D4.2

The HEIR 2nd layer of services package: 1st complete version

Project number	883275
Project acronym	HEIR
Project title	A secure Healthcare Environment for Informatics Resilience
Start date of the project	September 1st, 2020
Duration	36 months
Programme	H2020-SU-DS-2019

Deliverable type	Demonstrator
Deliverable reference no.	D4.2
Workpackage	WP4
Due date	**28/02/2022 [M18]**
Actual submission date	04/04/2022

Deliverable lead	Bitdefender (BD)
Editors	Ovidiu Mihăilă
Contributors	Michalis Vakalellis (Aegis), Michalis Smyrlis (Sphynx), Stelar, Bogdan Prelipcean (BD)
Reviewers	Eftychia Lakka (FORTH), Hervé Debar (IMT)
Dissemination level	PU
Revision	1.0
Keywords	#servicespackage #heirarchitecture #heirframework #cybersecurity

Abstract

The deliverable 4.2 serves as the document presenting the achieved progress of implementing the complete version of HEIR's 2nd layer of services package. The work reflected within this report has been conducted between M13 and M18 and involved the partners' personnel active within WP4 and the connecting WPs such as WP2, WP3 and WP5.

Disclaimer

The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author`s view – the European Commission is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883275

Executive Summary

The current deliverable presents the work that has been carried out towards the delivery of the HEIR's 2nd layer of services package – the 1st complete version. The development from the initial version demonstrates the effective implementation of the 2nd layer of services within a consistent integrated framework that showcases the impact of the proposed solution across the use-cases.

The 2nd layer of services package for the intermediate version includes focuses on the following components:

I. The HEIR Global Benchmarks,
II. The HEIR Observatory,
III. The 2nd level of visualisation and
IV. The legal aspects involving the cybersecurity for the health environment.

The technical advancements achieved since the MVP version, concerning the above-mentioned components are reflected within the use-cases setting, mainly PAGNI and HYGEIA. Thus, from the mediator status between the Local RAMA Score Calculator of a single pilot (PAGNI) and the Observatory described within D4.1, now this component underwent several updates and contributes to the creation of a single Global Score that incorporates Local RAMA Scores between all the available pilots (PAGNI, HYGEIA) and allows the beneficiaries to either compare their Local RAMA score to the global one, or to identify the status of attack surface and resilience. This applies to the HEIR Observatory too. Thus, data is collected from the HEIR Aggregators deployed within the available pilots (PAGNI, HYGEIA). The HEIR Global RAMA Score Calculator consumes the collected data and provides the Global RAMA score and relevant metadata. The available results are presented in the 2nd layer of visualisation.

The intermediate version of the 2nd layer of services package serves as an advancement since the HEIR Minimum Viable Product (MVP) published by M12 and the foundation which will drive the implementation toward the release of final version (M30).

Table of Contents

List of Figures

1. Introduction

1.1 Scope and objectives

HEIR Project aims to provide healthcare units with tools and services for threat identification and cybersecurity knowledge base system. HEIR comprises four "use-cases" – two healthcare units from Greece, one from United Kingdom and one from Norway. The variations within technical infrastructures size, complexity and personnel, the geographic localisation together with the different regulations were considering when the HEIR architecture was initiated, designed and developed. Starting from these assumptions, the report provides the overview of the advancements, starting from the initial work reflected within deliverable D4.1 – The HEIR 2nd layer of services package for the MVP.

1.2 Relation to other Tasks and Work Packages

The current deliverable is part of ***WP4 – The HEIR Observatory*** and continues the presentation initiated by D4.1. It is regarded as an intermediate snapshot of the current status of HEIR's 2nd layer of services, between the MVP (M12) and the final version (M26). The document reflects the activities done from T4.1 to T4.4 as well as the connections with WP2, WP3 and WP5 activities:

- "D3.2 - The HEIR 1st layer of services package: 1st complete version", as the 2nd layer contains the HEIR global benchmark against which the RAMA scores of medical infrastructures will be compared.
- "D5.3 – HEIR integrated framework intermediate version" as HEIR 1st layer of services packaging will be part of the overall HEIR framework.

1.3 Structure of the document

The remainder of the document walks the reader through the three sections. Firstly, the initial version of the HEIR's 2nd layer of services is described and finalising with the conclusions. These presentation sections are complemented by the technical Annex 6 whose scope is to showcase the samples for the HEIR Global Benchmarks.

2. The HEIR 2nd layer of services.

2.1 *Overview*

This part of the current document presents an overview of architecture for the 2nd layer of services package. The following services are described below:

- the HEIR Global Benchmarks,
- the HEIR Observatory
- the HEIR 2nd layer of visualisation
- the HEIR legal.

2.2 *The HEIR Global Benchmarks*

During the MVP version of the Global RAMA Score calculator – acting as the HEIR Global benchmarks, reported in "D4.1 – The HEIR 2nd layer of services package for the MVP", the component acted as a mediator between the Local RAMA Score Calculator of a single pilot (PAGNI) and the Observatory. During the 1st complete version of the HEIR Global Benchmarks, the Global RAMA Score calculator underwent several updates contributed to the creation of a single Global Score that incorporates Local RAMA Scores between all the available pilots (PAGNI, HYGEIA, and CUH). Having said that, this allows interested parties to either compare their Local RAMA score to the global one or to identify the status of attack surface and resilience in a more "globalised" way. Moreover, as the HEIR Global benchmarks require input from the HEIR Aggregator (and subsequently the HEIR Local RAMA Score calculator and HEIR Client), extra attention was given to the development of the components of WP3. Having said that, during the final version of the HEIR Global benchmarks, HEIR aims to define benchmarks that could also be used from healthcare stakeholders in a national level. Such benchmarks will also take into consideration, were available, national regulations that need to be adopted by hospitals.

Finally, the complete 1st version of the HEIR Global benchmarks (HEIR Global RAMA Score) is a weighted sum of the three Local RAMA aggregated scores as depicted in the equation below.

$$Global\ RAMA\ Score = \sum_{i=1}^{3} LRAi$$

where i is the number of the available Local RAMA aggregated scores and LRA is the Local RAMA Aggregated score (as provided through the local HEIR Aggregator (see "D3.2 – The HEIR 1st layer of services package: 1st complete version").

The Global RAMA Score also aggregates the metadata provided by the HEIR Aggregator, such as, the top ten (10) vulnerabilities in all the involved healthcare facilities.

The Global Rama Score can also be translated in a qualitative form, as mentioned below:

- 100 = None
- 80 – 99 = Low
- 50 – 79 = Medium
- 10 – 49 = High
- 0 – 9 = Critical

A sample output of the Global Rama Score calculator is available in Appendix A.

2.2.1 HEIR Global Benchmarks deployment information

As presented in Figure 1, the local instantiation of the RAMA Score calculator will communicate with the HEIR aggregator to provide the local RAMA score as well as the above-mentioned metadata. These will constitute the main part of the HEIR's MVP Global Benchmark and will be made available to the interested parties through the HEIR Observatory module.

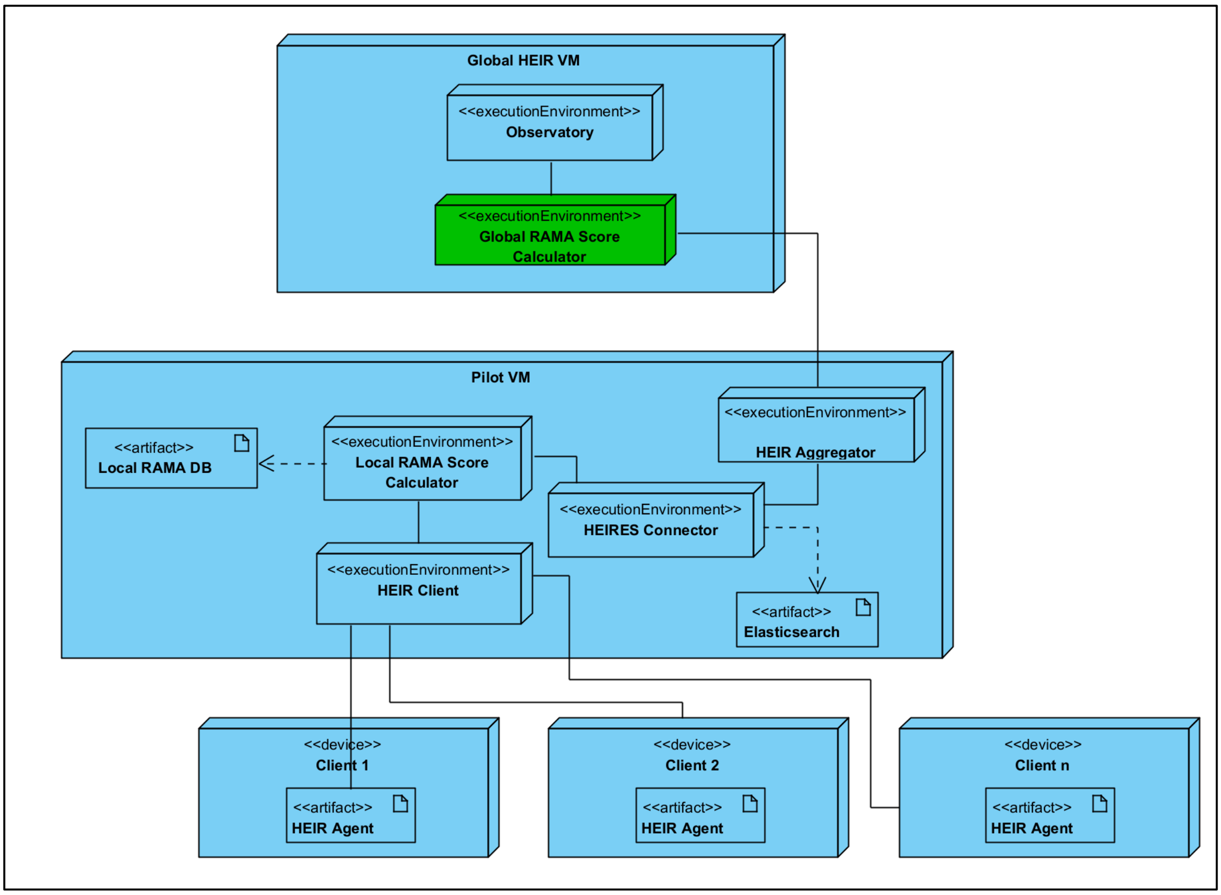


Figure 1. HEIR Global Benchmark (Global RAMA Score calculator) deployment diagram

As depicted in Figure 1,**Erreur ! Source du renvoi introuvable.** the Global RAMA Score calculator is deployed inside the Global HEIR VM and communicates with the HEIR Aggregator (receives data). The communication is being done through a Kafka message broker, over a TLS secured communication channel. Prior to transferring data from the HEIR Aggregator to the Global RAMA Score calculator, the former anonymises data (mostly metadata fed by the Local RAMA Score calculator) that might expose personal information for a specific hospital.

Lastly, the Global RAMA score and the metadata, are being visualised through the HEIR Observatory GUI (see Section **Erreur ! Source du renvoi introuvable.Erreur ! Source du renvoi introuvable.**).

A sample output of the 1st complete Global RAMA Score is available in **Erreur ! Source du renvoi introuvable.Erreur ! Source du renvoi introuvable.**.

2.3 *The HEIR Observatory*

2.3.1 The functional description

The HEIR Observatory is responsible to collect, analyse and present the results of all the deployed HEIR Clients in order to provide global insights on the level of security in healthcare environments. The Observatory database will store all this information which will be analysed by the HEIR Analytics Engine in order to produce statistics, historical analysis and trends as well as recommendations and best practices. In the current version, data will be collected from the HEIR Aggregators deployed in each hospital. The HEIR Global RAMA Score Calculator consumes the collected data, provides the Global RAMA score and relevant metadata. The available results are presented in the 2nd layer of visualisation.

2.3.2 The Component Design

The following figure depicts the high-level architecture of HEIR Observatory. The Aggregator of each hospital inside the HEIR's environment will send the aggregated RAMA score and relevant metadata as analysed in D3.2, without any hospital identifying indicator. This de-association of events sent to the repository will be applied to all clients to preserve anonymity and make any aggregated information and statistical information on cybersecurity events displayed in the observatory impossible to be connected with any particular hospital.

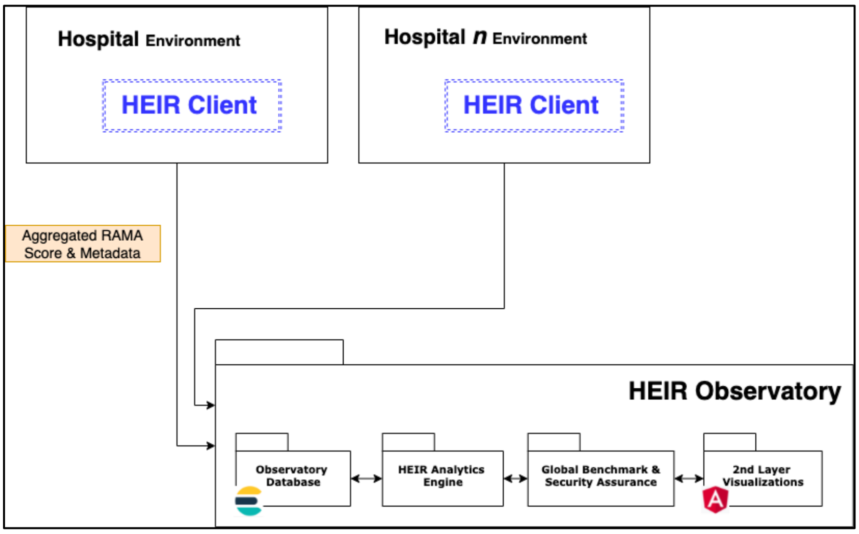


Figure 2. HEIR Observatory architecture

The technology used for the HEIR database is Elastic Search[1] which can accommodate storage, fast searching, and analysis of huge numbers of data items. It provides a RESTful API for advanced searching and aggregation queries that support statistical analysis and has built-in support for scaling operations such as automatic management of cluster-based deployments.

The 2nd layer of Visualisations has been developed as a web application as described in the next section.

[1] https://www.elastic.co/elasticsearch/

2.4 *The 2nd layer of visualisation*

2.4.1 The functional description

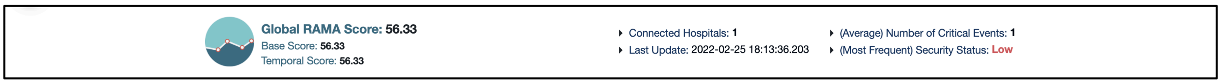
The 2nd layer of Visualisations includes all the elements and methods to present information gathered by the HEIR Observatory. Currently, the Global RAMA Score, relevant metadata and statistics are produced based on the local RAMA, derived by the connected hospitals (HEIR Aggregator). Basic recommendations are available through the visualisation dashboard.

Users accessing the HEIR Observatory will have a read-only access to data collected from the HEIR Clients.

2.4.2 The Component Design

The 2nd layer of Visualisations is a web application presenting the aforementioned information.

Figure 3 below shows how the Global RAMA Score (including the Base and the Temporal score) is presented along with significant information about the whole HEIR environment.



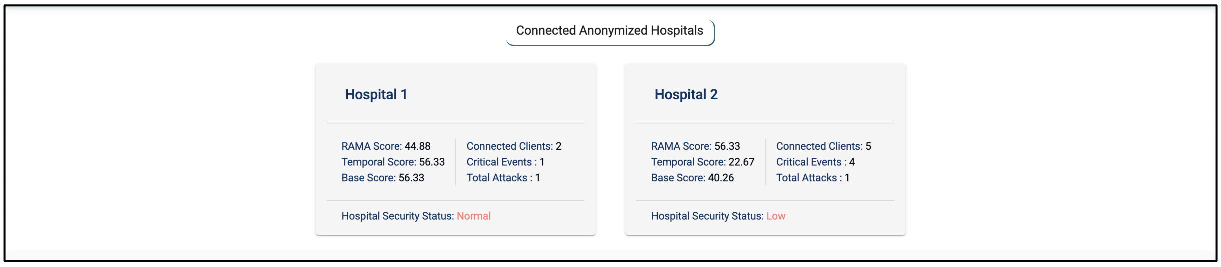
Global RAMA Score: 56.33
Base Score: 56.33
Temporal Score: 56.33

- Connected Hospitals: 1
- Last Update: 2022-02-25 18:13:36.203
- (Average) Number of Critical Events: 1
- (Most Frequent) Security Status: Low

Figure 3. Global RAMA Score

Additional security related information about the status of each connected hospital, along with analytical data that reveal meaningful information are available in an anonymized manner (i.e. no hospital will be given by name since this information will not be available as described in previous section).

Figure 4 below shows how this information is displayed.



Connected Anonymized Hospitals

Hospital 1

RAMA Score: 44.88
Temporal Score: 56.33
Base Score: 56.33

Connected Clients: 2
Critical Events : 1
Total Attacks : 1

Hospital Security Status: Normal

Hospital 2

RAMA Score: 56.33
Temporal Score: 22.67
Base Score: 40.26

Connected Clients: 5
Critical Events : 4
Total Attacks : 1

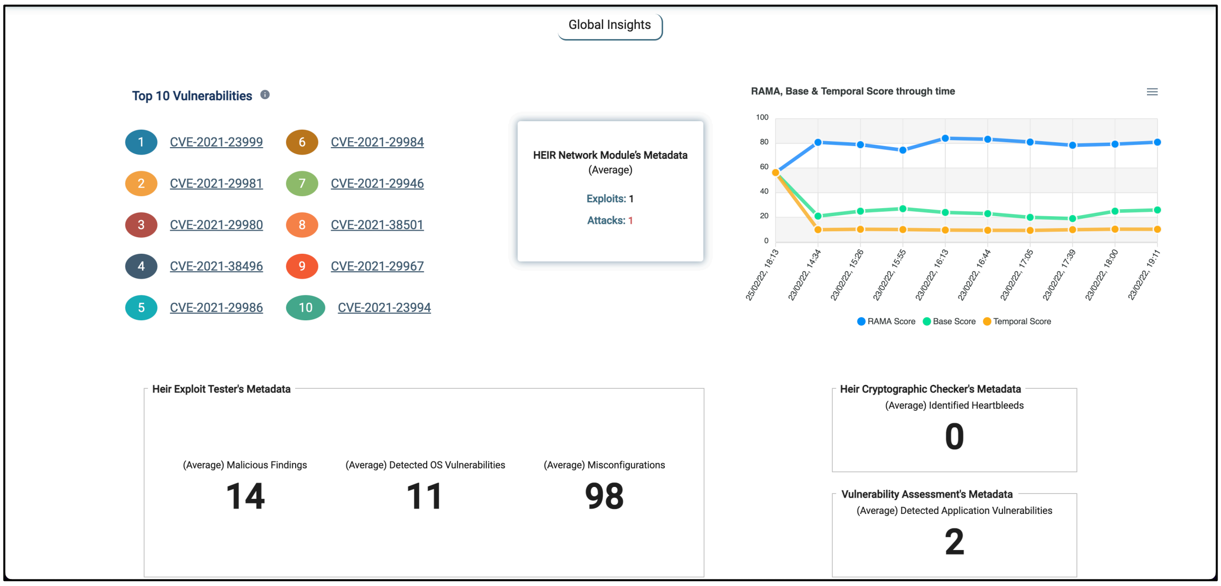
Hospital Security Status: Low

Figure 4. Connected Anonymized Hospitals

Moreover, the 'Global Insights' section contains the initial statistical information derived by the HEIR Global Calculator and a multi-series line chart that demonstrates the evolution of the RAMA scores through time. Statistical data refer to the top global-identified vulnerabilities and the analysis of the output of the HEIR Client's modules. In this version, as part of the recommendations of the platform, the end user can see the top 10 vulnerabilities either by severity or by count detected and then the user can navigate to MITRE's CVE knowledgebase[2] by clicking on any of these.

[2] https://cve.mitre.org/

HEIR client's metadata are displayed in groups, by highlighted numbers and different graphical representations, so as to enhance the end-user's situational awareness. *Figure 5* below depicts how the information is displayed.



Global Insights

Top 10 Vulnerabilities

1 CVE-2021-23999
2 CVE-2021-29981
3 CVE-2021-29980
4 CVE-2021-38496
5 CVE-2021-29986
6 CVE-2021-29984
7 CVE-2021-29946
8 CVE-2021-38501
9 CVE-2021-29967
10 CVE-2021-23994

HEIR Network Module's Metadata
(Average)

Exploits: 1
Attacks: 1

Heir Exploit Tester's Metadata

(Average) Malicious Findings
14

(Average) Detected OS Vulnerabilities
11

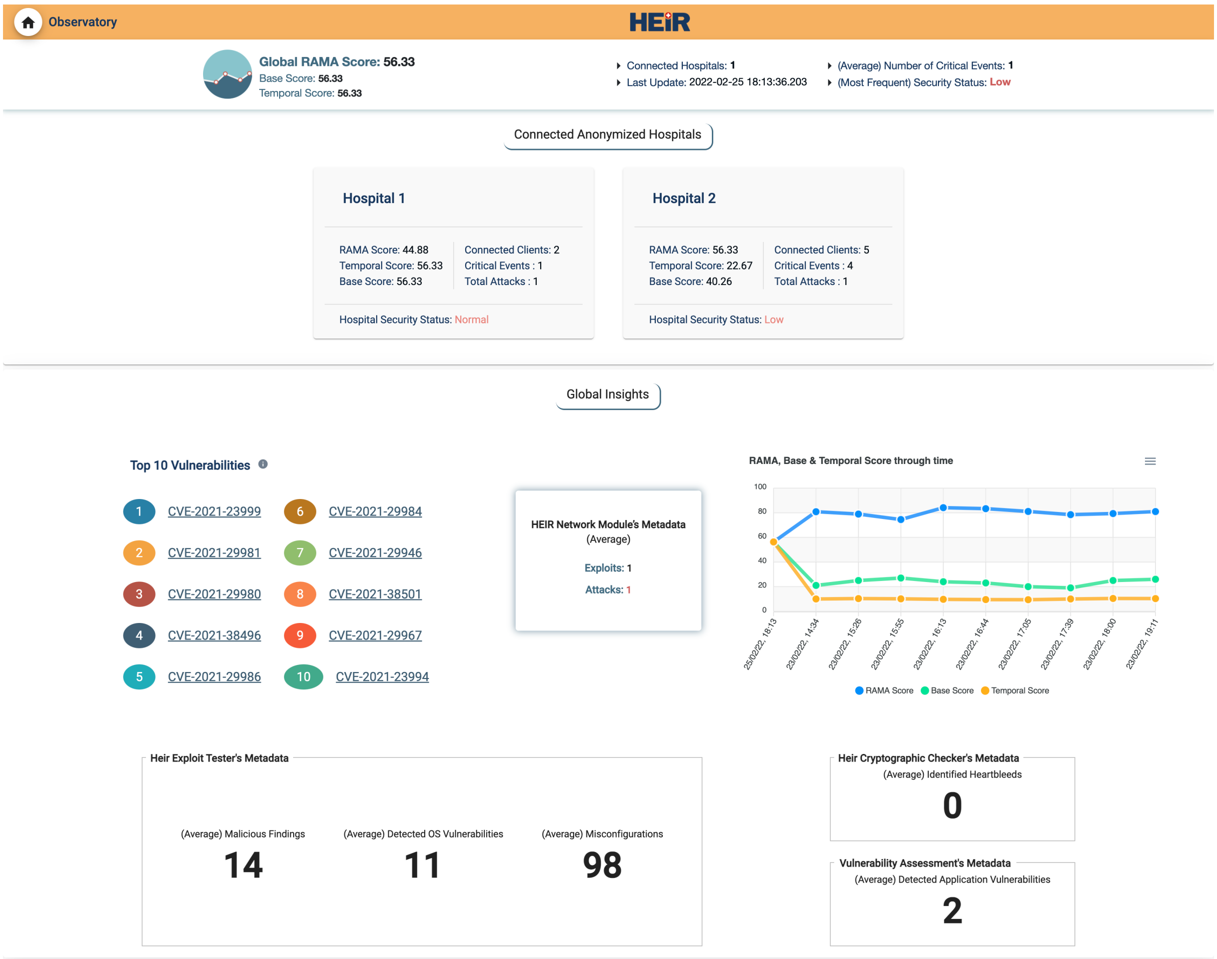
(Average) Misconfigurations
98

Heir Cryptographic Checker's Metadata
(Average) Identified Heartbleeds
0

Vulnerability Assessment's Metadata
(Average) Detected Application Vulnerabilities
2

Figure 5. Global Insights

The 2nd layer visualizations provide an overview of the cybersecurity status within the HEIR ecosystem. Authorised researchers and relevant audience will have the opportunity to explore knowledge gathered from HEIR Clients and identify common and critical vulnerabilities and exposures that threaten healthcare infrastructures.



Observatory

HEiR

Global RAMA Score: 56.33
Base Score: 56.33
Temporal Score: 56.33

- Connected Hospitals: 1
- Last Update: 2022-02-25 18:13:36.203
- (Average) Number of Critical Events: 1
- (Most Frequent) Security Status: Low

Connected Anonymized Hospitals

Hospital 1

RAMA Score: 44.88
Temporal Score: 56.33
Base Score: 56.33
Connected Clients: 2
Critical Events : 1
Total Attacks : 1

Hospital Security Status: Normal

Hospital 2

RAMA Score: 56.33
Temporal Score: 22.67
Base Score: 40.26
Connected Clients: 5
Critical Events : 4
Total Attacks : 1

Hospital Security Status: Low

Global Insights

Top 10 Vulnerabilities

1 CVE-2021-23999
2 CVE-2021-29981
3 CVE-2021-29980
4 CVE-2021-38496
5 CVE-2021-29986
6 CVE-2021-29984
7 CVE-2021-29946
8 CVE-2021-38501
9 CVE-2021-29967
10 CVE-2021-23994

HEIR Network Module's Metadata
(Average)
Exploits: 1
Attacks: 1

RAMA, Base & Temporal Score through time

Heir Exploit Tester's Metadata

(Average) Malicious Findings	(Average) Detected OS Vulnerabilities	(Average) Misconfigurations
14	11	98

Heir Cryptographic Checker's Metadata
(Average) Identified Heartbleeds
0

Vulnerability Assessment's Metadata
(Average) Detected Application Vulnerabilities
2

Figure 6. Observatory full page

2.5 *Legal Aspects concerning the health environment cybersecurity*

In healthcare organisations, health data security and privacy are two of the most crucial concerns. In particular, the healthcare systems may involve access to anonymised data provided by participants to advance research. Medical datasets are intended to be kept confidential. This means that control should be provided over the ability to share health information without compromising patients' privacy. Data security is a central aspect of the HEIR project. For this reason, compliance with legislation such as the General Data Protection Regulation (GDPR), ePrivacy Directive and other laws concerning data protection and privacy of any specific partner's home country will be ensured concerning personal data and protection of privacy in the electronic communication and networks.

The HEIR platform will rely on different security and privacy technologies and techniques. One part of this is Privacy-Enhancing Technologies (PET), a category of technologies (i.e., Software, Hardware,) designed at protecting the privacy of users by reducing personal data, usually without losing the functionalities of the systems to which the Privacy Enhancing Technologies are applied. These technologies are a very board category and measures covering anything from a broadly speaking sensor to advanced cryptographic techniques [15]. However, Privacy Enhancing Technologies includes techniques that allow for personal data to be tagged with instructions about how this data can and should be used, for example, for anonymising networks, prevent tracking online and secure messaging [16].

From a legislative perspective cybersecurity is governed by the Directive 2016/1148 of the European Parliament and of the Council on measures to ensure an integrated high level of security of network and information systems throughout the Union (NIS Directive) [6]. To support the legislation, the NIS Cooperation Group (national ministries and cybersecurity agencies) work towards the EU-wide consistent transposition of the Directive and guides the EU CSIRT network. The draft NIS 2 Directive [7] further develops the cybersecurity requirements and explicitly includes healthcare as a group of services subject to the legislation as well as services of Electronic Identification and Trust Services for Electronic Transactions (eIDAS). Another novelty would comprise the setup of an EU Cyber Crisis Liaison Network (EU-CyCLONe) to facilitate cross-border communication about security incidents.

The General Data Protection Regulation (GDPR) is the legislative framework for the processing of data about people in the EU. It aims to protect the rights of citizens but also to promote free data flow across borders of the EU Member States (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2]). The GDPR principles (Article 5) include lawfulness (e.g. consent; see Articles 6 to 9), data quality, proportionality, data security, fairness, accountability, and transparency (see e.g. Articles 12 to 14). In contrast to the NIS Directive(s) which need(s) to be transposed into national law, the GDPR is directly applicable in the EU Member States. Other pieces of legislation include the Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [4] and the ePrivacy Directive [5] (to be repealed by a Regulation). In order to be able to trust information received by individuals and organisations using signatures, seals, time stamps, documents, delivery, certificates, etc., the eIDAS Regulation sets the EU level of electronic identification, trust and authentication services (Regulation (EU) 2014/910 [3]).

The application of the GDPR is only required the data are "personal", that is, the information concerns an "identified or identifiable" natural person [2]. However, this is not a trivial assessment and there are techniques to achieve anonymisation and pseudonymisation (see e.g. [13]). It is to be highlighted that pseudonymous data are still considered "personal". For the concept of personal data [21], it is central to consider the latest state of the art in technology and business practice because the GDPR defines data as non-anonymous if any means are "reasonably likely to be used" to identify the individuals ([2] Recital 26). But even if data are considered anonymous, the safeguards for achieving and maintaining the state of anonymity is precisely what can be considered as a legal requirement to be able to rely on the inapplicability of the GDPR. Anyway, the stakeholders (developer, controller, processor, patient, researcher) need to be considered. In order to comply with the legal obligations, the state of the art needs to be considered, for example, according to Article 25(1) GDPR. European and international privacy standards specify the state of the art (see analysis in [18]) such as:

- ISO/IEC 27701 [8], ISO 27799 [9] on security management
- CEN Standard on the implementation of the International Patient Summary [10]
- prEN 17529 (public consultation draft) [11] on data protection by design
- ISO/IEC 29134 [12] on privacy impact assessment
- ISO 25237, ISO/IEC 20889 [13] on pseudonymisation and de-identification techniques
- ISO/IEC 62304 [14] on secure health software development lifecycle.

Specifically for healthcare, Member State law is still applicable. Article 9(4) GDPR stipulates that "Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health." Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 (Patient's Rights Directive) regulates the application of patients' rights in cross-border healthcare and is the main political and strategic Governance Body for eHealth in Europe, connecting the National Authorities responsible for National Contact Points for eHealth (NCPeH) [1]. It sets up the eHealth Network (eHN) under Article 14 to develop interoperability for cross-border eHealth services. The Patient's Rights Directive is supported by the Agreement between EU Member States governing the data exchange among National eHealth Contact Points (NCPeH) [13]. An analysis of data protection in healthcare can be found in [17]. In order to address security in HEIR, the legal aspects mentioned above will be taken into account to prevent unauthorised access, modification, replication, or destruction of data. This is true for data transport but also storage in online repositories, the sensitivity level of the data in question, the on-premises data use (for research and development) and communication (e.g. email) and the software used.

3. The complete version of HEIR's 2nd layer of services package for the PAGNI Use Case

The most advanced use case in HEIR is the PAGNI use case. Hence, this deliverable is focusing on this specific use case, where we have been able to draw experience from the deployment.

PAGNI's PANACEA is a patient management information system (bed management system), providing the health professional with the right information, when needed, in a way that can easily monitor a hospitalisation incident, ensuring a "paperless" environment. At the same time, it enables the treating physician to have a complete picture of his/her patient, as he/she can gather information from all the hospitals of Crete. In more detail, PANACEA is a complete hospital electronic file, accessible from any computer system (PC, tablet, smartphone, etc.)

PANACEA servers are located at the hospital's server room running. For the 1st complete version of services, the 2nd layer of services package works as follows:

Step 1. The HEIR Client in PAGNI generates events and RAMA Score; the events are anonymised and sent to the HEIR Database,
Step 2. RAMA Score is sent to the HEIR Database,
Step 3. The Global benchmark is calculated.
Step 4. The 2nd layer visualisations fetch data from the HEIR Database and present them using the UI.
Step 5. The Anonymous users can access statistical data and view aggregated, global information about RAMA Scores and cybersecurity events.

The next use-case deployment focuses on HYGEIA infrastructure considering its technical specificities. The above-described steps will be replicated for HYGEIA providing the interested parties with an overview of the cybersecurity status within the HEIR ecosystem. The relevant audience will have the opportunity to explore knowledge gathered from HEIR Clients and identify common and critical vulnerabilities and exposures that threaten specific healthcare infrastructures.

4. Conclusion

This document explained the design and definition of the HEIR 2nd layer of services package: the 1st complete version. The current status of the services package has been firstly conceptualised following inputs from deliverables D3.2, D4.1 and D5.2. Then, the technical advancements made between M12 and M18 were illustrated within the document complemented by the showcase of how the current version impacts the use-cases. Lastly, Appendix 6 presents the samples output concerning the HEIR Global Benchmarks.

The next steps include continuous updating of the HEIR 2nd layer of services considering the evaluators input that will be received during the evaluation period, as well as the ongoing work within the WP4 and connecting WPs such as 2, 3 and 5. Further internal updates will be deployed across the modules based on the use-cases particularities, to achieve a homogenous 2nd layer of services.

In parallel with the further updates of the components, an important focus will be on adjusting the HEIR 2nd layer of services package for the next use-cases, mainly HYGEIA and CUH. The technologies providers will continue to work together with the use-cases representatives to deploy and adapt the 1st complete version.

The next phase of reporting the WP4 activities will be described by “D4.3: The HEIR 2nd layer of services package, final version, by M26, which will serve as an instrument to present the final configuration for services like the HEIR Global Benchmarks, the HEIR Observatory and the 2nd level of visualisation. Also, a newer version of the legal framework concerning the cybersecurity for the health environment will be illustrated considering the technical implementations for the use-cases as well as the latest regulations and recommendations.

5. References

[1] Directive 2011/24/EU of The European Parliament and of The Council of 9 March 2011 on the application of patients' rights in cross-border healthcare.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[3] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG.

[4] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). COM/2017/010 final - 2017/03 (COD), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010.

[5] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058.

[6] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148.

[7] Shaping Europe's digital future. 16 December 2020. Proposal for directive on measures for high common level of cybersecurity across the Union https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union.

[8] ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines, https://www.iso.org/standard/71670.html.

[9] ISO 27799:2016 Health informatics — Information security management in health using ISO/IEC 27002, https://www.iso.org/standard/62777.html.

[10] CEN standard TS 17288 'The International Patient Summary: Guideline for European Implementation', https://www.cen.eu/news/brief-news/Pages/NEWS-2021-009.aspx.

[11] EN 17529 Data protection and privacy by design and by default, https://standardsdevelopment.bsigroup.com/projects/2020-00802#/section.

[12] ISO/IEC 29134:2017 Information technology — Security techniques — Guidelines for privacy impact assessment, https://www.iso.org/standard/62289.html.

[13] ISO/IEC 20889:2018 Privacy enhancing data de-identification terminology and classification of techniques https://www.iso.org/standard/69373.html.

[14] IEC 62304:2006 Medical device software — Software life cycle processes, https://www.iso.org/standard/38421.html.

[15] The Royal Society, protecting privacy in practice: The current use, development, and limits of Privacy Enhancing Technologies in data analysis. ISBN 978-1-78252-390-1, https://royalsociety.org/topics-policy/projects/privacy-enhancing-technologies/.

[16] ENISA PETs Controls Matrix report, 12/2016, https://www.enisa.europa.eu/publications/pets-controls-matrix/pets-controls-matrix-a-systematic-approach-for-assessing-online-and-mobile-privacy-tools.

[17] Conley, E.C. and Pocs, M., "GDPR Compliance Challenges for Interoperable Health Information Exchanges (HIEs) and Trustworthy Research Environments (TREs)", European Journal for Biomedical Informatics, Volume 14 (2018), Issue 3, pages 48-61. Available online at https://www.ejbi.org/abstract/gdpr-compliance-challenges-for-interoperable-health-information-exchanges-hies-and-trustworthy-research-environments-tre-4619.html.

[18] Quemard et al., Report of the European Cybersecurity Agency ENISA: Guidance and gaps analysis for European standardisation, 2019. Available online at https://www.enisa.europa.eu/publications/guidance-and-gaps-analysis-for-european-standardisation.

[19] Guidelines 05/2020 on consent under Regulation 2016/679, point 1(2), also 2(9), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

[20] Working Party Opinion 1/2010 on the concepts of "controller" and "processor, 2010, page 13, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf.

[21] WP29. Opinion 4/2007 on the concept of personal data, 2007. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf, page 5.

6. Appendix A. 1st complete version of the HEIR Global Benchmarks

```
{
  "numberOfExploits": 17,
  "temporalScore": 9.6,
  "numberOfCriticalEvents": 137,
  "created": "2022-02-26 17:23:00.226",
  "number_of_hospitals": 4,
  "numberOfAttacks": 6,
  "connected_hospitals": [
    "1",
    "2",
    "4",
    "5"
  ],
  "baseScore": 13.1034,
  "cyberSecurityStatus": "Low",
  "noOfMisconfigurations": 70,
  "noOfAppVulnerabilities": 438,
  "numberOfBenignFindings": 59,
  "numberOfMaliciousFindings": 16,
  "ramaScore": 81.83,
  "numberOfIdentifiedHeartbleeds": 0,
  "noOfOSVulnerabilities": 438,
  "id": 1,
  "top10Vulnerabilities": {
    "CVE-2022-21983": 100,
    "CVE-2021-29981": 67,
    "CVE-2020-21983": 99,
    "CVE-2021-29980": 67,
    "CVE-2021-38496": 67,
    "CVE-2021-29983": 100,
    "CVE-2021-293983": 100,
    "CVE-2021-23992": 100,
    "CVE-2023-21983": 100,
    "CVE-2021-21983": 100
  },
  "updated": "2022-02-26 19:36:28.042"
}
```