



D4.3

The HEIR 2nd layer of services package: final version

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

Deliverable type	Demonstrator
Deliverable reference no.	D4.3
Workpackage	WP4
Due date	28/02/2023 [M30]
Actual submission date	28/02/2023

Deliverable lead	AEGIS
Editors	Andreas Alexopoulos, Miltiadis Kokkonidis
Contributors	Chronis Ballas (AEGIS), Aris Sotiropoulos (AEGIS), Michalis Smyrlis (Sphynx), Sofia Spanoudaki (Sphynx), Dimitris Tsolovos (STELAR), George Tsakirakis (ITML)
Reviewers	Bogdan Prelipcean (Bitdefender), Dimitris Tsolovos (STELAR)
Dissemination level	PU
Revision	1.0
Keywords	#servicespackage #heirarchitecture #heirframework #cybersecurity

Abstract

Deliverable 4.3 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 M30 and involved the partners' personnel active within WP4 and the related WPs such as WP2, WP3 and WP5. This deliverable supersedes D4.2 which reported on the work between M13 and M18 producing the first complete version of the HEIR 2nd layer of services package.

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, specifically its final version prepared as one of the key outcomes of the HEIR project. It 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 final version comprises the following main services:

- I. The HEIR Global Benchmarks: a mechanism for computing the aggregate security status of a group of clinical sites,
- II. The HEIR Observatory: a centralised security monitoring data hub accumulating data points from HEIR agents at different clinical sites and subjecting them to cybersecurity-focused analyses,
- III. The 2nd level of visualisation: visualisations offering a bird's eye view over clinical sites monitored by the HEIR platform and viewing individual clinical sites as parts of a larger whole.
- IV. The Global Policy Observatory: a tool for sharing and reviewing security policies, and
- V. The legal aspects involving the cybersecurity for the health environment.

The current, final, version builds on the solid foundation of the 1st complete version, providing qualitative enhancements, as well as enhanced and additional functionality. Moreover, it has been deployed across all four HEIR pilots adjusting to their specific conditions and requirements.

Data is collected from the HEIR Aggregators deployed within all pilots (PAGNI, HYGEIA, NSE, CROYDON). The HEIR Global Risk Assessment for Medical Applications (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 visualisations (as well as made available to the 1st layer visualisations for comparing the local with the global security status).

The Global Policy Observatory, a new feature added in the current, final, version of the 2nd layer of services is being validated in the context of the NSE/NOKLUS pilot adding a further dimension to the HEIR value proposition.

Table of Contents

EXECUTIVE SUMMARY	2
1. INTRODUCTION.....	5
1.1 SCOPE AND OBJECTIVES	5
1.2 RELATION TO OTHER TASKS AND WORK PACKAGES	5
1.3 STRUCTURE OF THE DOCUMENT	5
2. THE HEIR 2ND LAYER OF SERVICES.....	7
2.1 OVERVIEW	7
2.2 HEIR GLOBAL BENCHMARKS.....	7
2.2.1 <i>Global RAMA score definition and metadata</i>	7
2.2.2 <i>HEIR Global Benchmarks deployment information</i>	8
2.3 THE HEIR OBSERVATORY	9
2.3.1 <i>The functional description</i>	9
2.3.2 <i>The Component Design</i>	9
2.3.3 <i>Deployment Information</i>	10
2.4 THE 2 ND LAYER OF VISUALISATION	10
2.4.1 <i>The functional description</i>	10
2.4.2 <i>Component Design</i>	11
2.5 GLOBAL POLICY OBSERVATORY.....	14
2.6 LEGAL ASPECTS CONCERNING THE HEALTH ENVIRONMENT CYBERSECURITY	15
3. HEIR 2ND LAYER OF SERVICES PACKAGE AND HEIR USE CASES.....	18
4. CONCLUSIONS	20
REFERENCES.....	21
APPENDIX A. FINAL VERSION OF THE HEIR GLOBAL BENCHMARKS	23

List of Figures

FIGURE 1. HEIR GLOBAL BENCHMARK (GLOBAL RAMA SCORE CALCULATOR) DEPLOYMENT DIAGRAM	8
FIGURE 2. HEIR OBSERVATORY ARCHITECTURE	9
FIGURE 3 OBSERVATORY'S LOGIN PAGE.....	11
FIGURE 4 OBSERVATORY'S HEADER INFORMATION & GLOBAL INSIGHTS.....	12
FIGURE 5 GENERIC STATISTICS.....	13
FIGURE 6 CONNECTED HOSPITALS	13
FIGURE 7 ACTIVE POLICIES PAGE	15
FIGURE 8 GLOBAL RAMA SCORE CALCULATION RESULT.....	24
FIGURE 9 GLOBAL RAMA SCORE CALCULATOR IN ACTION	24

List of Abbreviations

ACIMS	Access Control and Identity Management System
AVT	Advanced Visualisation Toolkit
CPU	Central Processing Unit
CSIRT	Computer Security Incident Response Team
eIDAS	Electronic Identification and Trust Services for Electronic Transactions
FVT	Forensics Visualisation Toolkit
GDPR	General Data Protection Regulation
IT	Information Technology
ML	Machine Learning
MVP	Minimum Viable Product
NCPeH	National Contact Points for eHealth
NIS	Network and Information Systems
OPA	Open Policy Agent
PAF	Privacy Aware Framework
PGHD	Patient-Generated Health Data
PHI	Personal/Protected Health Information
RAMA	Risk Assessment for Medical Applications
SIEM	Security Information and Event Management
VM	Virtual Machine

1. Introduction

1.1 Scope and objectives

HEIR 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. Whereas the 1st layer of HEIR services package focuses on individual hospitals and their Information Technology (IT) infrastructures, giving users the ability to focus on anything from the entire infrastructure to a detailed, low-level view of a single device, the 2nd layer of HEIR services package aims to provide high-level security oversight and insights obtainable from aggregated analytics carried out on the HEIR Observatory (as per the HEIR high-level architecture described in D1.1). The present report presents the final version of the HEIR 2nd layer of services package as deployed on the HEIR cloud and connected with all four HEIR hospitals.

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 and continued by D4.2. Whereas D4.1 presented early work that resulted into an MVP at the end of the first year of the project (M12), and D4.2 (M18) presented a first, intermediate yet complete version, the present deliverable, D4.3 (M30), presents the final version of the HEIR 2nd layer of services. Viewed in sequence, the three deliverables document the evolution of the HEIR 2nd layer of services throughout the project presenting focused snapshots at different important milestones. D4.3 supersedes D4.2 as the most up-to-date description of the HEIR 2nd layer of services, reflecting both earlier work documented previously and refinements, improvements and functional enhancements carried out between M19 and M30. The document presents the direct outcomes of WP4 activities (T4.1 to T4.4). These were closely intertwined with WP2, WP3 and WP5 activities. As a result, the deliverable is closely related to

- “D2.3 The HEIR facilitators package: Final complete version”, the deliverable presenting the final version of the HEIR facilitators and the associated WP2 work.
- “D3.3 The HEIR 1st layer of services package: final version”, a sister deliverable, presenting the 1st level services package offering both the hospital-specific services of HEIR and an opportunity to compare a specific hospital’s security status with the overall status of all HEIR hospitals as analysed and evaluated by the HEIR 2nd layer services package.
- “D5.4 HEIR integrated framework final version” as HEIR 2nd layer of services package will be part of the overall HEIR framework.

1.3 Structure of the document

The remainder of the document is structured as follows:

Section 2 presents the HEIR 2nd layer of services package including both back-end mechanisms and the front-end user interface and visualisations, as well as an overview of the legal aspects and relevant landscape relevant to the provision of HEIR services.

Section 3 outlines the status of the demonstration of the HEIR 2nd layer of services package across the four HEIR use cases, noting the progress made since D4.2

Section 4 concludes the presentation of the final version of the HEIR 2nd layer of services packages, linking progress made to the project’s goals and future developments.

Appendix A. Final version of the HEIR Global Benchmarks showcases an example of the results obtained by 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 Global Policy Observatory
- the HEIR legal.

2.2 HEIR Global Benchmarks

HEIR introduces the concept of the Local RAMA (Risk Assessment for Medical Applications) score as a simple yet effective means of conveying to IT personnel, security experts and other parties, the overall security status of an individual clinical site. The Global RAMA score does the same for a group of such clinical sites. As described in the previous iterations of this deliverable (D4.1 and D4.2), the Global RAMA score acts as a benchmark against which the local RAMA scores will be compared.

2.2.1 Global RAMA score definition and metadata

The definition of the HEIR Global benchmarks (HEIR Global RAMA Score) provided in D4.2 is a weighted sum of the three Local RAMA aggregated scores as depicted in the equation below.

$$Global\ RAMA\ Score = \sum_{i=1}^N LRA_i$$

where N is the number of the available Local RAMA aggregated scores and LRA_i is the Local RAMA Aggregated score for clinical site i as provided through its local HEIR Aggregator.

This definition is retained in the final version of the HEIR 2nd layer of services package. However, during the final year of the project, advancements were made towards the finalisation of the Local RAMA score and the corresponding calculator. As a consequence, the Global RAMA calculator was updated to reflect the changes that occurred in the Local RAMA aggregated score (see “D3.3 – The HEIR 1st layer of services package: final version”).

As described in D4.2, starting with the 1st complete version of the HEIR 2nd layer of services, the Global RAMA Score also comes with metadata provided by the HEIR Aggregator, such as, the top ten (10) vulnerabilities in all the involved healthcare facilities. In the current, and final version, the Global RAMA score’s metadata were enriched with the addition of the top 10, most severe and most frequent vulnerabilities, allowing a hospital to also identify if the, locally identified vulnerabilities, were also identified in other hospitals around Europe.

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

2.2.2 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 constitute the main part of HEIR’s Global Benchmark and are made available to the interested parties through the HEIR Observatory module.

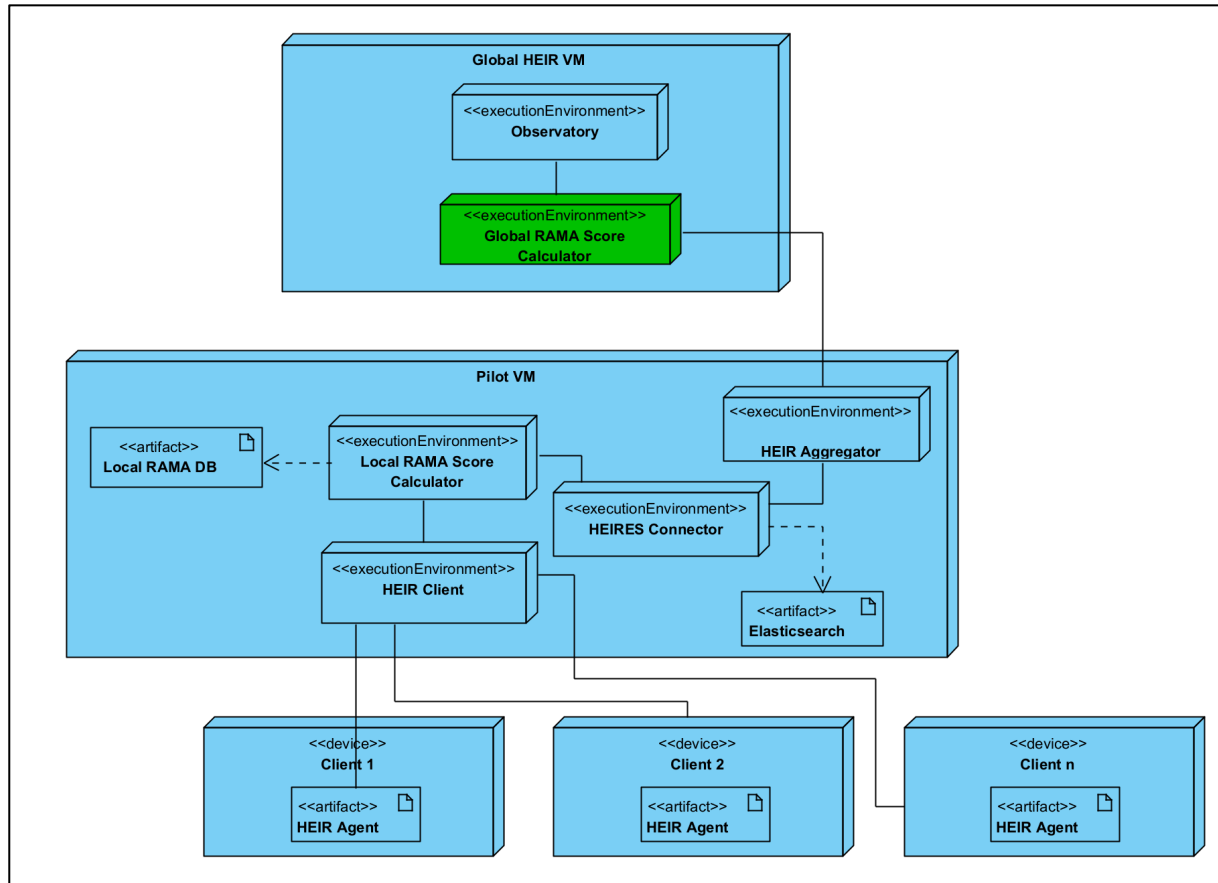


Figure 1: HEIR Global Benchmark (Global RAMA Score calculator) deployment diagram

As depicted in Figure 1 the Global RAMA Score calculator is deployed inside the Global HEIR VM and communicates with the HEIR Aggregator. Communication takes place via a Kafka message broker, over a TLS-secured communication channel. Prior to the data transfer from the HEIR Aggregator to the Global RAMA Score calculator, the former anonymises data to be sent (mostly metadata fed by the Local RAMA Score calculator) that might expose personal information from a specific hospital.

The Global RAMA score and the metadata, are being visualised through the HEIR Observatory GUI (see Section 2.4).

A sample output of the Global Rama Score calculator is available in Appendix A. Final version of the HEIR Global Benchmarks.

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.

In the final version of the Observatory, an additional functionality has been added that allows authorised users to view the active policies of the participating hospitals. This new functionality is presented separately in Section 2.5.

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 final and updated aggregated RAMA score and relevant metadata as analysed in D3.3, without any hospital identifying indicator. This de-association of events sent to the repository will be applied to all clients with the aim of preserving anonymity and preclude the possibility of associating any aggregated information and statistical information on cybersecurity events displayed in the observatory with any particular hospital.

In order to support the new added functionality of active policies access that mentioned above, a pipeline that transfers these policies that exists in PAF (Privacy Aware Framework), from hospitals to the HEIR Observatory, has been utilised. Moreover, an identity manager has been integrated, so to ensure the secure role-based access to these policies.

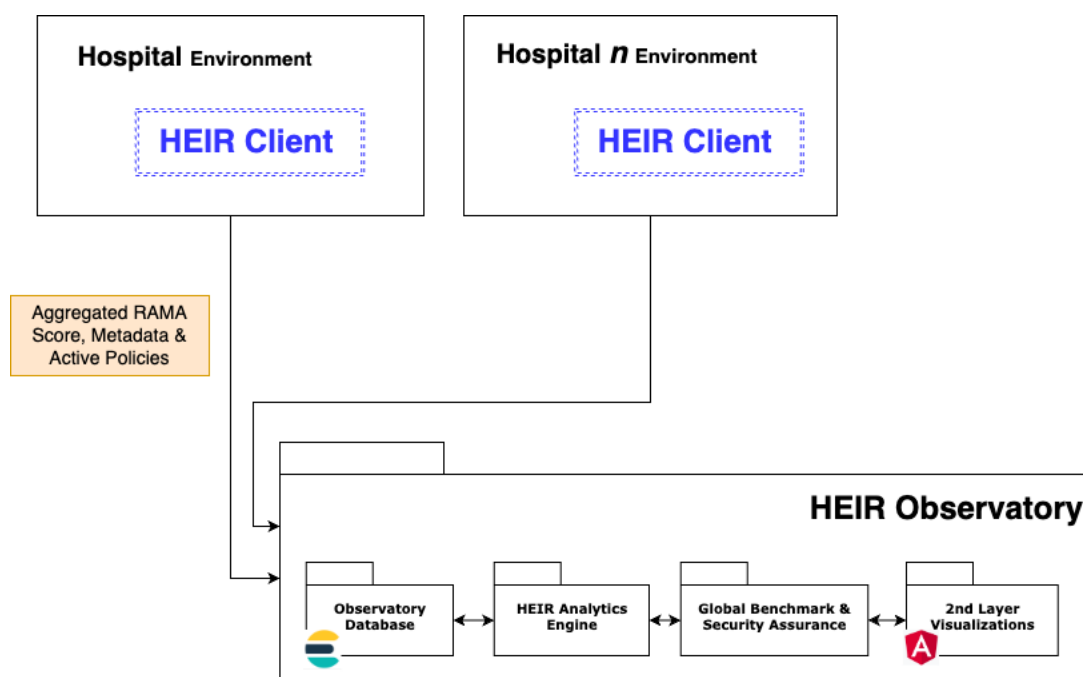


Figure 2: HEIR Observatory architecture

The technology used for the Observatory's HEIR database is Elastic Search¹ 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. Thus, it is a key-role tool that HEIR Analytics Engine takes advantage of.

The HEIR Analytics Engine extracts the outcome of the analysis on the available data to the 2nd layer of Visualizations, which is a web application as it is described in the next section. HEIR Analytics Engine serves as the back-end of HEIR's Observatory and handles all the available data, derived in Observatory. It is also tasked with providing a set of recommendations to the end-users.

2.3.3 Deployment Information

For the deployment of the HEIR Observatory, a hardware infrastructure has been configured to accommodate the participating HEIR Observatory and supporting infrastructure modules. The hardware infrastructure was selected after sizing the resource requirements (CPU, memory, storage etc.) of the Observatory.

It was determined that one dedicated VM would be allocated for the execution of the use cases, with the following characteristics: 8 cores, 16GB RAM, 155GB HDD, running Ubuntu 20.04.3 LTS (Focal Fossa)

This VM hosts all HEIR Observatory modules and supporting infrastructure modules, namely the Global RAMA Score calculator, the Observatory Database, the 2nd Layer of Visualisations and a tailor-made back-end component that provides analytics and role-based access control capabilities.

Additionally, the Observatory installation includes various tools that enable storing, visualising, and communicating data among the underlying modules as well as to and from the pilots, namely Kafka², Elasticsearch³, Kibana⁴.

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. For the final version, these refer to the Global RAMA Score (described in Section 2.2), relevant metadata, statistics and recommendations that are produced (HEIR Analytics Engine) based on the local RAMA, but also to active policies that were extracted from the Privacy Aware Framework as mentioned in Section 2.3.2. Part of this information is transferred to Observatory through the local HEIR Aggregators that are located at hospital's premisses. The corresponding results are available through the visualisation dashboard.

Users accessing the HEIR Observatory have read-only access to data collected from the HEIR Clients. In order to support the addition of functionality that offers access to non-public

¹ <https://www.elastic.co/elasticsearch/>

² <https://kafka.apache.org/>

³ <https://www.elastic.co/>

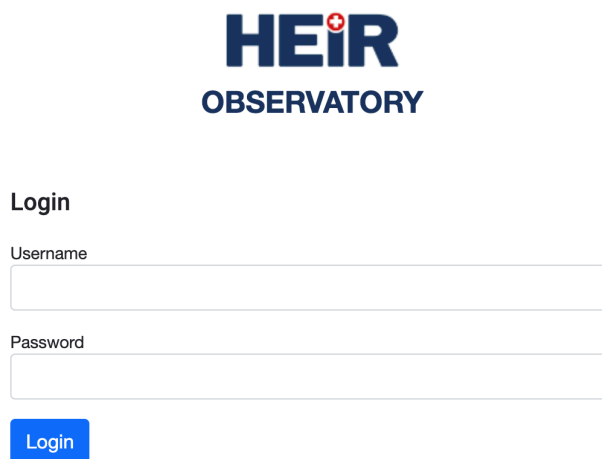
⁴ <https://www.elastic.co/kibana/>

information, authentication mechanisms and a login page has been incorporated into this new and final version.

As of the 1st complete version (D4.2) visualisations widgets are included in order to displaying the final version of RAMA's metadata, such as the 'Top 10 Vulnerabilities by Frequency' and the 'SIEM metadata'. Additional widgets have been provided in the final version to support the additional information available in this version (as mentioned in Section 2.2) such as the top 10, most severe and most frequent vulnerabilities. Functionality is also provided to support historical data requests with regards to the RAMA's recorded scores. HEIR 2nd layer visualisation widgets have been designed to be highly informative and visually appealing, providing users with a clear and concise overview of the relevant data.

2.4.2 Component Design

Users logging to Observatory will be granted different access permissions based on their role. Upon successful login, a redirection to the main visualisation dashboard takes place.



The image shows the login page for HEIR OBSERVATORY. At the top center is the logo, which consists of the word "HEIR" in a bold, blue, sans-serif font with a small red cross above the letter "I", and the word "OBSERVATORY" in a smaller, blue, sans-serif font directly below it. Below the logo, the word "Login" is written in a bold, black, sans-serif font. Underneath "Login" are two input fields: the first is labeled "Username" and the second is labeled "Password". Both labels are in a small, black, sans-serif font. Below the password field is a blue rectangular button with the word "Login" written in white, sans-serif font.

Figure 3: Observatory's Login page

The Observatory's home page has been designed to be intuitive and informative, providing users with easy access to key information and insights. By landing at the main dashboard, a summary of important information is presented at the top of the page, containing the number of connected hospitals, the average number of critical events, and the most frequent security reported levels. This summary provides users with a clear and concise overview of the HEIR's ecosystem activity. Moreover, navigation options and user-logged information are available at the top menu bar.

Below the header information, the Global Insights section is presented, which includes the main results of HEIR's Observatory. A line chart showing the evolution of Global RAMA Scores over time along with an integrated historical request functionality are placed at the top layer of this section. The scores consist of the main, the base and the temporal one which are explained in detail in D3.3. Based on the start and end time that a user selects, an average calculation of

the scores takes place, so to achieve a comprehensive and meaningful representation inside the corresponding time window. Zooming, panning and download chart's snapshot are some of the available control actions for the end-user. This is accompanied by a display of the Global RAMA, base and temporal scores, providing users with a detailed overview of the current HEIR's ecosystem state. These features have been designed to be visually appealing and informative, with clear and concise labelling and high-quality graphics.

Inside the second layer, users will find two lists providing detailed information regarding the ongoing reported top 10 vulnerabilities by severity and by frequency across all hospitals. This feature has been designed to provide users with a comprehensive overview of the security landscape at participating hospitals, allowing them to quickly identify areas for improvement and take appropriate action (Figure 4). Security experts can gain detailed information for the displayed vulnerabilities by clicking on the side buttons, since these navigate to global knowledge databases, like MITRE.

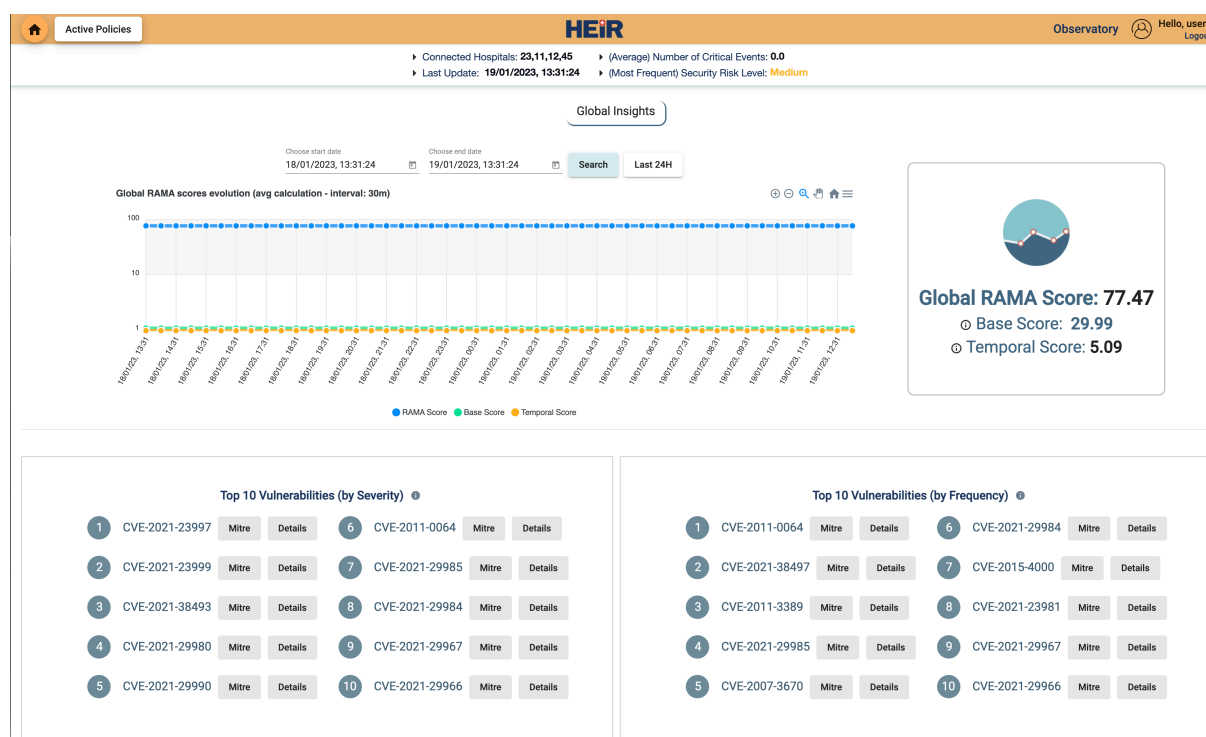


Figure 4: Observatory's Header Information & Global Insights

Moving further below, generic statistics are displayed, including information on the embedded modules of the HEIR Client in each hospital. This set of data is grouped into five categories: 'Heir Exploit Tester's Metadata', 'HEIR Network Module's Metadata', 'Heir Cryptographic Checker's Metadata', 'Vulnerability Assessment's Metadata', and 'SIEM Metadata'. The available information includes detected application and OS vulnerabilities, captured network-related events, active misconfigurations, and event analysis results, among others (Figure 5).

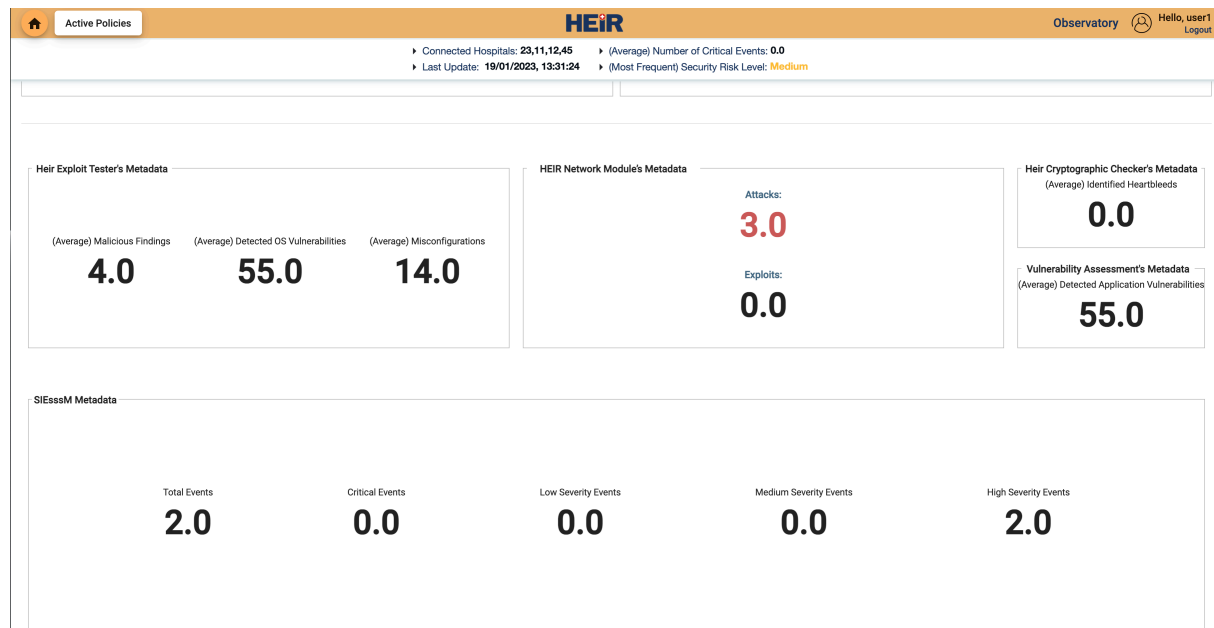


Figure 5. Generic Statistics

At the bottom of the page, users can check the list of connected hospitals in an anonymized manner, allowing them to easily monitor the Observatory's reach and impact. Additionally, a summary of useful information is displayed, providing users with quick access to key-role values (Figure 6).

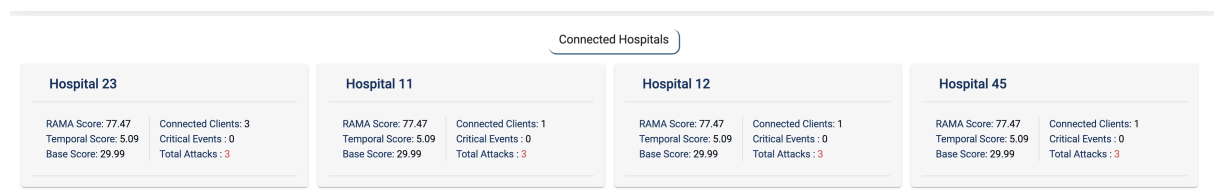


Figure 6: Connected Hospitals

As part of the final version of the HEIR's Observatory, the "Active Policies" screen that was mentioned above and will further be described in Section 2.5, is accessible through the 2nd layer of visualizations.

Overall, the visualizations used in Observatory have been designed to be simple, user-friendly but also informative and intuitive, so to provide valuable knowledge that could yield to an enhanced decision-making process, while to satisfy the needs of the different user-roles. The application has been developed in an Angular Framework, supported by Node.js middleware. The architectural design and the services' workflows were developed on top of AVT's (Advanced Visualization Toolkit) built-in skeleton. AVT is a tool being developed by AEGIS.

2.5 *Global Policy Observatory*

The Global Policy Observatory refers to the newly added feature in HEIR's Observatory, which is about the capability of an authorised policy expert, such as regional policy analysts, makers, advisors, or others with similar data clearance, to observe the enabled policies across the connected hospitals of HEIR ecosystem. By providing such information to the above-mentioned target group, the Policy Observatory aims to end up with significant observations that could lead to valuable recommendations and knowledge sharing between HEIR participated entities.

The full set of policies are located and handled by the Privacy Aware Framework in the local layers of the hospitals. The derived, in HEIR Observatory, policies do not contain any identifiers about their source (hospitals) or other relevant PHI (Personal/Protected Health Information) and are accessible only to authorized users.

The policy language used is Rego. Rego is the purpose-built declarative policy language of the Open Policy Agent (OPA). It is meant to facilitate writing policies that are easy to read. Fundamentally, Rego inspects and transforms data in structured documents, allowing OPA to make policy decisions. It was originally inspired by Datalog, a common query language with a decades-long history but extends its capabilities to support structured document models like JSON.

Rego queries, put simply, ask questions of data stored in OPA. Rego policies then evaluate whether data complies with, or violates, the expected state of a system — that is how policy decisions are returned.

Tailor-made visualisation has been developed by the 2nd layer of Visualisations (AVT), which provides the maximum detailed view to the experts, combining a user-friendly interactive widget setup (Figure 7).

Therefore, the “Active Policies” screen, serves as a hub of continuously updated policies in the HEIR interconnected environment. The goal is to facilitate the exchange of knowledge and expertise between hospitals, contribute to the overall goal of improving healthcare outcomes and enhance the transparency and accountability of the participating health actors.

Active Policies
HEIR
Observatory Hello, policyauthor [Logout](#)

Active Policies

Hospital 1

Policy 1:

```
id: "fybrik-system/fhir-read-policy/policy_nse.rego"
raw: "package dataapi.authz rule({"action": {"name": "JoinAndRedact", "joinTable": "Consent", "whereClause": " WHERE consent.provision_provision_0_period_end >= observation.issued AND consent.provision_provision_0_period_start <= observation.issued", "joinStatement": " JOIN consent ON observation.subject_reference = consent.patient_reference ", "columns": column_names), "policy": description}) { description := "Executes a JOIN on the Consent table" input.resource.metadata.tags.observation_column_names := [input.resource.metadata.columns[i].name | input.resource.metadata.columns[i].tags.FII count(column_names) > 0 ] rule({"action": {"name": "RedactColumn", "columns": column_names, "isRedact": "admin"}, "policy": description}) { description := "RedactColumns for blockchain" input.resource.metadata.tags.blockchain_column_names := [input.resource.metadata.columns[i].name | input.resource.metadata.columns[i].tags.FII count(column_names) > 0 ] }
ast:
+ package:
- path: Array[3] [{"type": "var", "value": "data"}, {"type": "string", "value": "dataapi"}, {"type": "string", "value": "authz"}]
+ rules:
- 0: Object {"head":{"name":"rule", "key":{"type":"object", "value":{"type":"string", "value":"action"}, {"type":"object", "value":{"type":"string", "value":"columns"}, {"type":"var", "value":"__lo
- 1: Object {"head":{"name":"rule", "key":{"type":"object", "value":{"type":"string", "value":"action"}, {"type":"object", "value":{"type":"string", "value":"columns"}, {"type":"var", "value":"__lo
```

Policy 2:

```
id: "bootstrap/policy-lib-default_policy.rego"
raw: "package dataapi.authz verdict[output] { count(rule) == 0 output = {"action": {"name":"Deny", "Deny": {}}, "policy": "Deny by default" } verdict(outputFormatted) { count(rule) > 0 output = rule[_] actionName := output.action.name actionWithoutName := json.remove(output.action, ["name"]) outputWithoutAction := json.remove(output, ["action"]) actionFormatted := {"name": actionName, output.action.name: actionWithoutName} outputFormatted := object.union({"action": actionFormatted, outputWithoutAction}) rule({}) { false } "
ast:
+ package: Object {"path":{"type":"var", "value":"data"}, {"type":"string", "value":"dataapi"}, {"type":"string", "value":"authz"}}
+ rules:
- 0: Object {"head":{"name":"verdict", "key":{"type":"var", "value":"output"}, "body":{"terms":{"ref": {"type":"var", "value":"eq"}, {"type":"var", "value":"__local18__"}, {"type":
- 1: Object {"head":{"name":"verdict", "key":{"type":"var", "value":"__local1__"}, "body":{"terms":{"ref": {"type":"ref", "value":{"type":"var", "value":"eq"}, {"type":"var", "value":"__local19__"}, {"ty
- 2: Object {"head":{"name":"rule", "key":{"type":"object", "value":{}}, "body":{"terms":{"type":"boolean", "value":false}, "index":0}}
```

Figure 7: Active Policies page

2.6 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 broad category and measures covering anything from a broadly speaking sensor to advanced cryptographic techniques [15]. However, Privacy Enhancing Technologies include techniques that allow for personal data to be tagged with instructions about how these 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 (Network and Information Systems (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 Computer Security Incident Response Team (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. HEIR 2nd layer of services package and HEIR Use Cases

The present deliverable, D4.3 (M30), documents an advancement over the state of affairs since its predecessor, D4.2 (M18). D4.2 focused on the PAGNI use case, which was at the highest readiness level on M18 and was the only one that provided data for the Global RAMA computation. In accordance with D6.1, each pilot was meant to focus on utilising and demonstrating specific aspects of the HEIR platform, as seen below. In terms of input to the HEIR 2nd layer of services package, the 1st complete version was limited, not so much in terms of technical development, but in terms of only having available input from the PAGNI use case. This has been documented in D4.2.

- PAGNI**
 - a) Detection of outdated software
 - b) Threat detection
 - c) HIS logs monitoring and reporting
- NSE/**
 - a) Automatic data redaction of Patient-generated health data (PGHD)
- NOKLUS**
 - b) Policy access an ad-hoc analysis platform of Patient-Generated Health Data (PGHD)
 - c) Blockchain-based data access auditing system
- HYGEIA**
 - a) SIEM Agents
 - b) FVT GUI
 - c) HEIR Client
 - d) ML-based Anomaly Detection & Threat Classification
- CUH**
 - a) RAMA Score Calculator
 - b) SIEM Agents
 - c) FVT GUI
 - d) HEIR Client
 - e) ML-based Anomaly Detection & Threat Classification

Experiences with the PAGNI use case and subsequently with the remaining use cases have helped direct the evolution of the HEIR 2nd level of services posing challenges to be addressed and providing feedback that either verified or challenged early design decisions and assumptions. As the final version of 2nd layer of services package has been deployed across all HEIR pilot sites and all teething issues have been resolved, all four pilots can now provide data to the Global Observatory.

Furthermore, the final version of the HEIR 2nd layer of services package introduced the Global Policy Observatory (Section 2.5). This, alongside the HEIR Privacy Aware Framework and the HEIR auditing mechanism, are piloted in the context of the NSE- NOKLUS pilot. While these are only demonstrated in the NSE/NOKLUS use case, our current implementation allows deployment in other clinical site IT infrastructures also.

The HEIR 2nd layer of services package works as follows:

- Step 1.** The HEIR Client in each clinical site generates events and computes a RAMA Score
- Step 2.** The relevant metadata are anonymised and sent to the HEIR Database

Step 3. The RAMA Score is sent to the HEIR Database

Step 4. The Global benchmark is calculated

Step 5. The 2nd layer visualisations fetch data from the HEIR Database and present them using the UI

Step 6. Anonymous users can access statistical data and view aggregated, global information about RAMA Scores and cybersecurity events, whereas authenticated users can view the active policies of the participating hospitals.

D6.2 outlines the final pilots execution providing a comprehensive view of developments in each pilot/use-case. D6.3 will provide the results of the evaluation of HEIR in the context of its four pilots/use-cases.

4. Conclusions

This document explained the design and definition of the HEIR 2nd layer of services package: final version. The current, final, version is an evolution of the 1st complete version of the HEIR layer of services package through technical advancements in the context of the WP4 until M30. The 2nd layer of services adds to the HEIR value proposition by the anonymous collection and further processing of security monitoring data from HEIR agents deployed on a multitude of clinical sites, visualised accordingly in the 2nd layer of visualisations, and providing an additional layer of insights, shared with the clinical sites to help facilitate an estimate of their relative status.

It is important to note that HEIR is not a one-size-fits-all framework. On the one hand, more limited deployments in a clinical site can still deliver value with respect to the real-time monitoring of its security status, providing real-time forensics support, and informing the aggregate security status of the HEIR 2nd layer of services. On the other hand, the full-fledged deployments of the HEIR tools can offer advanced services and high levels of automation.

The deployments in the four pilots exemplifies those assertions, including at the level of the HEIR 2nd layer of services package. Whereas in D4.2 the HEIR Observatory only had data from the PAGNI pilot, the current deliverable. As the use cases progressed, more and more data became available for use by the HEIR 2nd layer of services, the Global RAMA Score started being informed not by a single clinical site but by all four HEIR pilots, and the NSE/NOCLUS policies became available for inspection in the Global Policy Observatory.

The present deliverable, “D4.3 the HEIR 2nd layer of services package, final version”, is the final WP4 deliverable. Similarly, “D3.3 The HEIR 1st layer of services package, final version” is the final WP3 deliverable and “D2.3 The HEIR facilitators package: Final complete version” the final WP2 deliverable.

While WP2, WP3 and WP4 will produce no further deliverables, WP5 will conclude the project’s technical work and WP6 will conclude the validation and evaluation of the HEIR platform, whereas WP7 will finalise dissemination and exploitation activities. We highlight the main deliverables below.

- WP5: “D5.4 HEIR integrated framework final version” is to provide a more holistic view of the technical achievements of the HEIR project, presenting the final version of the HEIR integrated framework. Upcoming deliverable “D5.5 Best practices for maintaining/operating the framework in the long-run–TRL7” (M36) will present the best-practices for maintaining/operating the HEIR framework in the long-run.
- WP6: “D6.2 HEIR Demonstration -final execution” is to present the execution of the HEIR pilots. Upcoming deliverable “D6.3 Assessment report and impact analysis” (M36) will present the results of the evaluation of the HEIR platform.
- WP7: The work package will present updated reports on dissemination (D7.4), the legal framework (D7.6) and exploitation planning (D7.8) all due in M36, as well as a report on training activities (D7.10). It will also produce “D7.9 Final business model and long-term sustainability report” showing how the HEIR platform can be developed and evolve beyond the confines of the HEIR project on the basis of experience gained in it, the overall exploitation planning of D7.8, a concrete business model, taking into consideration the intellectual property rights, market access and capabilities of the HEIR Consortium partners.

These forthcoming steps will not only put the HEIR 2nd layer of services package, in the context of the overall HEIR platform (D5.4), explain how the HEIR platform was evaluated (D6.2) and present the results of this evaluation (D6.3), but ultimately explore how the subject of the present deliverable can be further exploited, transforming the HEIR research into innovation that will both offer benefits to HEIR partners and improve the security and privacy-preserving data processing capabilities of the healthcare industry (D7.8, D7.9).

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.cjbi.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. Final version of the HEIR Global Benchmarks

An example of a Global RAMA Score with associated Metadata can be seen in Figure 8 below.

```
{
  "id": "1",
  "numberOfHospitals": "3",
  "connectedHospitals":
  [
    1,
    4,
    3
  ],
  "updated": "2023-02-16 15:45:14.335",
  "ramaScore": "96.97833",
  "cyberSecurityStatus": "Low",
  "temporalScore": "0.0",
  "baseScore": "4.316666",
  "numberOfCriticalEvents": "0.0",
  "numberOfIdentifiedHeartbleeds": "0.0",
  "noOfOSVulnerabilities": "4.0",
  "noOfMisconfigurations": "1.0",
  "numberOfBenignFindings": "1.0",
  "numberOfMaliciousFindings": "0.0",
  "noOfAppVulnerabilities": "4.0",
  "numberOfAttacks": "0.0",
  "numberOfExploits": "0.0",
  "numberOfSIEMCriticalEvents": "0.0",
  "numberOfSIEMMediumEvents": "0.0",
  "numberOfSIEMHighEvents": "0.0",
  "numberOfSIEMLowEvents": "0.0",
  "totalNumberOfSIEMEvents": "0.0",
  "top10Vulnerabilities":
  {
    "CVE-2022-3725": 75,
    "CVE-2022-3724": 75,
    "CVE-2022-29072": 72,
    "CVE-2023-0412": 70,
    "CVE-2023-0415": 65,
    "CVE-2022-4345": 65,
    "CVE-2023-0413": 65,
    "CVE-2023-0416": 65,
    "CVE-2023-0417": 65,
    "CVE-2023-0411": 65
  },
  "top10FreqVulnerabilities":
  {
    "CVE-2023-0415": 277,
    "CVE-2023-0412": 277,
    "CVE-2022-4345": 277,
    "CVE-2023-0413": 277,
    "CVE-2022-4344": 277,
    "CVE-2023-0416": 277,
    "CVE-2023-0417": 277,
    "CVE-2022-3724": 277,
    "CVE-2023-0411": 277,
    "CVE-2022-3190": 277
  },
  "hospitalInformation":
  [
    {
      "id": "1",
      "ramaScore": "99.59167",
      "temporalScore": "0.0",
      "baseScore": "0.5833334",
      "connectedClients": "2",
      "criticalEvents": "0",
      "totalAttacks": "0"
    }
  ],
}
```

```

    {
      "id": "3",
      "ramaScore": "100.0",
      "temporalScore": "0.0",
      "baseScore": "0.0",
      "connectedClients": "2",
      "criticalEvents": "0",
      "totalAttacks": "0"
    },
    {
      "id": "4",
      "ramaScore": "91.34334",
      "temporalScore": "0.0",
      "baseScore": "12.366665",
      "connectedClients": "1",
      "criticalEvents": "0",
      "totalAttacks": "0"
    }
  ]
}

```

Figure 8: Global RAMA Score Calculation Result

The final version of the Global RAMA Score calculator was successfully deployed and tested in HEIR's infrastructure, as depicted in Figure 9 below.

```

...: [5, 3], "noOfClients": "2", "globalRamaScore": "99.59167", "global
...BaseScore": "0.5833334", "globalTemporalScore": "0.0", "global
Heartbleeds": "0", "noOf0SVulnerabilities": "0", "noOfMisconfigurations": "1"
, "numberOfBenignFindings": "1", "numberOfMaliciousFindings": "0",
, "noOfAppVulnerabilities": "1", "numberOfAttacks": "0", "numbe
rOfExploits": "0", "totalHNMFFindings": "0", "numberOfSIEMCriticalEvents": "0"
, "numberOfSIEMMediumEvents": "0", "numberOfSIEMHighEvents": "0",
, "numberOfSIEMLowEvents": "0", "totalNumberOfSIEMEvents": "0",
"top10Vulnerabilities": {CVE-2022-29072=72}, "top10FreqVulnerabilities": {CVE-201
1-0220=1}
2023-02-16 15:45:14.337 WARN 1 --- [ntainer#0-0-C-1] c.s.g.listener.GlobalRAMAScoreListener : Global rama calculated: {
"connectedHospitals": [1, 4, 3], "id": "1", "updated": "2023-02-16 15:45:14.335", "numberOfHospitals": "3", "ramaScore": "96.9783
3", "baseScore": "4.316666", "cyberSecurityStatus": "Low", "temporalScore": "0.0", "numberOfIde
ntifiedHeartbleeds": "0.0", "noOf0SVulnerabilities": "4.0", "noOfMisconfigur
ations": "1.0", "numberOfBenignFindings": "1.0", "numberOfMaliciousFindings":
: "0.0", "noOfAppVulnerabilities": "4.0", "numberOfAttacks": "0.0",
"numberOfExploits": "0.0", "numberOfSIEMCriticalEvents": "0.0",
"numberOfSIEMMediumEvents": "0.0", "numberOfSIEMHighEvents": "0.0", "numb
erOfSIEMLowEvents": "0.0", "totalNumberOfSIEMEvents": "0.0", "top10Vulnerabi
lities": {
"CVE-2022-3725" : 75,
"CVE-2022-3724" : 75,
"CVE-2022-29072" : 72,
"CVE-2023-0412" : 70,
"CVE-2023-0415" : 65,
"CVE-2022-4345" : 65,
"CVE-2023-0413" : 65,
"CVE-2023-0416" : 65,
"CVE-2023-0417" : 65,
"CVE-2023-0411" : 65
},
"top10FreqVulnerabilities": {
"CVE-2023-0415" : 277,
"CVE-2023-0412" : 277,
"CVE-2022-4345" : 277,
"CVE-2023-0413" : 277,
"CVE-2022-4344" : 277,
"CVE-2023-0416" : 277,
"CVE-2023-0417" : 277,
"CVE-2022-3724" : 277,
"CVE-2023-0411" : 277,
"CVE-2022-3190" : 277
},
"hospitalInformation": [{
"globalRamaScore": "99.59167", "temporalScore": "0.0", "criticalEvents": "0", "baseScore": "0.5833334", "ramaScore": "
",
"connectedClients": "2", "criticalEvents": "0", "baseScore": "0.5833334", "totalAttacks": "0"}
],
{
"criticalEvents": "0", "baseScore": "0.0", "ramaScore": "100.0", "connectedClients": "2", "temporalScore":
"0.0", "id": "3", "ramaScore": "100.0", "connectedClients": "2", "temporalScore":
"criticalEvents": "0", "totalAttacks": "0"}, {
"ramaScore": "91.34334", "connectedClients": "1", "temporalScore": "0.0", "criticalEvents": "0", "t
otalAttacks": "0"}]}
sphinx@heir1:~$

```

Figure 9: Global RAMA Score Calculator in action