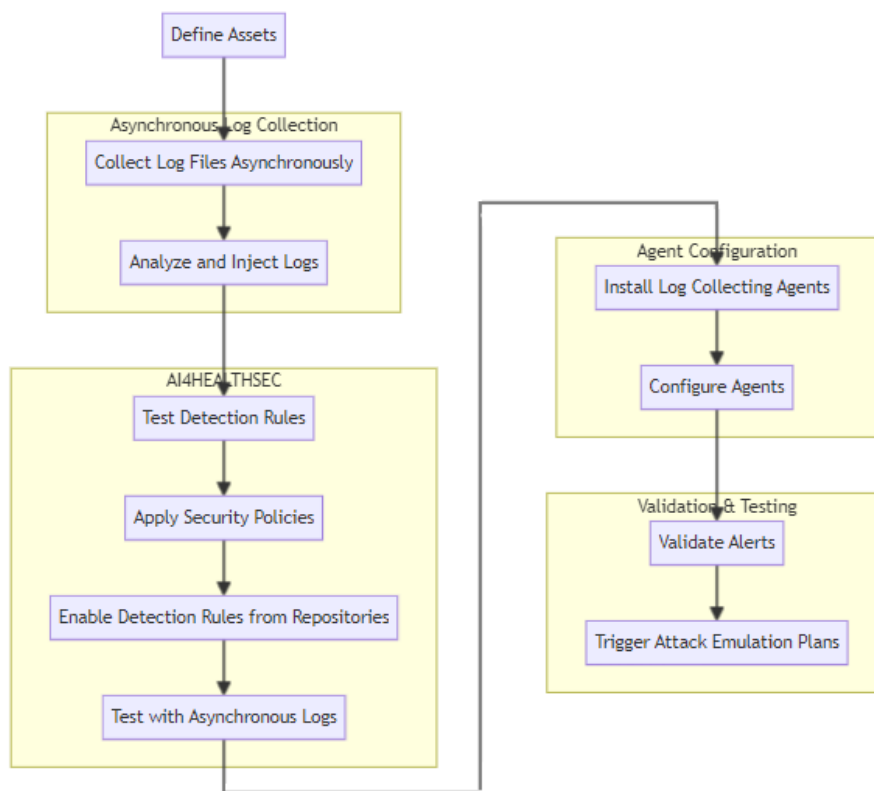


Figure 5-7 Integration plan of AI4HEALTHSEC platform.

- **Define Assets:** One of the crucial aspects of this integration plan is enumerating important assets. This step involves identifying and categorizing critical assets within the healthcare ecosystem, including sensitive patient data, healthcare systems, IoT devices, and more. A clear understanding of what needs to be safeguarded is essential in tailoring the AI4HEALTHSEC solution to address specific security challenges. In this initial step, you identify the critical assets within your organization, such as servers, databases, applications, and data stores that need to be protected. It's essential to have a clear understanding of what needs to be secured before proceeding with integration.
- **Collect Log Files Asynchronously:** This step involves setting up a system to collect log files from various sources, such as operating systems, network devices, and applications. Asynchronous collection means that logs are gathered independently of real-time events, ensuring that historical log data is also considered for analysis. This historical data is valuable for identifying past security incidents.
- **Analyze and Inject Logs:** The collected log data is analyzed for patterns, anomalies, and security-related information. After analysis, the log data is injected into the AI4HEALTHSEC platform for further processing and correlation. This step is essential for preparing the data for security detection and analysis.
- **Test Detection Rules:** Security professionals create and test detection rules within the AI4HEALTHSEC platform. These rules are designed to identify specific security threats, such as intrusion attempts, malware infections, or unauthorized access. Rigorous testing is crucial to



ensure that the detection rules are accurate and efficient in identifying potential security incidents.

- *Apply Security Policies*: A critical step in the integration plan is defining requirements. This entails specifying desired outcomes, setting performance benchmarks, outlining the scope of monitoring, and establishing clear incident response protocols. Customization and fine-tuning of AI4HEALTHSEC is also paramount, aligning the system with the specific cybersecurity challenges faced by the healthcare organization. This involves configuring AI models, developing detection rules, and setting alert thresholds. Security policies define the guidelines and rules for how security should be enforced within your organization. They include access control policies, data encryption, and other security measures. Applying these policies within the AI4HEALTHSEC platform ensures that security measures are consistently enforced.
- *Enable Detection Rules from Repositories*: Common repositories contain pre-defined detection rules that are based on industry best practices and known security threats. Enabling these rules within AI4HEALTHSEC leverages collective knowledge and helps enhance security without reinventing the wheel.
- *Test with Asynchronous Logs*: Continuously testing the system with asynchronous logs is crucial for ongoing monitoring and improvement. It ensures that detection rules and security policies are effective even for historical log data. Any changes or updates to the system can be tested against this historical data to ensure they don't introduce new vulnerabilities.
- *Install Log Collecting Agents*: To enable seamless log data collection, the deployment of agents is necessary. These agents should be strategically positioned to collect log data from diverse sources such as network devices, servers, databases, and IoT devices. Their configuration should ensure secure and efficient transmission of log data to a centralized platform, enhancing the overall visibility of the healthcare organization's cybersecurity landscape. When determining the deployment of AI4HEALTHSEC as either internal or external, organizations should base their decision on their unique requirements and capabilities. Internal deployment is suited for organizations with robust IT infrastructures and in-house security teams, while external deployment offers a feasible option for organizations looking to outsource their cybersecurity needs to trusted external providers. Log collecting agents are software components that are installed on the systems you want to monitor. These agents are responsible for gathering log data from these systems and forwarding it to the AI4HEALTHSEC platform in real-time.
- *Configure Agents*: Properly configuring the log collecting agents is essential to ensure they collect and transmit relevant log data accurately. Configuration settings include specifying which log types to collect, where to send the logs, and how often to transmit them.
- *Validate Alerts*: The alerts generated by the AI4HEALTHSEC platform should be thoroughly validated. This involves reviewing the alerts, investigating the security incidents they represent, and fine-tuning the alerting system to reduce false positives. Accurate alerts are essential for a timely and effective response to security threats.
- *Trigger Attack Emulation Plans*: Emulating security attacks allows you to assess how the AI4HEALTHSEC platform responds to real-world threats. This step helps you identify any gaps

or weaknesses in your security measures and fine-tune your response strategies to better protect your assets.

The integration plan doesn't end with deployment; it includes ongoing monitoring and continuous improvement. Regular review and analysis of log data and AI model performance are essential to stay ahead of evolving threats. The system should be seamlessly integrated with the incident response plan of the healthcare organization, ensuring a coordinated and effective response to security incidents. Proper documentation and training complement the plan, guaranteeing that the system is used effectively and that teams are well-prepared to handle cybersecurity challenges.

Deploying AI4HEALTHSEC to a new healthcare environment is a meticulous process, necessitating careful planning and execution. The initial phase encompasses assessment and requirements gathering, enabling a deep understanding of the unique needs and existing security measures in the target healthcare setting. Resource allocation is pivotal to determine the hardware and personnel requirements for a successful deployment. The subsequent installation and configuration steps involve setting up AI4HEALTHSEC within the new pilot environment. This includes deploying the necessary infrastructure and configuring the platform to harmonize with the specific security needs of the healthcare system. The integration of data is a critical facet, encompassing comprehensive log collection from diverse sources and the analysis and preprocessing of these logs for effective security monitoring.

Extensive testing and validation are imperative. This entails meticulous evaluation of detection rules and alerts to ensure they align with the new pilot's security objectives. User training and documentation are integral for equipping healthcare staff and security personnel with the skills to operate AI4HEALTHSEC proficiently. Gradual deployment, systematic monitoring, and incident response planning guarantee the platform's seamless integration and the capacity to respond to security incidents.

## 6 Conclusion

In this deliverable we described recommendations and guidelines for ensuring that AI4HEALTHSEC platform is replicable and can be more widely adopted. It cannot be done without mentioning legal, ethical, and related policies.

Therefore, we started with the assessment of legal and ethical considerations, where we identified and described the following crucial points:

- The development and deployment of AI4HEALTHSEC adhered to the principles outlined in the GDPR.
- AI4HEALTHSEC project is in alignment with the EU's strategic cybersecurity framework, which increasingly encourages efficient reporting and resource pooling.
- The legal framework also incorporates principles that guide legislation and standards, including references to documents such as the Ethics Guidelines for Trustworthy AI and the forthcoming AI Act.
- Throughout the development and implementation of AI4HEALTHSEC solutions, the detailed legal and ethical framework has been diligently considered.

Furthermore, in an attempt to offer feedback to relevant policies aligned with those addressed in the project, we described four step methodology that we followed:

- Identification of policy instruments
- Selection of the most related policy instruments
- Identification of main topics of the policy instruments
- Identification of relevance and provision of recommendations, comments and feedback

Section 0 summarises four policies that AI4HEALTHSEC consortium provided recommendation to. After that we provided conclusions in the following areas: risk assessment, AI and cybersecurity, and incident response.

Organised by AI4HEALTHSEC consortium open call demonstrated how the system would perform in other critical infrastructure (i.e., transportation). Additionally, open call participants suggested and ran scenarios that differ from the ones performed in WP6, which provided us with new feedback and insight.

At the end, lessons learned and best practices from internal pilot operation have been presented. During internal pilot operation different attack scenarios were executed. Based on AI4HEALTHSEC detection the necessary best practices were defined that can broadly be applied to avoid the attacks. Additionally, after integrating AI4HEALTHSEC platform with 6 internal pilots a guideline on AI4HEALTHSEC deployment is described.

## 7 Appendix

### 7.1 Feedback on the consultation to the European Cyber Resilience Act

The following represents a transcript of the feedback provided to the online consultation system of the EC. This consultation comprised of questions split in 4 sections. The text below contains (for clarity) not only the answers of the AI4HealthSec project but also the relevant questions. The answers provided by the AI4HealthSec project are in blue.

#### Section 1: Cybersecurity of digital products and the users of digital products

This section contains questions on the state of cybersecurity of digital products marketed in the European Union and users' ability to choose secure products and use them in a secure manner, and the role that vendors can play in securing products and providing cybersecurity related information on their products.

##### Sub-section 1.a. – The state of cybersecurity of digital products

**Q1:** In your view, what is the overall level of cybersecurity of digital products marketed within the European Union (on a scale from 1 to 5 with 5 indicating a very high level of cybersecurity)?  
2

Please elaborate - 1000 character(s) maximum

For the time being the requirements for cybersecurity products are very limited. Requirements are planned to be imposed based on the Cybersecurity Act (CSA) which amongst other will introduce the European cybersecurity certification framework, with a view to creating a digital single market for ICT products, ICT services and ICT processes. With the exception of some specific industries (e.g. Medical Devices - 745/2017 (MDR) and 746/2017 (IVDR)) specific requirements for cybersecurity have not been introduced. This leads to a low level of cybersecurity of digital products marketed within the European Union.

**Q2:** In your view, during the last five years, how has the level of risk of cybersecurity incidents affecting digital products evolved?

Risk level has decreased significantly

Risk level has decreased

Risk level is the same

Risk level has increased

✓ -- Risk level has increased significantly

Don't know / no opinion

Please elaborate, 1000 character(s) maximum

Cyberattacks and cybercrime are increasing in number and sophistication across Europe. In the latest Global risk report, there is a chapter (Chapter 3) dedicated on Digital Dependencies and Cyber Vulnerabilities. Based on this report, there is a 435% increase in ransomware in 2020, there is a US\$ 800 billion estimated growth in value of digital commerce by 2024.

### Sub-section 1.b. – Consequences of cyber incidents and non-secure digital products

**Q3:** How would you evaluate the actual impact of cybersecurity incidents affecting digital products on you or your organisation (on a scale from 1 to 5 with 5 indicating a very high negative impact)?

	1	2	3	4	5	Don't know / no opinion
Financial cost of implementing measures to respond to a cybersecurity incident				X		
Financial cost of disruption (e.g. due to a ransomware attack)				X		
Reputational damage				X		
Compromising the security of our economy and society				X		
Damage to health and life					X	
Damage to fundamental rights (e.g. privacy, protection of personal data, consumer protection)					X	
Environmental damage	X					

Please elaborate, if possible quantify, *1000 character(s) maximum*

The responses provided above are given from the perspective of healthcare organizations. The healthcare sector has undergone dramatic changes in the past several years, primarily spurred by the adoption of new medical technology including IoT, Cloud Computing, and Big Data. The adoption of electronic health records and amongst others the increased use of medical applications, patient portals, connected devices, and wearables, the healthcare sector has been capitalizing on digital advancements to improve overall patient experiences and outcomes. The increasing interconnection of technology in healthcare between devices at the physical and cyber levels has transformed these infrastructures into large Health Care Information Infrastructures (HCIIIs). Patients can be permanently or temporarily injured through direct actions such as performing inadequate medical acts or turning off critical medical devices; but their health may also be affected by indirect actions aiming at disrupting care.

**Q4:** In your view, if a digital product is not cyber secure, how does it impact the user (on a scale from 1 to 5 with 5 indicating that you fully agree)?

	1	2	3	4	5	Don't know / no opinion
The user bears additional cost when affected by a cybersecurity incident					X	
The user bears additional costs due to highly priced cybersecurity insurance			X			
The user bears additional costs due to the need to deploy highly priced technical security solutions					X	

Please elaborate, if possible quantify, 1000 character(s) maximum

The responses provided above are given from the perspective of healthcare organizations. The user in this case would be the healthcare organization. If there is a cybersecurity incident there will be indirect and direct costs to the user organization. Indirect by the impacts to the patients and indirect due to the loss of revenue (if there is a disruption of service), due to impacts on reputation, due to the cost for the remediation of the effects of the incidents and the fortification of the systems after the fact etc. Cybersecurity insurance is still developing and there is no specific scheme that takes into consideration the devices individually, so it is difficult to quantify.

### Sub-section 1.c. – Trust, cybersecurity awareness and capabilities of users

**Q5:** To what extent do you agree with the following statements as regards your awareness and understanding of cybersecurity properties of digital products (on a scale from 1 to 5 with 5 indicating that you strongly agree)?

	1	2	3	4	5	Don't know / no opinion
In general terms, I am aware of the cybersecurity risks associated with digital products					X	
There is sufficient and clear information made available on the cybersecurity properties of digital products		X				
I understand the cybersecurity properties I should expect from a product and have the skills to operate it securely				X		

	1	2	3	4	5	Don't know / no opinion
I value aspects of usability and price of a digital product higher than its cybersecurity features			X			

### Sub-section 1.d - The role of vendors in providing secure digital products

**Q6:** To what extent do you agree with the following statements on the role of the vendors? Please rate the following statements on a scale from 1 to 5 (with 5 indicating that you strongly agree).

	1	2	3	4	5	Don't know / no opinion
Vendors of hardware are addressing effectively cybersecurity vulnerabilities and incidents affecting their customers		X				
Vendors of software are addressing effectively cybersecurity vulnerabilities and incidents affecting their customers			X			

**Q7:** If you are a vendor: which of the following aspects have the biggest impact on your decision related to cybersecurity of your digital product?

	Very relevant	Relevant	Neither nor	Not too relevant	Not relevant at all	Don't know / no opinion
The potential reputational damage and the loss of trust of the users following an incident						
Customer expectations, including						

	Very relevant	Relevant	Neither nor	Not too relevant	Not relevant at all	Don't know / no opinion
contractual obligations						
Public procurement practices (e.g. guidelines)						

What are other aspects affecting your decision related to cybersecurity of your digital product?

*1000 character(s) maximum*

**Q8:** To what extent are hardware manufacturers and software developers taking the cybersecurity of their digital products into account in each of the following phases of the product lifecycle (on a scale from 1 to 5 with 5 indicating that cybersecurity is taken very seriously)?

	1	2	3	4	5	Don't know / no opinion
Design		X				
Development		X				
Delivery of the product on the market		X				
Maintenance and evolution of the product (e.g. after-sale)		X				

## Section 2: Improving the cybersecurity of digital products

This section explores various policy options to improve the cybersecurity of digital products. This includes also questions on the types of products to be covered by an intervention, on other relevant legislation, on security requirements, on risk as well as ways to assess the conformity of manufacturers.



## Sub-section 2.a. – Exploring ways to make digital products more secure

**Q9:** To what extent do you think that the following measures could be effective in raising the level of cybersecurity of digital products marketed in the Union (on a scale from 1 to 5 with 5 indicating that a measure would be very effective)?

	1	2	3	4	5	Don't know / no opinion
Guidelines or recommendations for the development of secure digital products issued at EU level addressed to vendors				X		
Further voluntary European cybersecurity certification schemes for digital products and services		X				
EU public procurement guidelines taking into account cybersecurity requirements				X		
Amending existing legislation regulating specific products with a digital dimension (such as the legislation on lifts or gas appliances)					X	
Introducing mandatory horizontal cybersecurity requirements for hardware products				X		
Introducing mandatory horizontal cybersecurity requirements for software products				X		

Please elaborate, 1000 character(s) maximum

Guidelines and recommendations can be helpful for organizations, when they try to understand and implementation the related requirements. But, additional measures need to be implemented. Just guidelines without the appropriate assessment mechanisms can not exist. The assessment mechanisms will provide an external opinion regarding the correct implementation and adoption of the guidelines. For products that may lead to high risk (as for example is already implemented for Medical Devices), there need to be stricter, recognized and controlled processes.

**Q10:** How would you assess the impact of the following measures on the level of cybersecurity of digital products and of the consumers/organisations using such products (on a scale from 1 to 5 with 5 indicating that a measure would have a very high impact)?

	1	2	3	4	5	Don't know / no opinion
Require vendors to make available information and provide instructions on securely installing, operating and using the product in question			X			
Require vendors to take corrective actions (such as patching, recalling or withdrawing a product) when a product is found to be not secure				X		

### Sub-section 2.b. – Exploring ways to make users more aware

**Q11:** How would you assess the relevance of the following measures for the users' ability to evaluate the cybersecurity properties of a digital product and to make better informed purchase or usage decisions (on a scale from 1 to 5 with 5 indicating that a measure is very relevant)?

	1	2	3	4	5	Don't know / no opinion
Making available technical documentation (containing information to demonstrate the conformity of the product to the applicable requirements) on the cybersecurity properties of a product (such as on risks and proper use)		X				
Making available EU Declaration of conformity (stating that all the relevant requirements of the applicable legislation are satisfied)		X				
Affixed symbol of compliance (such as CE marking)		X				

	1	2	3	4	5	Don't know / no opinion
Training on the secure use of digital products				X		

Which other measures would allow for better informed purchase or usage decisions by the user?  
Please elaborate, *1000 character(s) maximum*

There should be easy to read and understand information and labelling that indicates the conformity of a product to applicable cybersecurity requirements. Digital products may have different audiences, with a different level of technical skills and knowledge in relation to cybersecurity. Any statement of conformity should be clear and if possible based on maturity schemes.

### Sub-section 2.c. – Digital products to be covered by a European initiative

**Q12:** To what extent do you agree that subjecting certain products marketed in the Union to cybersecurity requirements would be effective (on a scale from 1 to 5 with 5 indicating that you strongly agree)?

	1	2	3	4	5	Don't know / no opinion
Hardware products				X		
Embedded software				X		
Ancillary services*				X		
Hardware products subject to higher cybersecurity risks					X	
All standalone software products			X			
Software products subject to higher cybersecurity risk					X	

\* Ancillary service means a (digital) service, the absence of which would prevent the tangible product from performing its functions (e.g. a website through which you access to the functionality of a device).

Please elaborate, *1000 character(s) maximum*

Hardware as well as software should have incorporated cybersecurity requirements. Known vulnerabilities and attacks are clear evidence of that. Ancillary services and embedded software are part of these products and should also have these requirements consolidated.

## Sub-section 2.d. – Existing legislation on the cybersecurity of digital products

**Q13:** To what extent do you agree with the following statements about how cybersecurity is addressed in existing EU legislation (e.g. the [General Product Safety Directive](#) and the [Machinery Directive](#), both currently under review; the [Delegated Regulation of 29 October 2021 under the Radio Equipment Directive](#)) (on a scale from 1 to 5 with 5 indicating that you strongly agree with a statement)?

	1	2	3	4	5	Don't know / no opinion
Existing EU regulation appropriately addresses cybersecurity of tangible digital products (hardware) throughout their lifecycle	X					
Existing EU regulation appropriately addresses cybersecurity of intangible digital products (software) throughout their lifecycle	X					
Existing EU regulation appropriately addresses all relevant cybersecurity risks (material and non-material damages) related to the use or misuse of a digital product	X					

**Q14:** In the absence of horizontal cybersecurity requirements at European level, Member States could adopt national laws placing certain requirements on vendors. To what extent do you agree that there is a risk of increasing costs and legal uncertainty for market stakeholders, in the absence of an EU initiative? (on a scale from 1 to 5 with 5 indicating you fully agree)?

5

Please elaborate, 1000 character(s) maximum

If member states have the ability to create and enforce national rules and requirements, the produced result for the European Union in general will be greatly varied. This would lead to confusion and fragmentation of the market. If a vendor wanted to market his product / service in the entire European Union or in multiple countries, they would need to comply to various

(even conflicting) requirements. This would definitely lead to increased costs and legal uncertainty.

**Q15:** If you are a vendor: are your digital products subject to legal requirements as regards their cybersecurity? In your answer, please take into account European, national but also legislation stemming from third countries.

### Sub-section 2.e. – Cybersecurity requirements for digital products

**Q16:** Should hardware manufacturers and software developers be responsible for the full life cycle of a digital product (such as by being required to provide updates)?

Yes

Please elaborate, *1000 character(s) maximum*

In general the producer has the resources and the ownership to manage and respond to security throughout the life cycle of the products and services.

**Q17:** To what extent can the following approaches contribute to the cybersecurity of a digital product (on a scale from 1 to 5 with 5 indicating that a measure would be very effective)?

	1	2	3	4	5	Don't know / no opinion
Cybersecurity is taken into account during all phases of the development process (security by design)					X	
Products are placed on the market with the most secure settings enabled by default (security by default)					X	
Hardware manufacturers and software developers should make available to relevant stakeholders (e.g. end-users) a list containing the details and supply chain relationships of various components used in building the digital product (so-called (Software) Bill of Materials)				X		
Products should be designed in such a way that they are fully updatable					X	

	1	2	3	4	5	Don't know / no opinion
Hardware manufacturers and software developers provide updates when vulnerabilities are discovered, including after a product has been put on the market				X		
Hardware manufacturers and software developers should provide updates free of charge					X	
Hardware manufacturers and software developers facilitate vulnerability disclosure (e.g. by public authorities; independent researchers)				X		
Products must feature all the necessary functional (e.g. two-factor authentication) and non-functional (e.g. resilience against DDoS (Distributed Denial of Services) attacks) security requirements		X				

Which other measures taken by hardware manufacturers and software developers could improve the cybersecurity of digital products?

1000 character(s) maximum

Security testing (own or from an external independent party) should be integrated. This would include incorporating security testing through specific tools, code review etc. These practices should be current, updated and implemented by competent personnel. Continuous education, training and assessment of the personnel of the organization to the specific requirements, implementation mechanisms, secure coding principles, etc.

## Sub-section 2.f. – The role of risk

**Q18:** Under this initiative, hardware manufacturers and software developers would need to demonstrate their compliance with cybersecurity requirements. Should digital products with a higher risk be subject to a stricter process of demonstrating conformity with these requirements?

✓ -- Yes

No

Don't know / no opinion

## Sub-section 2.g. – Demonstrating compliance with security requirements

**Q19:** How would you assess the following statement regarding self-declaration as a way for hardware manufacturers and software developers to demonstrate compliance with security requirements (on a scale from 1 to 5 with 5 indicating that you strongly agree)?

	1	2	3	4	5	Don't know / no opinion
A self-declaration of conformity by a hardware manufacturer or software developer gives a sufficient confidence that security requirements are met		X				

**Q20:** If you consider that self-declaration is not enough to demonstrate compliance with security requirements, do you think that the involvement of a third party should be required under certain circumstances?

YES

Please elaborate, *1000 character(s) maximum*

Third parties (private or public) should be involved, and depending on the risk profile of the product or service should provide verification and conformity assessment services. For example, for products / services belonging to the low risk categories, self assessment could be used provided that there is a control (oversee mechanism) and enforced penalties for the parties found to have mislead/ wrongly declared either after investigation because of an incident, or after the sampling control mechanisms /audits implemented. In the case of products / services belonging to the medium / high risk categories, third party conformity assessment methods should be implemented.

## Section 3: Stakeholder impact of potential regulatory measures

This section focuses on the EU added value and estimated impacts of potential measures on stakeholders.

### Sub-section 3.a. – Relevance of horizontal requirements for digital products at European level

**Q21:** To what extent do you agree with the following statements that look into the potential effectiveness of an EU initiative on horizontal (cross-sectoral) cybersecurity requirements?

	Strongly disagree	Disagree	Agree	Strongly agree	Don't know / no opinion
Cyber risks can propagate across borders and sectors at high speed, which is why cybersecurity rules for digital products should be aligned at Union level			X		
Horizontal cybersecurity requirements for digital products would increase awareness of users when it comes to cyber risks			X		
Horizontal cybersecurity requirements for digital products would enhance and ensure a consistently high level of the security of digital products and ancillary services				X	
Horizontal cybersecurity requirement would improve the functioning of the internal market by levelling the playing field for vendors of digital products and ancillary services as regards cybersecurity features				X	

**Q22:** The [EU Action Plan on synergies between civil, defence and space industries](#) underlines the importance of promoting and applying common standards across sectors and the increased relevance of digital products that are used both in a civilian and military context ('dual-use products'). To what extent could horizontal requirements applying to digital dual-use products contribute to moving the security performance of such products closer to the needs of the defense community and to raising the overall level of cybersecurity in civilian uses (on a scale from 1 to 5 with 5 indicating a very positive contribution)?

4

Please elaborate, 1000 character(s) maximum

Identify existing innovative EU cyber products and innovative prototypes that can meet the needs of both the EU civilian and military industrial markets. Bring the two communities (civilian and military integrators) together to upgrade existing cyber products and prototypes to meet their requirements. Avoid double-spending by strengthening the prospects of EU civilian and military maritime industrial markets; by shaping, implementing and coordinating industrial, military and civilian cybersecurity and cyber defence research and efforts (e.g. programs, activities, funds).



### Sub-section 3.b. – Impact on your organisation in terms of cost

**Q23:** How would you assess the impact of the following types of intervention on the costs of your organisation (on a scale from 1 to 5 with 5 indicating that the intervention would be very costly)?

	1	2	3	4	5	Don't know / no opinion
Guidelines or recommendations for the development of secure digital products issued at EU level addressed to vendors	X					
Further voluntary European cybersecurity certification schemes for digital products and services			X			
EU public procurement guidelines taking into account cybersecurity requirements		X				
Amending existing legislation regulating specific products with a digital dimension (such as the legislation on lifts or gas appliances)			X			
Introducing mandatory horizontal cybersecurity requirements for hardware products			X			
Introducing mandatory horizontal cybersecurity requirements for software products			X			

Please elaborate your answer, by quantifying the costs if possible, *1000 character(s) maximum*  
Any mandatory requirements that need to be implemented, would incur cost for the organization. The implementation of security by design, testing and training of the relevant personnel would lead to increased costs for the organizations. Also, mandatory requirements usually are accompanied by penalties which will also incur costs.

### Sub-section 3.c. – Regulatory burden and costs for small and medium-sized companies

**Q24:** Which of the following approaches would in your view ensure that small and medium-sized hardware manufacturers and software developers, including individual entrepreneurs, are subject to proportionate obligations (balance between administrative burden and compliance costs on the one hand and a high level of cybersecurity on the other hand) under a European legislation introducing mandatory horizontal cybersecurity requirements (on a scale from 1 to 5 with 5 indicating that you strongly agree with a statement)?

	1	2	3	4	5	Don't know / no opinion
Subject small and medium-sized companies to the same obligations as larger companies				X		
Introduce simplified procedures to demonstrate conformity for small companies and individual entrepreneurs				X		

Which other approaches could ensure proportionate obligations vis-à-vis small and medium-sized hardware manufacturers and software developers, including individual entrepreneurs?, 1000 character(s) maximum

Even a small organization may produce / market a device that may have a great penetration to the market and if compromised could affect great impact on organizations and individual users. So, the SME customization should be done not on the point of the requirement but rather on the method and funding mechanisms that could be customized and provided to the SMEs.

### Sub-section 3.d. – Impact on competition

**Q25:** An EU initiative laying down mandatory horizontal cybersecurity requirements would apply to all vendors placing products on the internal market, irrespective of their origin and location. To what extent would you agree with the following statements regarding the impact on competition of such an initiative (on a scale from 1 to 5 with 5 indicating that you strongly agree with a statement)?

	1	2	3	4	5	Don't know / no opinion
Mandatory cybersecurity requirements will put smaller hardware manufacturers and software developers at a disadvantage compared with larger competitors				X		
Mandatory cybersecurity requirements will put EU manufacturers and software developers at a disadvantage on the non-EU markets compared to non-EU competitors that are not subject to such requirements			X			

### Sub-section 3.e. – Impact on fundamental rights

**Q26:** To what extent to you agree with the following statements regarding the impact of horizontal cybersecurity requirements on fundamental rights (on a scale from 1 to 5 with 5 indicating that you strongly agree with a statement)?

	1	2	3	4	5	Don't know / no opinion
Horizontal cybersecurity requirements for digital products would enhance protection of privacy and personal data					X	
Horizontal cybersecurity requirements for digital products would ensure a high level of consumer protection				X		

## Section 4: Other issues

**This section focuses on cybersecurity challenges for the internal market other than those related to digital products.**

**Q27:** In addition to the issues above, are there other cybersecurity related challenges not directly linked to the cybersecurity of products that you think the Cyber Resilience Act should include to enhance the cyber resilience of the internal market? Please elaborate, *1000 character(s) maximum*

The importance of cybersecurity has been fully recognized and emphasized for the implementation of the EDI Strategy (SWD(2019), 1240 final) as well as its compliance with all cyber security legislative framework and strategies (e.g. NIS-2 Directive, Cybersecurity Act, GDPR, eID, EPCIP, TNCEIP, and the European Cybersecurity Certification Act). All these aims to increase citizens' confidence in a trustworthy Digital Single market. In addition, it's increasingly important for the industry stakeholders **to build up knowledge and develop skills related to** cybersecurity and also to undertake actions to enhance their cybersecurity preparedness.

## **7.2 Feedback on the consultation to the amendment of the Cybersecurity Act**

The following represents a transcript of the feedback provided to the online consultation system of the EC. This consultation did not have questions, but rather provided a space (limited to 4.000 characters) for feedback and the ability to add also a document as attachment. Within the following space, both the feedback text and the document that was attached are depicted.

### **Feedback:**

The AI4HEALTHSEC project salutes the inclusion of managed security services in the scope of the Cybersecurity Act (Regulation (EU) 2019/881) as one of the ways to strengthen resilience and capacities to protect . Services, and specifically ICT services i.e., services consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems were already included within the scope of the Cybersecurity Act, and have been already identified as playing a vital role in society and have become the backbone of economic growth. The ICT supply chain security is critical to the effective, resilient and secure operation of organizations. This is why it is imperative that security service providers (as part of the supporting structure supply chain of organizations) that can (under guarantee) provide security services at the required assurance level exist within the European Market. Comments For the inclusion of managed security services to be effective and allow for the design and implementation of useful certification schemes, it is important the definition of managed security services is clear and the scope of the resulting certification schemes is specific. Managed security services (or trusted cybersecurity services , trusted services ) are, within the proposal for amendment, defined as: - (14a) managed security service means a service consisting of carrying out, or providing assistance for, activities relating to cybersecurity risk management, including incident response, penetration testing, security audits and consultancy; The above definition is aligned to NIS(2), Directive (EU) 2022/2555 and the EU Cyber Solidarity Act and adds consultancy to the type of services provided in assistance for, activities relating to their customers cybersecurity risk management. BUT, the definition does not provide a distinction regarding what makes a cybersecurity (or security) service a managed service. The AI4HEALTHSEC project, strongly recommends that the term be further clarified and this clarification is taken into consideration in the creation of the relevant certification schemes. Since, managed security service providers are considered also as part of the NIS(2), this further clarification would support those related processes also. In the attached file, you can find a more formulated answer with relevant references and examples.

### **Attached document:**

The AI4HEALTHSEC project **salutes** the inclusion of managed security services in the scope of the Cybersecurity Act (Regulation (EU) 2019/881) **as one of the ways to “strengthen resilience and capacities to protect”<sup>30</sup>**.

Services, and specifically ICT services – i.e., services consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems<sup>31</sup>– were already included within the scope of the Cybersecurity Act, and have been already identified as playing “a vital role in society and have become the backbone of economic growth”<sup>32</sup>.

As noted also in Council conclusions on ICT supply chain security - Council conclusions approved by the Council at its meeting on 17 October 2022<sup>33</sup>:

- the character of the risks associated with ICT supply chain, which is composed of a linked set of resources and processes between economic operators (as defined in Regulation (EU) 2019/1020) that begins with the sourcing of raw material and extends through the manufacturing, processing, handling and delivery of ICT products and services, including provision of support during ICT products and services’ life cycle, brings unique challenges and potentially far-reaching consequences.
- .... it is equally important to strengthen the overall resilience and security of ICT supply chains against the whole variety of threat factors, such as natural events, system failures, insider threats, or human errors. In this sense, RECOGNISES that ICT supply chain security encompasses ensuring the protection of ICT products and services produced, delivered, procured and used in ICT supply chains, including by means of protecting individual components and transmitted data.

The ICT supply chain security is critical to the effective, resilient and secure operation of organizations. This is why it is imperative that security service providers (as part of the supporting structure – supply chain of organizations) that can (under guarantee) provide security services at the required assurance level exist within the European Market.

For the inclusion of managed security services to be effective and allow for the design and implementation of useful certification schemes, it is important the definition of managed security services is clear and the scope of the resulting certification schemes is specific.

---

<sup>30</sup> Text from the approved conclusions by the Council on developing the Union’s cyber posture - 23rd of May 2022 - <https://www.consilium.europa.eu/en/press/press-releases/2022/05/23/cyber-posture-council-approves-conclusions/>

<sup>31</sup> Definition 13, Article 2 of the Regulation (EU) 2019/881

<sup>32</sup> Recital 1, Regulation (EU) 2019/881

<sup>33</sup> <https://data.consilium.europa.eu/doc/document/ST-13664-2022-INIT/en/pdf>

Managed security services (or trusted cybersecurity services<sup>34</sup>, trusted services<sup>35</sup>...) are, within the proposal for amendment, defined as:

- (14a) ‘managed security service’ means a service consisting of carrying out, or providing assistance for, activities relating to cybersecurity risk management, including incident response, penetration testing, security audits and consultancy’;

The above definition is aligned to NIS(2), Directive (EU) 2022/2555 and the EU Cyber Solidarity Act and adds consultancy to the type of services provided in assistance for, activities relating to their customers’ cybersecurity risk management.

**BUT**, the definition does not provide a distinction regarding what makes a cybersecurity (or security) service – a managed service.

The AI4HEALTHSEC project, **strongly recommends** that the **term be further clarified** and this clarification is taken into consideration in the creation of the relevant certification schemes.

Since, managed security service providers are considered also as part of the NIS(2), this further clarification would support those related processes also.

Although, we could not find an official definition for managed security services, we provide the following text to highlight the issue that may arise from the generic nature of the definition:

Based on Gartner<sup>36</sup>,

“A managed service provider (MSP) delivers services, such as network, application, infrastructure and security, via ongoing and regular support and active administration on customers’ premises, in their MSP’s data center (hosting), or in a third-party data center.

MSPs may deliver their own native services in conjunction with other providers’ services (for example, a security MSP providing sys admin on top of a third-party cloud IaaS). Pure-play MSPs focus on one vendor or technology, usually their own core offerings. Many MSPs include services from other types of providers. The term MSP traditionally was applied to infrastructure or device-centric types of services but has expanded to include any continuous, regular management, maintenance and support.”

This definition includes the following characteristics:

---

<sup>34</sup> Conclusions on developing the Union’s cyber posture of the Council.

<sup>35</sup> proposal for a regulation laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents

<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52023PC0209>

<sup>36</sup> <https://www.gartner.com/en/information-technology/glossary/msp-management-service-provider>

- ongoing and regular support
- active administration from any location (even on customers' premises)
- in conjunction with other services
- technology or vendor focused
- continuous, regular management,
- continuous, regular maintenance and
- continuous, regular support.

If this definition is adapted to fit managed security services, then this would mean that:

- cybersecurity services like consulting on security architecture – provided once by the provider of the service would be excluded. [Although based on the definition of the proposed amendment they would be considered as included - a service consisting of providing assistance for, .... Consultancy.]
- cybersecurity services like provision and customization of technological solutions and tools for the cybersecurity risk management of an organization would be excluded. [Although based on the definition of the proposed amendment they would be considered as included - a service consisting of providing assistance for relating to cybersecurity risk management.....]

## About AI4HEALTHSEC

The AI4HEALTHSEC project, a project receiving funding from the European Union's Horizon 2020 research and innovation programme, under Grant Agreement 883273, aims to provide a solution that improves the detection and analysis of cyber-attacks and threats on Health Care Information Infrastructures, and increase the knowledge on the current cyber security and privacy risks.

Two of the main topics of the project are Cybersecurity Risk Assessment and Incident Response. The final aim of the project is to provide a tool and service to provide evidence based risk assessment to organizations, allow for the collaboration between the entities of the supply chain on threat information sharing and incident response.

As such we believe that the project consortium, is in a position to provide relevant feedback to this consultation.