Position Paper

of the **AI4HealthSec*** and **HEIR**** projects on the **Regulation** of the European Parliament and of the Council laying down **measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union**.

© Image by rawpixel.com on Freepik

JULY 2023

* The AI4HealthSec project has received funding from the European Union's Horizon 2020 research and innovation program, under Grant Agreement 883273.

** The HEIR project has received funding from the European Union's Horizon 2020 Research and Innovation program under Grant Agreement 883275.

Ai4HealthSec

HEIR

Executive Summary

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

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

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

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

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

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

The new processes that will consider big data must ensure full compliance with the underlying data protection EU regulations, have a clear legal basis, be proportionate and ensure accountability for those processing them. As such, synergies when data is been managed within the context of

cybersecurity and personal data protection are necessary so that citizens' rights to the protection of personal data and privacy do not slip and ensuring that mechanisms to be imposed must be clear, traceable, homogeneous, transparent, effective and correctly complement the existing legislation on personal data protection.

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

"A high level of security is achieved by implementing preventive controls and effective response"

Introduction

On the 22nd of March 2022, the European Commission published a Proposal for a 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 Proposal). The Council subsequently, in November 2022, adopted its position on a draft regulation aimed at ensuring a high common level of cybersecurity across the EU institutions, bodies, offices and agencies, and it is now ready to start trilogues with the European Parliament, once the Parliament has voted on its negotiating mandate.

This proposal is aimed at increasing the cybersecurity resilience of the Union institutions, bodies and agencies against cyber threats, while aligning with existing legislation as identified within the relevant proposal.

This proposal establishes a framework for ensuring common cybersecurity rules and measures among the Union institutions, bodies and agencies. It aims at further improving all entities' resilience and incident response capacities. It is in line with the Commission's priorities to make Europe fit for the digital age and to build a future-ready economy that works for the people. Moreover, ensuring a secure and resilient public administration is a cornerstone in the digital transformation of society as a whole.

This proposal builds on the EU Security Union Strategy (COM(2020) 605 final) and the EU's Cybersecurity Strategy for the Digital Decade (JOIN(2020) 18 final).

With this position paper, the AI4HealthSec project would like to provide views and suggestions on the Proposal from the perspective of a collection of entities and a project highly involved with Risk Management and Incident Response within organizations identified as critical infrastructures.

Background

The legal basis for this Regulation is Article 298 of the Treaty on the Functioning of the European Union (TFEU) which provides that in carrying out their missions, the institutions, bodies, offices and agencies of the Union shall have the support of an open, efficient and independent European administration. In compliance with the Staff Regulations and the Conditions of Employment adopted on the basis of Article 336, the European Parliament and the Council, acting by means of regulations in accordance with the ordinary legislative procedure, shall establish provisions to that end.

Information technology has provided new ways for Union institutions, bodies and agencies to work, interact with citizens and improve overall operations. As technology continues to evolve, the cyber threat landscape evolves along with it. Union institutions, bodies and agencies have become highly attractive targets of sophisticated cyberattacks. The establishment of systems and requirements to ensure cybersecurity appears to be contributing to the efficiency and the independence of the European administration, so that Union institutions, bodies, offices and agencies can operate in a more efficient manner in a digital world in the conduct of their missions.

From 2019 to 2021, the number of significant incidents[1] affecting Union institutions, bodies and agencies, authored by advanced persistent threat (APT) actors, has surged dramatically. The first half of 2021 saw the equivalent in significant incidents as in the whole of 2020. This is also reflected in the number of forensics images (snapshots of the contents of affected systems or devices) CERT-EU analysed in 2020, which tripled in comparison to 2019, while the number of significant incidents rose more than ten-fold since 2018.

The Commission has carried out an evaluation of the cybersecurity functioning of 20 Union institutions, bodies and agencies. This provided insight into established cybersecurity practices, and cybersecurity management capabilities with external benchmarking of some technical security controls. This evaluation concluded amongst others that:

- Cybersecurity maturity, IT infrastructure size and levels of capability vary substantially among the evaluated Union institutions, bodies and agencies.

[1] 'Significant incident' means any incident unless it has limited impact and is likely to be already well understood in terms of method or technology.

- Whereas there are mature detection and response capabilities among many Union institutions, bodies and agencies in general, there are varying levels of integrated risk management in their cybersecurity governance capabilities.

The structure

The structure of the proposal is the following:

The AI4HEALTHSEC & HEIR position

The AI4HEALTHSEC and HEIR projects, have selected some parts of the proposal and have provided relevant comments in the sections that follow. These sections are structured in a way to facilitate traceability.

The comments of the AI4HealthSec & HEIR projects cover parts of the following Articles: 4,5,7,8,9,11,12,13,14 and Chapter V.

Article 4 Risk management, governance and control

1. Each Union institution, body and agency shall establish its own internal cybersecurity risk management, governance and control framework ('the framework') in support of the entity's mission and exercising its institutional autonomy….

2. The framework shall cover the entirety of the IT environment of the concerned institution, body or agency, including any on-premise IT environment, outsourced assets and services in cloud computing environments or hosted by third parties ….

Comments

The AI4HealthSec & HEIR projects fully agree that each Union institution, body and agency needs to first design and then implement a cybersecurity risk management, governance and control framework ('the framework'), to ensure an effective and prudent management of all cybersecurity risks, and takes account of business continuity and crisis management. Risk management as stated also in various international best practices, should be in the center of any cybersecurity practice and should be an effective decision-making tool.

As mentioned in the recently updated publication by ENISA on Interoperable EU Risk Management Framework[2], "The risk management area is characterized by a plethora of frameworks, methodologies and methods, each of them with their own characteristics and following their own approach in managing risks.".

[2] https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework, **updated in January 2023**

We believe, that this part of the proposal should be enriched with at least one or more of the following:

- guidance on the minimum components of the cybersecurity risk management, governance and control framework. [Although in general the terms of cybersecurity risk management, governance and control may be understood by the various interested parties, this does not mean that the combination of these terms and what is needed to be done to fulfill this requirement is understood also. A guidance could be provided to indicate what the meaning of this framework is, what the meaning and purpose of each term are and which are the minimum components that should be included in such a construct.]
- to further assist the entities in the implementation processes, further information on methodologies / standards or tools could be provided. One path towards this could be the provision of a reference to acceptable, reliable and established standards, methodologies and tools for cybersecurity risk management that fulfill the minimum requirements (as mentioned in the previous point). This reference to such standards, methodologies and tools does not have to be included in the regulation (as the information may quickly become outdated), but it could be incorporated in the guidance prescribed to be provided by the IICB. [As risk management represents the starting point and the source of the decision-making process on cybersecurity controls, some more information should be provided on which methodologies could be used to achieve the desired results if implemented correctly.]
- the basic principles regarding cybersecurity risk management, governance and control that need to be adhered to.

All of the above, would be really helpful to the Union institutions, bodies and agencies that need to implement the proposal and would also ensure (to a degree) that the interested parties produce valuable, comparable and reproducible results.

5. Each Union institution, body and agency shall appoint a Local Cybersecurity Officer or an equivalent function who shall act as its single point of contact regarding all aspects of cybersecurity.

Comments

Considering the complex context and interdependences of the cybersecurity baseline, the role of a Local Cybersecurity Officer or an equivalent function should be scoped to fulfill the demand for single point of contact regarding all aspects of cybersecurity. In addition, the Local Cybersecurity Officer or the equivalent function should be involved in a local change management process of an institution, body, office or agency of the Union.

Both the highest level and the senior management should be in a regular dialog with a Local Cybersecurity Officer in order to be up-to-date on its institutional IT environment and have a common understanding about weak points and its impact to meet the cybersecurity baseline.

Article 5 Cybersecurity baseline

1. *The highest level of management of each Union institution, body and agency shall approve the entity's own cybersecurity baseline to address the risks identified under the framework referred to in Article 4(1). It shall do so in support of its mission and exercising its institutional autonomy. The cybersecurity baseline shall be in place by ……. at the latest [18 months after the entry into force of this Regulation] and shall address the domains listed in Annex I and the measures listed in Annex II.*
2. *The senior management of each Union institution, body and agency shall follow specific trainings on a regular basis to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risk and management practices and their impact on the operations of the organization.*

Comments

The AI4HEalthSec & HEIR projects acknowledge that cybersecurity falls within the responsibility of the highest level of management of each Union institution, body and agency.
It should be stated also, that cybersecurity is a complex domain and a cybersecurity baseline as defined within this proposal[3], is expected to be a complex and relatively technical document.
To that effect, the provision stated in point 2. of this article, is very much needed but should not be restricted to the senior management of each Union institution, body and agency. Since the approval falls under the highest level of management of each Union institution, body and agency, this requirement should also include this level also. In this case, the trainings should focus on providing an understanding on the types of cybersecurity risks, on the cybersecurity risk management principles, on the shortcomings of any such methodologies, on the types of measures implemented etc. When constructing and delivering such trainings, there should be no specific cybersecurity knowledge taken as a pre-requisite.
In Annex I, the proposal identifies domains of cybersecurity in alignment with well known standards like ISO 27002:2013[4]. Where the definition of cybersecurity used is "'cybersecurity' means the activities necessary to protect network and information systems, the users of such systems, and other persons

[3] 'cybersecurity baseline' means a set of minimum cybersecurity rules with which network and information systems and their operators and users must be compliant, to minimise cybersecurity risks**.**
[4] The alignment of the domains is only true for the version of 2013. In 2022, the new version of ISO 27002 no longer groups the information security controls in these domains. Instead the controls are split into Organizational, Technological, Physical and Human.

affected by cyber threats"[5]. The authors of this document believe, that based on this definition the related topics also include privacy (apart from confidentiality, integrity and availability), and for this reason, the AI4HealthSec & HEIR projects propose that controls related to privacy should also be included within the Annex I domains.

Specifically, Privacy by design (PbD) is a very important process including good (privacy related) practices in the operation and design of information technology (IT) systems, business practices and physical infrastructures. PbD aims at securing privacy and obtaining control over personal information to get a competitive and sustainable advantage on top of organizations. Critical infrastructures would be benefiting greatly from PbD, meaning that privacy is taken into consideration during the initial stages and is then implemented with the relevant controls already incorporates, rather than trying to comply and adjust afterwards.

Considering the already confirmed incompatibility ("*best practices were found to be unevenly applied by the evaluated Union institutions*") in the application of technical measures and good practices, along with unwillingness in disclosing information about cybersecurity incidents, guidance towards complying/integrating the requirements mentioned in Annex I and Annex II, we believe will boot harmonization.
Embedding the adoption of the PbD (as mentioned above) and "Security by Design" principles as a fundamental aspect to recommendations may lead to in a significant reduction of cybersecurity incidents exploiting basic vulnerabilities.

[5] REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

Article 6 Maturity Assessments

Each Union institution, body and agency shall carry out a cybersecurity maturity assessment at least every three years, incorporating all the elements of their IT environment as described in Article 4, taking account of the relevant guidance documents and recommendations adopted in accordance with Article 13.

Comments

The AI4HealthSec & HEIR projects identify the value of incorporating a cybersecurity assessment process as part of the identification of the current state of the organization in relation to cybersecurity controls and their maturity.

As described in Dams-C2M2, "A maturity model provides a benchmark against which an organization can evaluate the current capability level of its practices, processes, and methods and set goals and priorities for improvement. When a model is widely used in a particular industry (and assessment results are shared), organizations can also benchmark their performance against other organizations. An industry can determine how well it is performing overall by examining the capability of its member organizations."[6]

It should be pointed out though, that the text included in the proposal for regulation does not provide enough information for the cybersecurity maturity concept understanding and implementation. Specifically,

- The requirement does not indicate the purpose (aim) of designing and implementing a cybersecurity maturity model and framework for the organization to run periodically. It is not clear whether: The cybersecurity maturity assessment will be used for the assessment of the implementation of the controls (in the way that you would expect a cybersecurity audit or security assessment to be carried out). Or if the cybersecurity maturity assessment is an instrument to support the cybersecurity risk management (and especially the analysis of risks).
- No information is provided regarding the type of cybersecurity maturity used as part of these assessments. Literature has identified at least two main categories of cybersecurity maturity models. One of these categories is referred as Capability Maturity model. A Capability Maturity Model provides organizations with guidance on how to gain control of their processes for a

[6] https://www.cisa.gov/sites/default/files/publications/dams-c2m2-508.pdf

specific purpose and how to evolve toward excellence.[7] While the other category is referred as Process Maturity Models. In this category, the maturity models include levels which rank the maturity of processes from highest to lowest. The least is characterized by inconsistent management practices or teams that react to crises rather than predict them. Whereas, the highest levels are characterized continually improving.

As in the case with Article 5, we believe, that this part of the proposal should be enriched with:
A definition and guidance on the envisioned type of cybersecurity maturity model to be utilized as well as a clear iteration of what is the purpose served by the relevant periodic assessments and
Furthermore, as identified in the section above regarding risk management, guidance should be provided on the minimum components, principles and operations of the envisioned cybersecurity maturity model. This guidance should be enriched with a reference to already acceptable and established models.

[7] This definition has been adapted from the one included in "Technical Report CMU/SEI-93-TR-024, ESC-TR-93-177, February 1993, Capability Maturity Model [SM] for Software, Version 1.1, Software Engineering Institute, Carnegie Mellon University.

Article 7 Cybersecurity plans

1. Following the conclusions derived from the maturity assessment and considering the assets and risks identified pursuant to Article 4, the highest level of management of each Union institution, body and agency shall approve a cybersecurity plan without undue delay after the establishment of the risk management, governance and control framework and the cybersecurity baseline.

Comments

In Articles 5-7, a collection of elements that together are interrelated and together form the current and future (envisioned) status of the organizations. Specifically, the mandated elements are: risk assessment, cybersecurity baselines, results of cybersecurity maturity assessments and cybersecurity plans. Due to this complexity and to achieve a more effective implementation of this and other requirements introduced through this proposal, it is suggested to develop and establish 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. This includes advanced operational capabilities like early detection through automated real-time data aggregation and log collection, analysis and data correlation, incident forensics and information sharing – with the goal to achieve better prediction and management of cybersecurity threats.

Article 8 Implementation

1. Upon completion of maturity assessments, the Union institutions, bodies and agencies shall submit these to the Interinstitutional Cybersecurity Board. Upon completion of security plans, the Union institutions, bodies and agencies shall notify the Interinstitutional Cybersecurity Board of the completion.
2. Guidance documents and recommendations, issued in accordance with Article 13, shall support the implementation of the provisions laid down in this Chapter.

Comments

The AI4HealthSec & HEIR projects, perceive the value of the proposed activity by the Union institutions, bodies and agencies, to document and provide the maturity assessment results to the Interinstitutional Cybersecurity Board. It should be pointed out that in order for this activity to be as effective as possible, the methodology and maturity models utilized by the Union institutions, bodies and agencies should be at least comparable (interoperable). In this way the Interinstitutional Cybersecurity Board, will have the ability not just to collect but also effectively and efficiently evaluate the collected information and extract (to the extend possible) benchmarking results.

Article 9 Interinstitutional Cybersecurity Board

2. The IICB shall be responsible for:
(a)monitoring the implementation of this Regulation by the Union institutions, bodies and agencies;
(b)supervising the implementation of general priorities and objectives by CERT-EU and providing strategic direction to CERT-EU….

Comments

Considering that the imposed cybersecurity monitoring might have implications for personal data security, an additional responsibility for IICB should be the collaboration with the European Data Protection Supervisor (EDPS). Having this synergy in place, potential conflicts between the pursuit of cybersecurity objectives and protection and privacy of individuals is minimised only to those resulting from the requirements of Article 52(1) of EU Charter of Fundamental Rights (i.e., backed by legislation, necessary and proportionate, and respecting the essence of the right).

Article 11 Compliance

1. The IICB shall monitor the implementation of this Regulation and of adopted guidance documents, recommendations and calls for action by the Union institutions, bodies and agencies.

Comments

Considering that actors (Article 3, def. 1) in their effort to monitor cybersecurity posture they do not practice privacy conformance assessments to determine whether collected evidence (e.g., networking data, databases logs, connected devices identifiers, access control logs) might lead to identification (either from direct collection of personal data or from their association), privacy assessments must be also imposed and monitored to provide evidence that any cybersecurity process does not jeopardize the data protection and privacy framework, and that cybersecurity operations are integrated and managed in an accountable way. Such compatibility to be monitored as well by IICB.
Control procedures and resulting recommendations should consider the privacy and data protection framework as well to foster synergies to avoid duplication of efforts. To promote such synergy, IICB to foster the cooperation between the LCO (article 4, par. 5) and the DPO, and provide guidance to avoid overlapping activities.
SPHYNX - Ioannis Basdekis

Article 12 CERT-EU mission and tasks

1. The mission of CERT-EU, the autonomous interinstitutional Cybersecurity Centre for all Union institutions, bodies and agencies, shall be to contribute to the security of the unclassified IT environment of all Union institutions, bodies and agencies by advising them on cybersecurity, by helping them to prevent, detect, mitigate and respond to incidents and by acting as their cybersecurity information exchange and incident response coordination hub. ….

Comments

There is no reference on Guidance documents and recommendations that should be provided to CSIRTs and the support of the CERT-EU task for cyber threat intelligence, including situational awareness.
At a minimum, the article should include the minimum requirements that such methodologies should comply with. In addition, it is recommended that the IICB also provides guidance documents and recommendations on incident management practices that should be adopted by CSIRTs.
Moreover, the tasks and responsibilities mentioned within this document do not reference any link between this proposal and proposal for the Cyber Resilience Act. (There are measures included within the proposal for the Cyber Resilience Act related to products and maturity assessment that could be important to this proposal and the affected organizations).
Article 12 of the proposal lays out clear indications as to the missions of the CERT-EU. The article showcases an emphasis on the cooperative methodology that is undertaken by the CERT-EU. For instance, we notice that, in its 4th point, the article highlights “cooperation with the European Union Agency for Cybersecurity on capacity building, operational cooperation […]”.
In this context, we point out the possibility of expanding and explicating the cooperation potential of the CERT-EU with the European Data Protection Supervisor regarding the usage and threats that concern personal data.
We highlight that cybersecurity incidents can in fact result in personal data breaches that have variable but often serious consequences; In AI4HEALTHSEC, for instance, we approached health-related personal data that are considered sensitive special-category data in European instruments such as the GDPR and EUDPR.
For this reason, we foresee the possibility in this article of better highlighting the possible synergies that can be created between the CERT-EU and the European Data Protection Supervisor in frequent cases where cybersecurity incidents imply a breach of personal data.
We believe that this cooperation between the two entities can benefit both the operational measures to counter cyber incidents and vulnerabilities, as well as the overall goal of capacity building and increasing the resilience of the IT infrastructure of European institutions, bodies, and agencies.

In regard to the missions of the CERT-EU, emphasis can also be put on the need of clarifying legal grounds on which the CERT-EU will rely when processing personal data contained in the information that is transferred by the entities “without undue delay ”. Such clarifications are to be made in accordance with the European Union Data Protection Regulation (EUDPR).

Finally, on this subject, it should be pointed out that there is no link perceived between the CERT-EU and Standard Developing Organizations (SDOs). The AI4HealthSec & HEIR projects believe that such a connection would be of importance and value especially for CERT-EU tasks Article 13. 1. (b) and (c) (The provision to the IICB proposals for guidance documents and recommendations).

Article 13 Guidance documents, recommendations and calls for action

2. Guidance documents and recommendations may include:
(a)modalities for or improvements to cybersecurity risk management and the cybersecurity baseline
(b)modalities for maturity assessments and cybersecurity plans; and
(c)where appropriate, the use of common technology, architecture and associated best practices with the aim of achieving interoperability and common standards within the meaning of Article 4(10) of Directive [proposal NIS 2].

Comments

As mentioned in the comments of Article 4 and Article 6, we believe, that specific guidance needs to be provided on the subjects of cybersecurity risk management, the “framework”, the maturity models / methodology for assessment, incident management and others.
Please refer to that part of this document above.
The design and publication of such guidelines should be in line with well established international standards and where possible with the contribution or cooperation with the relevant Standard Developing Organizations (SDOs).

Article 14 Head of CERT-EU

The Head of CERT-EU shall regularly submit reports to the IICB and the IICB Chair on the performance of CERT-EU, financial planning, revenue, implementation of the budget, service level agreements and written agreements entered into, cooperation with counterparts and partners, and missions undertaken by staff, including the reports referred to in Article 10(1).

Comments

The submission period should be defined as (at least) “annual reports”.
Reports to include information on exchanging information with national counterparts in the Member States (notably including CERTs, National Cybersecurity Centres, CSIRTs), on cyber threats, vulnerabilities and incidents, on possible countermeasures and on all matters relevant for improving the protection of the actors (Article 3, def. 1).

Chapter V COOPERATION AND REPORTING OBLIGATIONS

To enable CERT-EU to coordinate vulnerability management and incident response, it may request Union institutions, bodies and agencies to provide it with information from their respective IT system inventories that is relevant for the CERT-EU support. The requested institution, body or agency shall transmit the requested information, and any subsequent updates thereto, without undue delay.

Comments

Given the regulatory framework under which national authorities (CERTs, National Cybersecurity Centres) receive information about cybersecurity incidents, the requested information should to be channeled through them.

Closing remarks

In overview, we consider that the proposal of a regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices, and agencies of the Union is an effective step toward the translation of the EU-level priority of increasing cyber resilience and countering threats and incidents.

It would be beneficial to integrate a more explicit reference to coordination between law enforcement agencies of member states and the EU-level entities in the fight against different forms of cyber criminality. This alignment can draw from ongoing work to update the international legal framework for such cooperation, mainly the Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes currently being drafted at the level of the United Nations Office on Drugs and Crime[8] (UNODC).

As an overlapping theme, we consider that the proposal can benefit from a more explicit alignment with the NIS 2.0 directive. In this sense, institutions, bodies, and agencies of the European Union should be governed by similar standards to those expected in the member states. And additional to that, more specific directions should be provided on how these requirements could be implemented (especially in the fields that have a plethora of available options e.g., Risk Management and Cybersecurity Maturity).

As a recurring space for adjustment, we note that the proposal focuses on cybersecurity measures without ensuring enough convergence with data protection standards. We consider that cybersecurity is intrinsically linked to the issue of personal data protection. The proposal, thus, has a role to play in aligning its provisions to those of the numerous EU-level texts that deal with data protection; Most notably the European Union Data Protection Regulation (EUDPR) and the General Data Protection Regulation (GDPR).

[8] Details on Privanova's involvement in the drafting of the convention can be found by following this link: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_session/Documents/Statements/Privanova_item_4.pdf

Contributing Projects

The AI4HealthSec project proposes a state-of-the-art solution that improves the detection and analysis of cyber-attacks and threats on HCIIs, and increases the knowledge on the current cyber security and privacy risks. Additionally, AI4HEALTHSEC builds risk awareness, within the digital Healthcare ecosystem and among the involved Health operators, to enhance their insight into their Healthcare ICT infrastructures and provides them with capability to react in case of security and privacy breaches. Last but not least AI4HEALTHSEC fosters the exchange of reliable and trusted incident.

The AI4HealthSec project has received funding from the European Union's Horizon 2020 research and innovation program, under Grant Agreement 883273.

https://www.ai4healthsec.eu/
https://www.facebook.com/Ai4HealthSec
https://twitter.com/aifourhealthsec
https://www.linkedin.com/company/ai4healthsec-eu-h2020-project/
https://www.youtube.com/channel/UCc8SMxJ665QHiTqCKssPh7w

HEIR will design and deploy an Electronic Medical Devices Cybersecurity Framework that will facilitate intelligent threat identification and hunting services leading to the delivery of the envisioned Risk Assessment of Medical Applications (RAMA). The outcome of these analyses will be available to the IT personnel responsible for the medical devices. More to that, the RAMA client software will submit anonymized statistical data to a central server which will host the envisioned Observatory for the Security of Electronic Medical Devices (OSEMD). The Observatory will provide statistics for each threat identified in the EMD Risk Index Score through advanced visualization tools.

The HEIR project has received funding from the European Union's Horizon 2020 Research and Innovation program under grant agreement No 883275.

https://heir2020.eu/
https://twitter.com/h2020_heir
https://www.linkedin.com/company/heir-h2020-project/
https://www.youtube.com/channel/UC_boW9_lfvcZxNpbSlQ8acw