D3.3

The HEIR 1st 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 1st, 2020
Duration	36 months
Programme	H2020-SU-DS-2019

Deliverable type	Demonstrator
Deliverable reference no.	D3.3
Workpackage	WP3
Due date	**28/02/2023 [M30]**
Actual submission date	

Deliverable lead	SIE
Editors	Iulia Ilie, Gabriel Danciu
Contributors	Dumitru Bogdan Prelipcean (BD), Michalis Smyrlis (STS), Iulia Ilie (SIE), Gabriel Danciu (SIE), Andreas Alexopoulos, Miltiadis Kokkonidis, Aris Sotiropoulos, Chronis Ballas (AEGIS)
Reviewers	Hervé Debar (IMT), Eftychia Lakka (FORTH)
Dissemination level	PU
Revision	final
Keywords	HEIR client, RAMA score, HEIR framework, Cybersecurity, Threat Detection

Abstract

Deliverable 3.3 documents the progress in implementing the final version of HEIR's 1st layer of services package. The work reflected within this report has been conducted between M19 and M30 and involved the partners' personnel active within WP3 and the connecting WPs such as WP2, WP4 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 1st layer of services package – the final version. The development carried from HEIR's 1st layer of services package – the 1st version demonstrates the effective implementation of the 1st layer components within a consistent integrated framework that showcases the impact of the proposed solution.

The final version of HEIR's 1st layer of services includes: (I) the novel HEIR Client; (II) the Threat Detection Module and the services for the RAMA score calculations at different levels; (III) the toolset for the visualisation of the HEIR reported security levels, incidents, threats, statistics, etc. and (IV) the novel HEIR Aggregator.

The demonstrator will be presented in a short report. The current and final version of the 1st layer of services package showcases the technical advancement achieved after the release of HEIR's 1st layer of services package – the 1st version (M18), until M30.

Table of Contents

List of Figures

1. Introduction

1.1 Scope and objectives

Deliverable D3.3 illustrates the technical progress achieved for building **the complete HEIR 1st layer of services** after the status of the HEIR 1st layer of services shown in deliverable D3.2 in M18 and until M30.

1.2 Relation to other Tasks and Work Packages

The current deliverable is the third and final report of the technical work done for **WP3: the HEIR client, RAMA calculator, GUI and Aggregator** in the HEIR project. This deliverable introduces the technical development done in **WP3** for HEIR's 1st layer of services between M19 and M30 of the HEIR project, after the WP3 progress reported in D3.2 that showcased HEIR's first complete version for the 1st layer of services. The technical work of WP3 was split in the following tasks:

- Task T3.1- The HEIR Client's Processing system
- Task T3.2- Vulnerability assessment, Threat detection and RAMA score calculation in the HEIR client
- Task T3.3- HEIR 1st layer of visualisations
- Task T3.4- The HEIR Aggregator

The development of the components of WP3 was connected to the development of components in WP2, WP4 and WP5 as well.

1.3 Structure of the document

The current document is structured as follows: **Sections 2 to 6** showcase the technical development achieved in HEIR's Work Package 3 between months 19 to 30 followed by **Conclusions** and the **Annexes** showcasing the JSON objects used to communicate between the different HEIR components developed in **WP3**.

2. The HEIR 1st layer of services

The main objective of WP3 was to design HEIR's Client and Aggregator as described in Section 1.3.2.4 and 1.3.2.6 of the Grant Agreement.

In particular, in this WP the following sub-systems, models and tools were designed and implemented:

- The novel HEIR Client.
- The threat detection module and the services for the RAMA score calculations at different levels.
- The toolset for the visualisation of the HEIR reported security levels, incidents, threats, statistics, etc. and
- The novel HEIR Aggregator.

3. The HEIR Client

3.1 Overview

The HEIR Client is the central component that collects and centralize data received from the facilitators and from the HEIR Client Components. During the final year the contribution include the update of existing components and the integration of the Threat Detection Module and SIEM product. The details about updates and integration will be described in the following subsections. In Figure 1 is the overview schema (light green the added components for the final version).

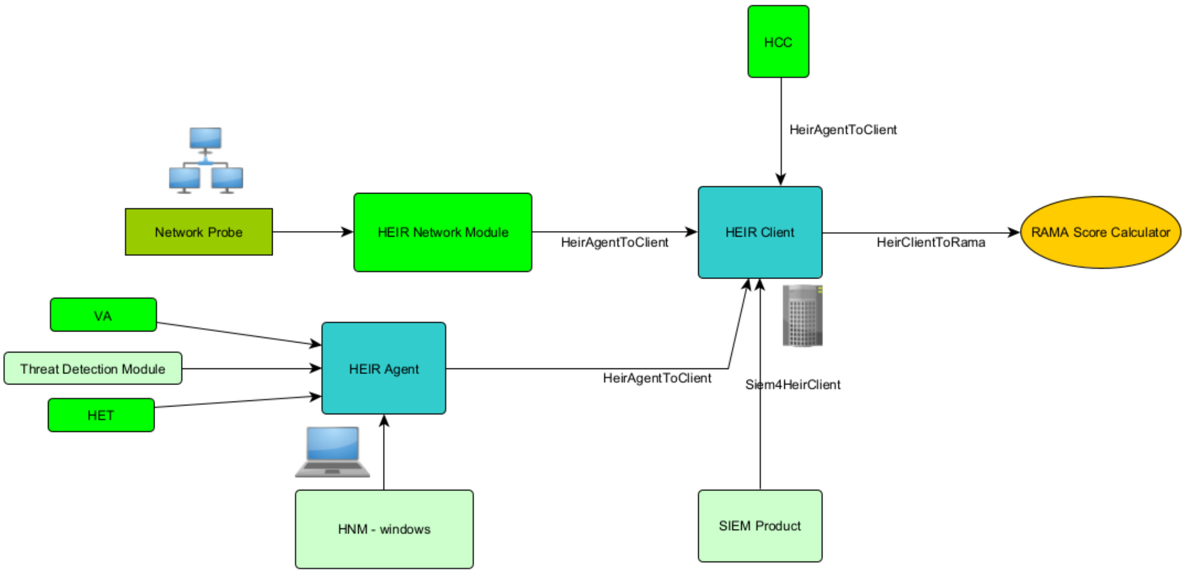


Figure 1: HEIR Client overview

In the Annex A, we also provide the overall output of the HEIR Client to the RAMA Score Calculator with the latest modules integrated.

3.2 The HEIR Network Module

We recall that the HEIR Network Module (HNM) is able to detect private information leaks, malicious content sent over the network (threat detection ability), on-going attacks over the network.

The final version of the HNM includes a Windows version that is integrated into the HEIR Agent that is able to provide more detailed information regarding about the activity on endpoints machines. It also contains updated threat definition that can be detected over the network.

3.3 The HEIR Exploit Tester

The HEIR Exploit Tester (HET) has the role to assess the attack surfaces for the operating system configuration. The final version of HET contains updated definitions for the attack surfaces and updated information regarding the possible misconfigurations.
The HEIR HET takes as input registry keys, configuration parameters from the Windows Operating system and produces as output a list of misconfigured items concerning security with recommendations and descriptions.

3.4 The HEIR Cryptographic Checker

The HEIR Cryptographic Checker (HCC) has the role to alert regarding the usage of outdated security protocols that are used inside the HEIR environment servers or to target the outside servers that are service providers for the HEIR system inside the environments.

The HCC tools are based on the open-source tool SSLScan1, and it can detect:

- The used protocol and version. This can be cross listed with the required one (latest version is recommended as default).
- Usage of vulnerable cryptographic implementations.

The output of HCC is submitted to the HEIR Client. For the final version better refining of the tool configuration and scanning triggers were added in order to provide better recommendations regarding the usage of cryptographic protocol and tools.

3.5 The Threat Detection Module

The Threat Detection Module (TDM) is a module integrated technically in the HEIR Agent but provides information to the HEIR Client in the same way and with the same meaning as the HNM. The module is able to scan local files and/or processes from an endpoint machine and to detect malicious content when executed. It provides another layer of information about malicious activity that influences further the RAMA Score and alerts.

The output contains information about the scanned object and along with information regarding the detection type (alert).

```
{
    "ScannedObject": "C:/test/samples.",
    "ObjectType": "File",
    "AlertType": "Malware",
    "event_name": "detection",
    "AlertName": "Trojan.NG.Test.1",
    "TimeCreated": 1670944872
}
```

The TDM is based on a lightweight approach of scanning technology from Bitdefender and specially tailored in order to accommodate the low impact on healthcare environments but at the same time to provide a high rated of detection.

3.6 Integrating the SIEM product

The SIEM product is integrated as a module to the HEIR Client. A connector for the SIEM product was implemented in order to submit alerts on a message broker (Kafka) topic, alerts that are then collected by the HEIR Client and submitted further to the RAMA Score Calculator. The alerts that are submitted are alerts that have a severity score over a threshold that would have an impact on the RAMA Score.

The data submitted further only contains the SIEM event description and severity score according with the SIEM product classification.

4. The LOCAL RAMA Score Calculator

4.1 Overview

As described in "D3.1 – The HEIR 1st layer of services package for the MVP" (Zacharakis, 2021) and "D3.2 - The HEIR 1st layer of services package: 1st complete version" (Mihaila, 2022), the Local RAMA Score calculator is the component responsible for the calculation of the Local RAMA score. In general, the Risk Assessment for Medical Applications (RAMA) provides a score and metadata that could help the assessed healthcare organization realize its security posture. The Local RAMA score is responsible for estimating the attack surface associated with the organization's (or a specific department's) medical devices by incorporating metrics from the risk assessment tools described in Section 2 and "D2.3 The HEIR facilitators package: Final complete version". For each participating tool, a corresponding sub-score is constructed.

4.2 Local RAMA Score – final version

During the final year of the project, two more tools were added to the suite of tools that contribute to the calculation of the Local RAMA score. The first, described in D2.3, is the HEIR's Security Information and Event Management (SIEM) tool (hereafter denoted SIEM sub-score) with the second being HEIR's Threat Detection Module which is described in Section 3.5 (hereafter denoted TDM sub-score).

For each of the newly added scores, a sub-score was created and is described in Sections 4.2.1 and 4.2.2. The rest of the sub-scores remained the same and are available in "D3.2 - The HEIR 1st layer of services package: 1st complete version". One minor update was that the Vulnerability Assessment's metadata now presents both the top 10 most frequent vulnerabilities and the top 10 most severe, per department.

Since the two newly added scores contributed to the temporal score of the Local RAMA score, the final formula for the calculation of the Local RAMA score and their two main scores, i.e., base and temporal, is as follows.

$$\text{LRS} = 0.7 * \text{Base}_{\text{score}} + 0.3 * \text{Temporal}_{\text{score}}$$

Where the $\text{Base}_{\text{score}}$ acts as a "static" risk assessment metric and incorporates the HET, Vulnerability Assessment, and Cryptographic checker sub-scores, and the $\text{Temporal}_{\text{score}}$ acts as a "dynamic" risk assessment metric incorporating HEIR's Network Module, SIEM, and Threat Detection Module sub-scores.

Concluding, the Local RAMA Score will be calculated per organisation's asset (device) and will take into consideration the threats (as identified through the Threat Detection Module), the vulnerabilities and the impact. More specifically, the impact is taken into consideration in the Aggregated Local RAMA Score (see Section 5) by incorporating the severity per department, i.e., the potential consequences if the system were to be compromised, such as loss of data, financial harm, or damage to reputation.

4.2.1 SIEM sub-score

After the integration of the SIEM product in the HEIR client, the novel SIEM sub-score contributes to the calculation of the temporal score.

The formula for calculating the SIEM sub-score (normalized from 0 to 100) takes the severity as reported through HEIR's SIEM component. Since the severity calculation is based on Wazuh's ruleset, no further reasoning is applied through the calculator. The SIEM's formula is as follows:

$$\mathrm{SIEM}_{\mathrm{score}} = \sum_{n}^{i=1} SIS_i$$

where ***n*** is the total number of identified issues and SIS_i is the SIEM impact score. The latter is calculated as follows and is based on Wazuh's rules classification (as denoted within the parentheses):

- ignored (0) = 0
- low (2-4) = 2
- medium (5-8) = 3
- high (9-12) = 5
- critical (13-14) = 8

The metadata for this sub-score includes the number of issues and the description reported from the SIEM component.

Lastly, the expected output of HEIR's SIEM component is as depicted below.

```
{
    "description":"Windows Defender: ERROR: BAD INPUT DATA",
    "severity": "12",
},
{
    "description":"Short-time multiple Windows Defender error events",
    "severity": "14"
}
```

4.2.2 Threat Detection Module (TDM) sub-score

The Threat Detection Module sub-score contributes to the calculation of the temporal score.

The formula for calculating the TDM sub-score (normalized from 0 to 100) is similar to the one of HEIR's Network Module (see D3.2). More specifically, it takes into consideration the alert type reported by the TDM as this reveals the severity of the identified issue. The alert type could be (a) none, (b) info, (c) suspicious, (d) malware, (e) attack, and (f) exploit. Based on this, the TDM formula is as follows.

$$\mathrm{TDM}_{\mathrm{score}} = \sum_{n}^{i=1} TDISi$$

where n is the total number of identified threats detected (alerts or detections) and TDIS_i is the threat detection impact score.

TDIS is calculated as:

- None = 0
- Info = 2
- Suspicious = 4
- Malware = 6
- Attack = 8
- Exploit = 10

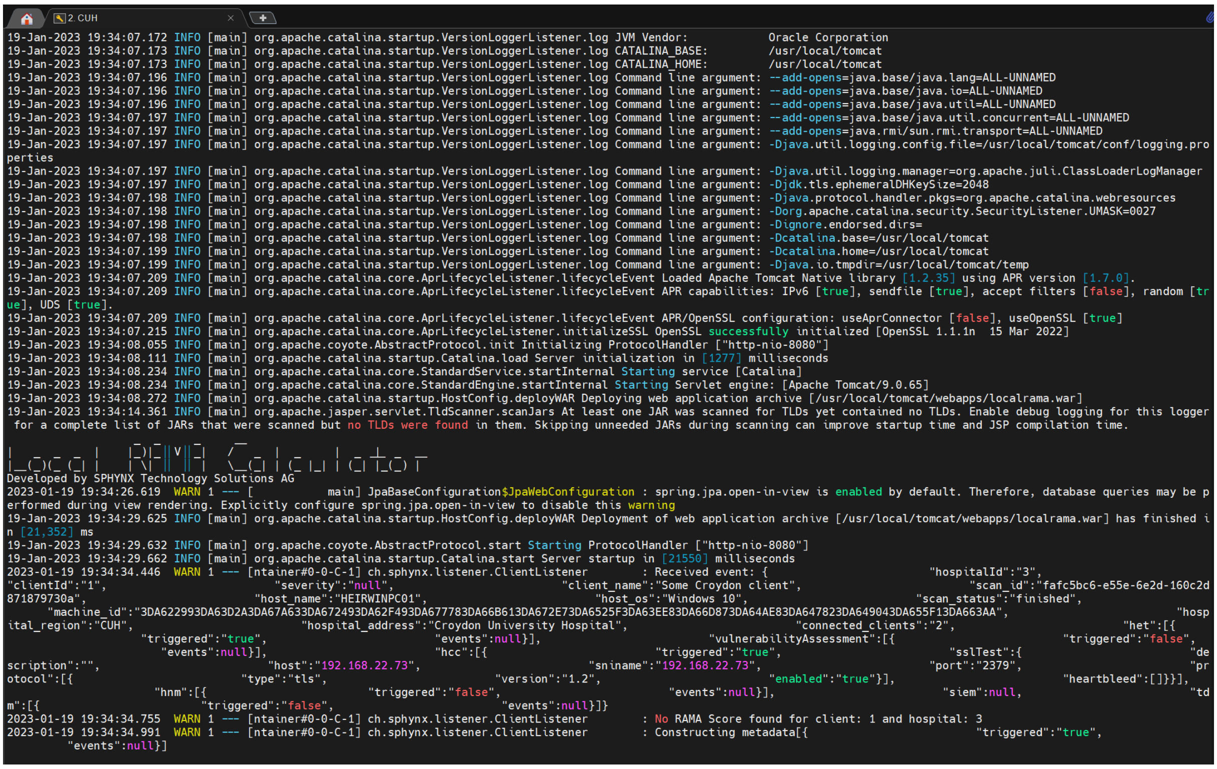
The metadata created by the Local RAMA Score calculator regarding the TDM include: (a) the number of exploits, (b) the number of attacks, and (c) the total number of findings.

Lastly, the expected output of HEIR's TDM component is as depicted below.

```
{
    "ScannedObject": "C:/test/samples.",
    "ObjectType": "File",
    "AlertType": "Malware",
    "event_name": "detection",
    "AlertName": "Trojan.NG.Test.1",
    "TimeCreated": 1670944872
}
```

4.3 Deployment

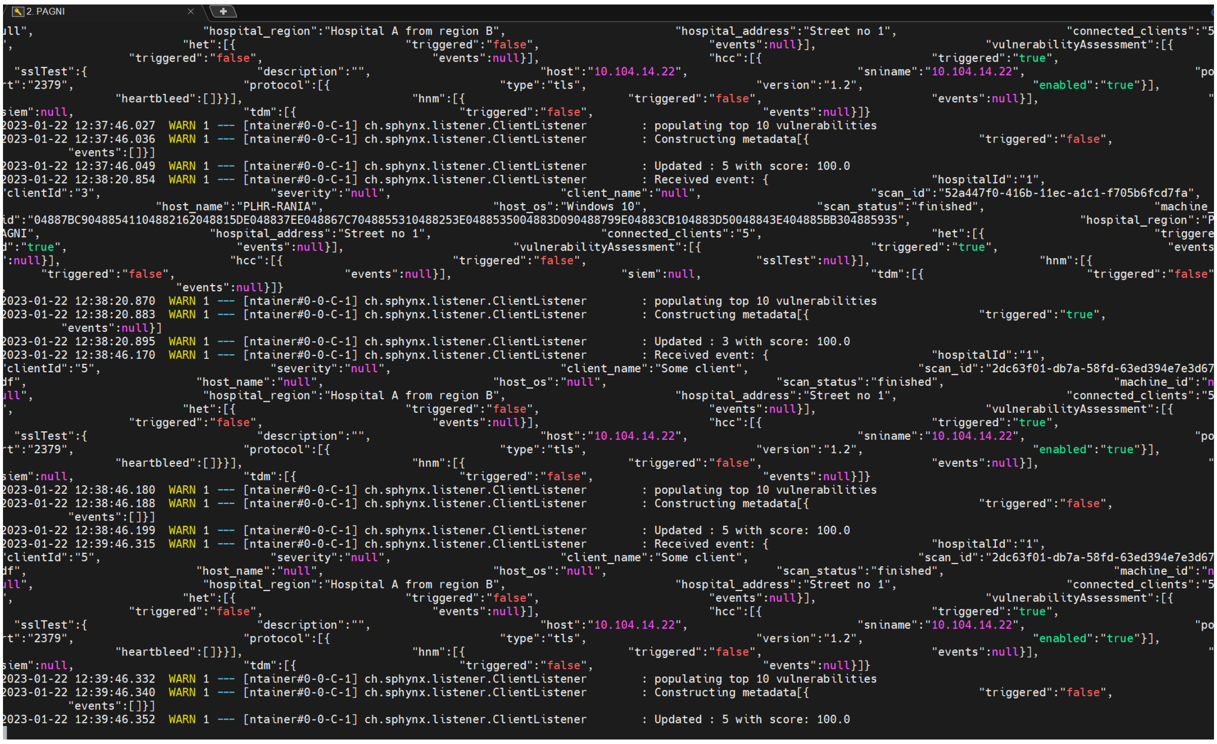
During the final year of the project, the Local RAMA Score Calculator was successfully deployed and tested in all four HEIR pilots. Figure 2 and Figure 3 show a snapshot of the installation in PAGNI's and CUH's environments.



```
19-Jan-2023 19:34:07.172 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log JVM Vendor:            Oracle Corporation
19-Jan-2023 19:34:07.173 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log CATALINA_BASE:         /usr/local/tomcat
19-Jan-2023 19:34:07.173 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log CATALINA_HOME:         /usr/local/tomcat
19-Jan-2023 19:34:07.196 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: --add-opens=java.base/java.lang=ALL-UNNAMED
19-Jan-2023 19:34:07.196 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: --add-opens=java.base/java.io=ALL-UNNAMED
19-Jan-2023 19:34:07.196 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: --add-opens=java.base/java.util=ALL-UNNAMED
19-Jan-2023 19:34:07.197 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: --add-opens=java.base/java.util.concurrent=ALL-UNNAMED
19-Jan-2023 19:34:07.197 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: --add-opens=java.rmi/sun.rmi.transport=ALL-UNNAMED
19-Jan-2023 19:34:07.197 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Djava.util.logging.config.file=/usr/local/tomcat/conf/logging.pro
perties
19-Jan-2023 19:34:07.197 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager
19-Jan-2023 19:34:07.197 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Djdk.tls.ephemeralDHKeySize=2048
19-Jan-2023 19:34:07.198 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Djava.protocol.handler.pkgs=org.apache.catalina.webresources
19-Jan-2023 19:34:07.198 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Dorg.apache.catalina.security.SecurityListener.UMASK=0027
19-Jan-2023 19:34:07.198 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Dignore.endorsed.dirs=
19-Jan-2023 19:34:07.198 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Dcatalina.base=/usr/local/tomcat
19-Jan-2023 19:34:07.199 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Dcatalina.home=/usr/local/tomcat
19-Jan-2023 19:34:07.199 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Djava.io.tmpdir=/usr/local/tomcat/temp
19-Jan-2023 19:34:07.209 INFO [main] org.apache.catalina.core.AprLifecycleListener.lifecycleEvent Loaded Apache Tomcat Native library [1.2.35] using APR version [1.7.0].
19-Jan-2023 19:34:07.209 INFO [main] org.apache.catalina.core.AprLifecycleListener.lifecycleEvent APR capabilities: IPv6 [true], sendfile [true], accept filters [false], random [tr
ue], UDS [true].
19-Jan-2023 19:34:07.209 INFO [main] org.apache.catalina.core.AprLifecycleListener.lifecycleEvent APR/OpenSSL configuration: useAprConnector [false], useOpenSSL [true]
19-Jan-2023 19:34:07.215 INFO [main] org.apache.catalina.core.AprLifecycleListener.initializeSSL OpenSSL successfully initialized [OpenSSL 1.1.1n  15 Mar 2022]
19-Jan-2023 19:34:08.055 INFO [main] org.apache.coyote.AbstractProtocol.init Initializing ProtocolHandler ["http-nio-8080"]
19-Jan-2023 19:34:08.111 INFO [main] org.apache.catalina.startup.Catalina.load Server initialization in [1277] milliseconds
19-Jan-2023 19:34:08.234 INFO [main] org.apache.catalina.core.StandardService.startInternal Starting service [Catalina]
19-Jan-2023 19:34:08.234 INFO [main] org.apache.catalina.core.StandardEngine.startInternal Starting Servlet engine: [Apache Tomcat/9.0.65]
19-Jan-2023 19:34:08.272 INFO [main] org.apache.catalina.startup.HostConfig.deployWAR Deploying web application archive [/usr/local/tomcat/webapps/localrama.war]
19-Jan-2023 19:34:14.361 INFO [main] org.apache.jasper.servlet.TldScanner.scanJars At least one JAR was scanned for TLDs yet contained no TLDs. Enable debug logging for this logger
 for a complete list of JARs that were scanned but no TLDs were found in them. Skipping unneeded JARs during scanning can improve startup time and JSP compilation time.

                          _  _     _       __
|    _  _  _  |      |_)|_|| V ||_|    /    _  |  _      |  _ _|_ _  _
|__(_)(_ (_| |       | \|  ||   ||  |   \__(_| | (_ |_| | (_| |_(_) |
Developed by SPHYNX Technology Solutions AG
2023-01-19 19:34:26.619  WARN 1 --- [           main] JpaBaseConfiguration$JpaWebConfiguration : spring.jpa.open-in-view is enabled by default. Therefore, database queries may be p
erformed during view rendering. Explicitly configure spring.jpa.open-in-view to disable this warning
19-Jan-2023 19:34:29.625 INFO [main] org.apache.catalina.startup.HostConfig.deployWAR Deployment of web application archive [/usr/local/tomcat/webapps/localrama.war] has finished i
n [21,352] ms
19-Jan-2023 19:34:29.632 INFO [main] org.apache.coyote.AbstractProtocol.start Starting ProtocolHandler ["http-nio-8080"]
19-Jan-2023 19:34:29.662 INFO [main] org.apache.catalina.startup.Catalina.start Server startup in [21550] milliseconds
2023-01-19 19:34:34.446  WARN 1 --- [ntainer#0-0-C-1] ch.sphynx.listener.ClientListener        : Received event: {                        "hospitalId":"3",
"clientId":"1",                       "severity":"null",                          "client_name":"Some Croydon client",                        "scan_id":"fafc5bc6-e55e-6e2d-160c2d
871879730a",                       "host_name":"HEIRWINPC01",                         "host_os":"Windows 10",                         "scan_status":"finished",
      "machine_id":"3DA622993DA63D2A3DA67A633DA672493DA62F493DA677783DA66B613DA672E73DA6525F3DA63EE83DA66D873DA64AE83DA647823DA649043DA655F13DA663AA",                          "hosp
ital_region":"CUH",                        "hospital_address":"Croydon University Hospital",                        "connected_clients":"2",                        "het":[{
                    "triggered":"true",                   "events":null}],                        "vulnerabilityAssessment":[{                       "triggered":"false",
                       "events":null}],                   "hcc":[{                        "triggered":"true",                        "sslTest":{                          "de
scription":"",                       "host":"192.168.22.73",                        "sniname":"192.168.22.73",                        "port":"2379",                        "pr
otocol":[{                        "type":"tls",                        "version":"1.2",                        "enabled":"true"}],                        "heartbleed":[]}}],
                      "hnm":[{                        "triggered":"false",                        "events":null}],                        "siem":null,                        "td
m":[{                        "triggered":"false",                        "events":null}]}
2023-01-19 19:34:34.755  WARN 1 --- [ntainer#0-0-C-1] ch.sphynx.listener.ClientListener        : No RAMA Score found for client: 1 and hospital: 3
2023-01-19 19:34:34.991  WARN 1 --- [ntainer#0-0-C-1] ch.sphynx.listener.ClientListener        : Constructing metadata[{                        "triggered":"true",
         "events":null}]
```

Figure 2: Local RAMA Calculator (CUH)



```
ull",                         "hospital_region":"Hospital A from region B",                         "hospital_address":"Street no 1",                          "connected_clients":"5
',                         "het":[{                         "triggered":"false",                         "events":null}],                          "vulnerabilityAssessment":[{
                   "triggered":"false",                         "events":null}],                         "hcc":[{                         "triggered":"true",
 "sslTest":{                          "description":"",                         "host":"10.104.14.22",                          "sniname":"10.104.14.22",                         "po
rt":"2379",                         "protocol":[{                         "type":"tls",                         "version":"1.2",                         "enabled":"true"}],
                 "heartbleed":[]}}],                         "hnm":[{                        "triggered":"false",                         "events":null}],                          "
siem":null,                         "tdm":[{                        "triggered":"false",                         "events":null}]}
2023-01-22 12:37:46.027  WARN 1 --- [ntainer#0-0-C-1] ch.sphynx.listener.ClientListener        : populating top 10 vulnerabilities
2023-01-22 12:37:46.036  WARN 1 --- [ntainer#0-0-C-1] ch.sphynx.listener.ClientListener        : Constructing metadata[{                         "triggered":"false",
          "events":[]}]
2023-01-22 12:37:46.049  WARN 1 --- [ntainer#0-0-C-1] ch.sphynx.listener.ClientListener        : Updated : 5 with score: 100.0
2023-01-22 12:38:20.854  WARN 1 --- [ntainer#0-0-C-1] ch.sphynx.listener.ClientListener        : Received event: {                        "hospitalId":"1",
'clientId":"3",                          "severity":"null",                        "client_name":"null",                         "scan_id":"52a447f0-416b-11ec-a1c1-f705b6fcd7fa",
                       "host_name":"PLHR-RANIA",                         "host_os":"Windows 10",                         "scan_status":"finished",                          "machine_
id":"04887BC90488541104882162048815DE048837EE048867C7048855310488253E0488535004883D090488799E04883CB104883D50048843E404885BB304885935",                         "hospital_region":"P
AGNI",                         "hospital_address":"Street no 1",                         "connected_clients":"5",                         "het":[{                          "triggere
d":"true",                         "events":null}],                         "vulnerabilityAssessment":[{                         "triggered":"true",                          "events
':null}],                         "hcc":[{                         "triggered":"false",                         "sslTest":null}],                          "hnm":[{
      "triggered":"false",                         "events":null}],                         "siem":null,                         "tdm":[{                         "triggered":"false"
,                         "events":null}]}
2023-01-22 12:38:20.870  WARN 1 --- [ntainer#0-0-C-1] ch.sphynx.listener.ClientListener        : populating top 10 vulnerabilities
2023-01-22 12:38:20.883  WARN 1 --- [ntainer#0-0-C-1] ch.sphynx.listener.ClientListener        : Constructing metadata[{                         "triggered":"true",
         "events":null}]
2023-01-22 12:38:20.895  WARN 1 --- [ntainer#0-0-C-1] ch.sphynx.listener.ClientListener        : Updated : 3 with score: 100.0
2023-01-22 12:38:46.170  WARN 1 --- [ntainer#0-0-C-1] ch.sphynx.listener.ClientListener        : Received event: {                        "hospitalId":"1",
'clientId":"5",                          "severity":"null",                        "client_name":"Some client",                          "scan_id":"2dc63f01-db7a-58fd-63ed394e7e3d67
df",                         "host_name":"null",                         "host_os":"null",                         "scan_status":"finished",                          "machine_id":"n
ull",                         "hospital_region":"Hospital A from region B",                         "hospital_address":"Street no 1",                          "connected_clients":"5
',                         "het":[{                         "triggered":"false",                         "events":null}],                          "vulnerabilityAssessment":[{
                   "triggered":"false",                         "events":null}],                         "hcc":[{                         "triggered":"true",
 "sslTest":{                          "description":"",                         "host":"10.104.14.22",                          "sniname":"10.104.14.22",                         "po
rt":"2379",                         "protocol":[{                         "type":"tls",                         "version":"1.2",                         "enabled":"true"}],
                 "heartbleed":[]}}],                         "hnm":[{                        "triggered":"false",                         "events":null}],                          "
siem":null,                         "tdm":[{                        "triggered":"false",                         "events":null}]}
2023-01-22 12:38:46.180  WARN 1 --- [ntainer#0-0-C-1] ch.sphynx.listener.ClientListener        : populating top 10 vulnerabilities
2023-01-22 12:38:46.188  WARN 1 --- [ntainer#0-0-C-1] ch.sphynx.listener.ClientListener        : Constructing metadata[{                         "triggered":"false",
          "events":[]}]
2023-01-22 12:38:46.199  WARN 1 --- [ntainer#0-0-C-1] ch.sphynx.listener.ClientListener        : Updated : 5 with score: 100.0
2023-01-22 12:39:46.315  WARN 1 --- [ntainer#0-0-C-1] ch.sphynx.listener.ClientListener        : Received event: {                        "hospitalId":"1",
'clientId":"5",                          "severity":"null",                        "client_name":"Some client",                          "scan_id":"2dc63f01-db7a-58fd-63ed394e7e3d67
df",                         "host_name":"null",                         "host_os":"null",                         "scan_status":"finished",                          "machine_id":"n
ull",                         "hospital_region":"Hospital A from region B",                         "hospital_address":"Street no 1",                          "connected_clients":"5
',                         "het":[{                         "triggered":"false",                         "events":null}],                          "vulnerabilityAssessment":[{
                   "triggered":"false",                         "events":null}],                         "hcc":[{                         "triggered":"true",
 "sslTest":{                          "description":"",                         "host":"10.104.14.22",                          "sniname":"10.104.14.22",                         "po
rt":"2379",                         "protocol":[{                         "type":"tls",                         "version":"1.2",                         "enabled":"true"}],
                 "heartbleed":[]}}],                         "hnm":[{                        "triggered":"false",                         "events":null}],                          "
siem":null,                         "tdm":[{                        "triggered":"false",                         "events":null}]}
2023-01-22 12:39:46.332  WARN 1 --- [ntainer#0-0-C-1] ch.sphynx.listener.ClientListener        : populating top 10 vulnerabilities
2023-01-22 12:39:46.340  WARN 1 --- [ntainer#0-0-C-1] ch.sphynx.listener.ClientListener        : Constructing metadata[{                         "triggered":"false",
          "events":[]}]
2023-01-22 12:39:46.352  WARN 1 --- [ntainer#0-0-C-1] ch.sphynx.listener.ClientListener        : Updated : 5 with score: 100.0
```

Figure 3: Local RAMA Calculator (PAGNI)

Finally, the final Local RAMA score schema is provided in Annex B – Local RAMA Score Calculator sample JSON output.

5. The HEIR 1st layer of services’ Graphical User Interface

5.1 Overview

As described in “D3.1 – The HEIR 1st layer of services package for the MVP“ and “D3.2 - The HEIR 1st layer of services package: 1st complete version”, 1st Layer GUI is a user-friendly dashboard that serves as the access point for authorized hospital staff to the HEIR services. It provides both hospital and department level security related information, meaningful metrics, recommendations, auditing insights and a micro-browser that fetches information from the HEIR Observatory. Through the 1st Layer GUI, security analysts can access the FVT (Forensics Visualisation Toolkit) for further departmental or device specific investigation. FVT provides detailed security relevant information, including ML outcomes, SIEM reports and RAMA score’s metadata. It also includes tools for investigating potential security incidents and identifying areas for improvement. The 1st Layer GUI is an essential tool for hospital security, helping security analysts to quickly identify and respond to potential security incidents, reducing the risk of harm to patients, staff, and hospital infrastructure.

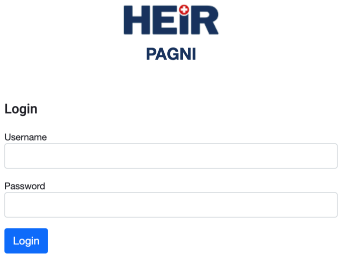
5.2 *First Layer GUI – final version*

5.2.1 Introduction

During the last year, the first layer graphical user interface (GUI) of the project has undergone several changes to enhance its functionality and usability. This section aims to present the new additions made to the 1st Layer GUI.

5.2.2 New Additions

A login page that restricts access to certain functionalities based on the user's role has been integrated (Figure 4). Security experts can access FVT and initiate forensics investigation, supported by a variety of visualization widgets and filtering capabilities. A detailed description of the latest updates for FVT can be found at "D2.3 The HEIR facilitators package: Final complete version".



Login

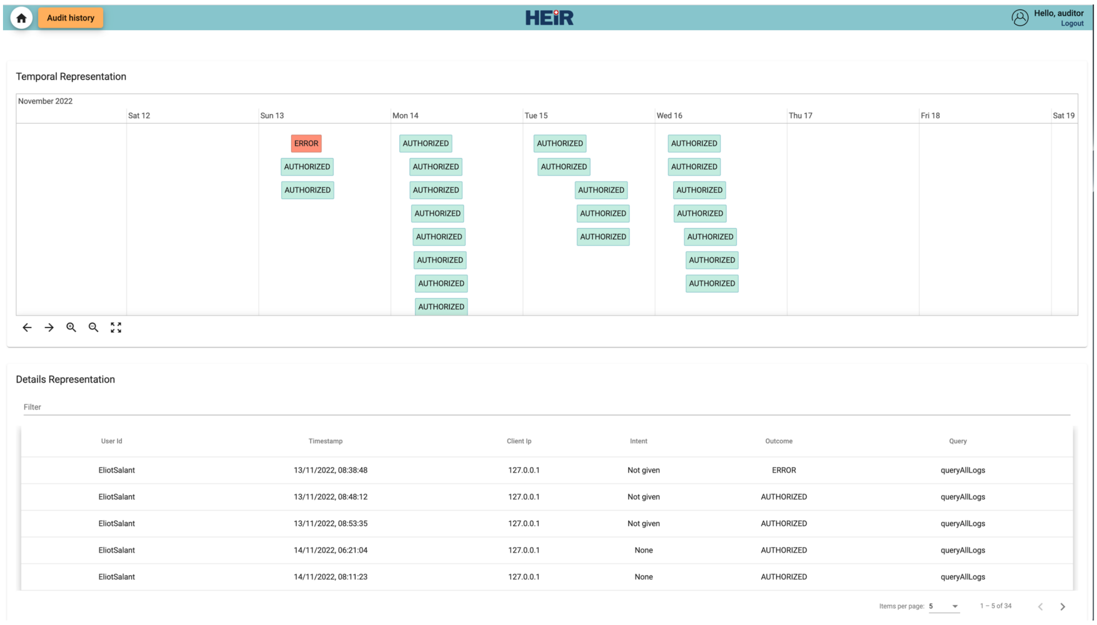
Username

Password

Login

Figure 4: Login page

Hospital's auditors are now able to access the "Audit history" page, so to monitor the access requests of the users (Figure 5, enlarged screenshot available in Annex D). These requests have been made through the PAF (Privacy Aware Framework) and were recorded to the HEIR's Blockchain. (More details about PAF and the Blockchain's functionalities were described in D2.3 as well).



Temporal Representation

Details Representation

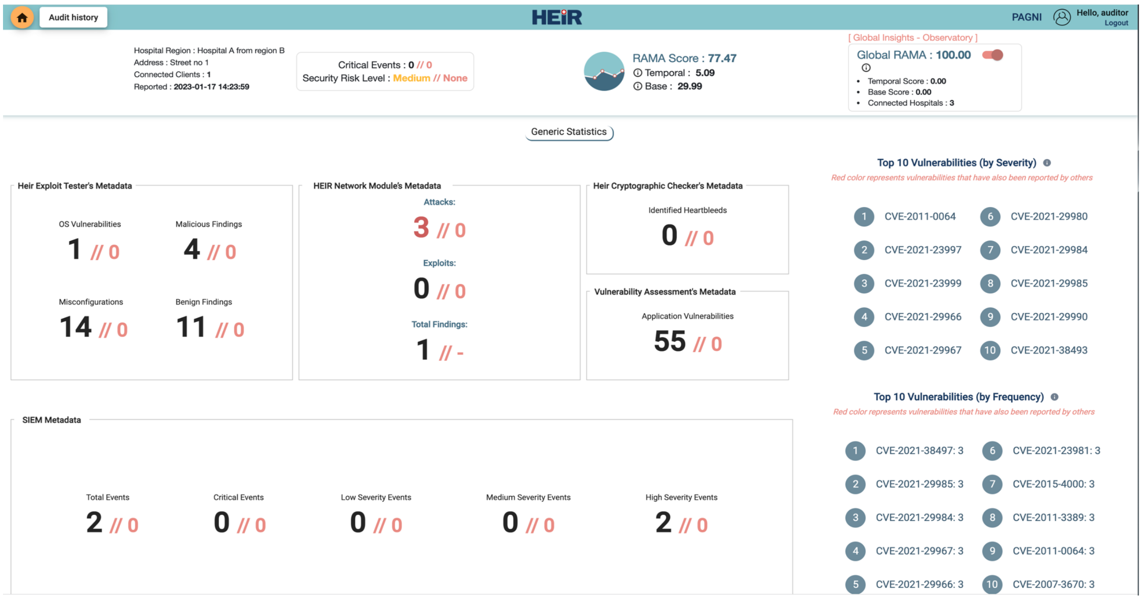
Filter

User Id	Timestamp	Client Ip	Intent	Outcome	Query
EliotSalant	13/11/2022, 08:38:48	127.0.0.1	Not given	ERROR	queryAllLogs
EliotSalant	13/11/2022, 08:48:12	127.0.0.1	Not given	AUTHORIZED	queryAllLogs
EliotSalant	13/11/2022, 08:53:35	127.0.0.1	Not given	AUTHORIZED	queryAllLogs
EliotSalant	14/11/2022, 06:21:04	127.0.0.1	None	AUTHORIZED	queryAllLogs
EliotSalant	14/11/2022, 08:11:23	127.0.0.1	None	AUTHORIZED	queryAllLogs

Items per page: 5 1 – 5 of 34

Figure 5: Audit History page (logged in as Auditor)

User roles with limited permissions can also monitor the access requests, but the derived information is redacted in terms of sensitive identifiers (Figure 6, full size screenshot available in Annex D).



Hospital Region : Hospital A from region B
Address : Street no 1
Connected Clients : 1
Reported : 2023-01-17 14:23:59

Critical Events : 0 // 0
Security Risk Level : Medium // None

RAMA Score : 77.47
Temporal : 5.09
Base : 29.99

[Global Insights - Observatory]
Global RAMA : 100.00
- Temporal Score : 0.00
- Base Score : 0.00
- Connected Hospitals : 3

Heir Exploit Tester's Metadata

OS Vulnerabilities: 1 // 0
Malicious Findings: 4 // 0
Misconfigurations: 14 // 0
Benign Findings: 11 // 0

HEIR Network Module's Metadata

Attacks: 3 // 0
Exploits: 0 // 0
Total Findings: 1 // -

Heir Cryptographic Checker's Metadata

Identified Heartbleeds: 0 // 0

Vulnerability Assessment's Metadata

Application Vulnerabilities: 55 // 0

SIEM Metadata

Total Events	Critical Events	Low Severity Events	Medium Severity Events	High Severity Events
2 // 0	0 // 0	0 // 0	0 // 0	2 // 0

Top 10 Vulnerabilities (by Severity)
Red color represents vulnerabilities that have also been reported by others

1	CVE-2011-0064	6	CVE-2021-29980
2	CVE-2021-23997	7	CVE-2021-29984
3	CVE-2021-23999	8	CVE-2021-29985
4	CVE-2021-29966	9	CVE-2021-29990
5	CVE-2021-29967	10	CVE-2021-38493

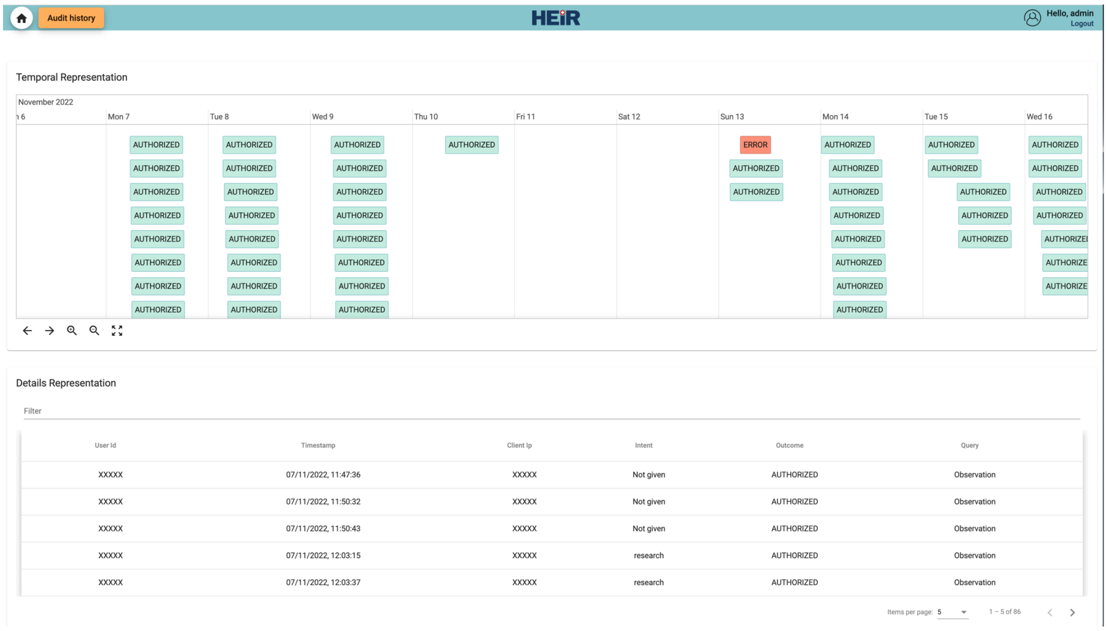
Top 10 Vulnerabilities (by Frequency)
Red color represents vulnerabilities that have also been reported by others

1	CVE-2021-38497: 3	6	CVE-2021-23981: 3
2	CVE-2021-29985: 3	7	CVE-2015-4000: 3
3	CVE-2021-29984: 3	8	CVE-2011-3389: 3
4	CVE-2021-29967: 3	9	CVE-2011-0064: 3
5	CVE-2021-29966: 3	10	CVE-2007-3670: 3

Figure 6: Audit History page (logged in as Admin)

Moreover, 1st Layer GUI now provides users the ability to compare their hospital's aggregated insights with those that have been produced in the Observatory, such as the Global RAMA score and the corresponding metadata and security related metrics, but also to identify common vulnerabilities between their environment and the most severe or frequent ones inside the whole HEIR ecosystem. (Reported from all hospitals). This comparison functionality can be enabled or disabled via a toggle button that is located on the top right of the screen.

Besides the above-described comparison visualization addition, 1st Layer GUI has been enriched with sections that provide meaningful information, such as aggregated metrics from HEIR's SIEM or the Top 10 identified Vulnerabilities across all departments, sorted either by frequency or severity score (Figure 7, full size screenshot available in Annex D).



Temporal Representation

November 2022

6	Mon 7	Tue 8	Wed 9	Thu 10	Fri 11	Sat 12	Sun 13	Mon 14	Tue 15	Wed 16
	AUTHORIZED	AUTHORIZED	AUTHORIZED	AUTHORIZED			ERROR	AUTHORIZED	AUTHORIZED	AUTHORIZED
	AUTHORIZED	AUTHORIZED	AUTHORIZED				AUTHORIZED	AUTHORIZED	AUTHORIZED	AUTHORIZED
	AUTHORIZED	AUTHORIZED	AUTHORIZED				AUTHORIZED	AUTHORIZED	AUTHORIZED	AUTHORIZED
	AUTHORIZED	AUTHORIZED	AUTHORIZED					AUTHORIZED	AUTHORIZED	AUTHORIZED
	AUTHORIZED	AUTHORIZED	AUTHORIZED					AUTHORIZED	AUTHORIZED	AUTHORIZEI
	AUTHORIZED	AUTHORIZED	AUTHORIZED					AUTHORIZED		AUTHORIZE
	AUTHORIZED	AUTHORIZED	AUTHORIZED					AUTHORIZED		AUTHORIZE
	AUTHORIZED	AUTHORIZED	AUTHORIZED					AUTHORIZED		

Details Representation

Filter

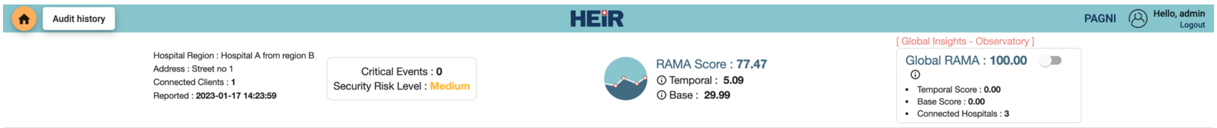
User Id	Timestamp	Client Ip	Intent	Outcome	Query
XXXXX	07/11/2022, 11:47:36	XXXXX	Not given	AUTHORIZED	Observation
XXXXX	07/11/2022, 11:50:32	XXXXX	Not given	AUTHORIZED	Observation
XXXXX	07/11/2022, 11:50:43	XXXXX	Not given	AUTHORIZED	Observation
XXXXX	07/11/2022, 12:03:15	XXXXX	research	AUTHORIZED	Observation
XXXXX	07/11/2022, 12:03:37	XXXXX	research	AUTHORIZED	Observation

Items per page: 5 1 – 5 of 86

Figure 7: HEIR Client GUI page with comparisons and SIEM metrics

5.2.3 Overview

Users who access the 1st layer of visualizations are able to see the aggregated RAMA scores, including RAMA, Base, and Temporal scores, generated by the HEIR Aggregator, along with general information about the hospital and its security status, which is part of the aggregator's output metadata. The HCG's page displays the average statistical data and indicators for the Global RAMA Score, which are obtained from the Observatory and are located in the upper right section, as depicted in Figure 8.



Hospital Region : Hospital A from region B
Address : Street no 1
Connected Clients : **1**
Reported : **2023-01-17 14:23:59**

Critical Events : **0**
Security Risk Level : Medium

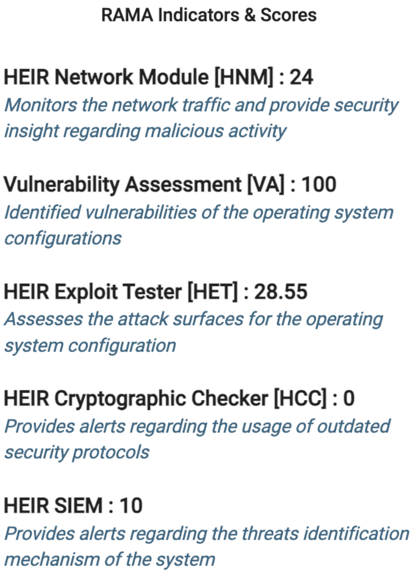
RAMA Score : **77.47**
ⓘ Temporal : **5.09**
ⓘ Base : **29.99**

[Global Insights - Observatory]
Global RAMA : **100.00**
ⓘ

- Temporal Score : **0.00**
- Base Score : **0.00**
- Connected Hospitals : **3**

Figure 8: Local and Global RAMA scores

A brief overview of the modules that contribute to the calculation of RAMA scores, along with their corresponding value indicators, is presented in Figure 9.



RAMA Indicators & Scores

HEIR Network Module [HNM] : 24
Monitors the network traffic and provide security insight regarding malicious activity

Vulnerability Assessment [VA] : 100
Identified vulnerabilities of the operating system configurations

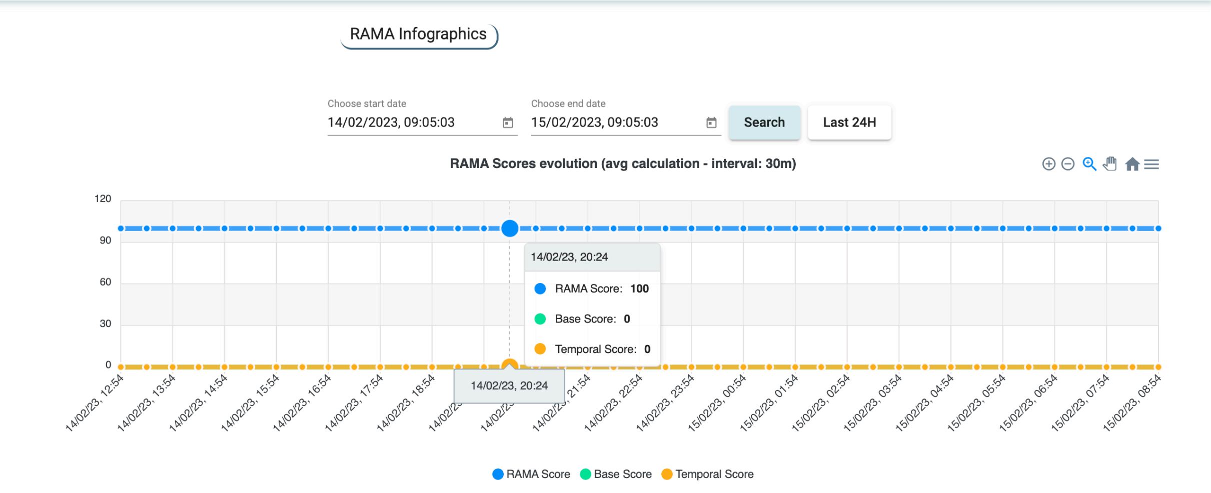
HEIR Exploit Tester [HET] : 28.55
Assesses the attack surfaces for the operating system configuration

HEIR Cryptographic Checker [HCC] : 0
Provides alerts regarding the usage of outdated security protocols

HEIR SIEM : 10
Provides alerts regarding the threats identification mechanism of the system

Figure 9: RAMA sub-scores

Moreover, ‘RAMA Infographics’ section includes a multi series line-chart that demonstrates the evolution of the aggregated scores through time, to enhance the end-user’s awareness and better monitor the deviations of the scores (Figure 10).



RAMA Infographics

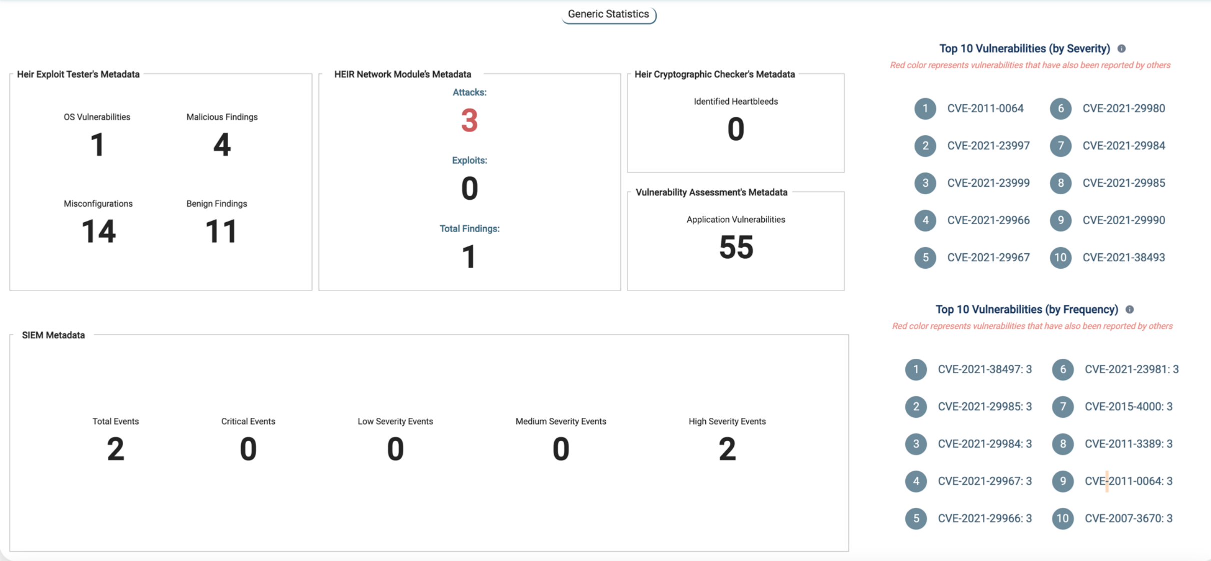
Choose start date: 14/02/2023, 09:05:03

Choose end date: 15/02/2023, 09:05:03

Figure 10: Historical RAMA Score evolution

The Aggregator's metadata includes information on the embedded modules of the HEIR Client in each department. This 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.

In addition, the top 10 vulnerabilities are presented, with a graph depicting the top 10 vulnerabilities by severity in the upper section and by frequency in the lower section (Figure 11).



Generic Statistics

Heir Exploit Tester's Metadata

OS Vulnerabilities: 1

Malicious Findings: 4

Misconfigurations: 14

Benign Findings: 11

HEIR Network Module's Metadata

Attacks: 3

Exploits: 0

Total Findings: 1

Heir Cryptographic Checker's Metadata

Identified Heartbleeds: 0

Vulnerability Assessment's Metadata

Application Vulnerabilities: 55

SIEM Metadata

Total Events	Critical Events	Low Severity Events	Medium Severity Events	High Severity Events
2	0	0	0	2

Top 10 Vulnerabilities (by Severity)

Red color represents vulnerabilities that have also been reported by others

1	CVE-2011-0064	6	CVE-2021-29980
2	CVE-2021-23997	7	CVE-2021-29984
3	CVE-2021-23999	8	CVE-2021-29985
4	CVE-2021-29966	9	CVE-2021-29990
5	CVE-2021-29967	10	CVE-2021-38493

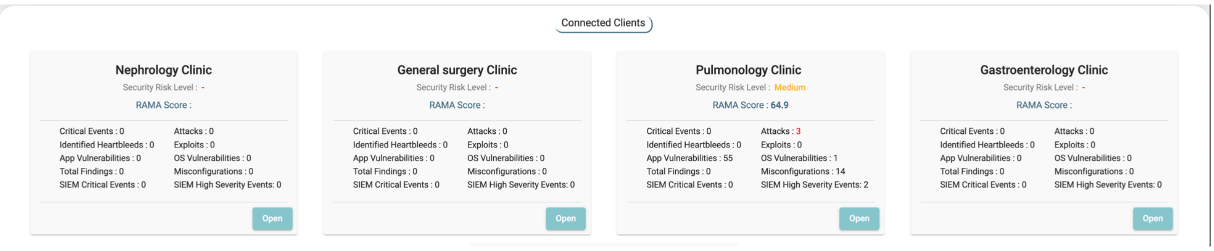
Top 10 Vulnerabilities (by Frequency)

Red color represents vulnerabilities that have also been reported by others

1	CVE-2021-38497: 3	6	CVE-2021-23981: 3
2	CVE-2021-29985: 3	7	CVE-2015-4000: 3
3	CVE-2021-29984: 3	8	CVE-2011-3389: 3
4	CVE-2021-29967: 3	9	CVE-2011-0064: 3
5	CVE-2021-29966: 3	10	CVE-2007-3670: 3

Figure 11: Client Statistics and top 10 vulnerabilities

At the bottom of the page users can check the connected departments (additional HEIR Clients) of the hospital (Figure 12). A summary of useful information is displayed and the option to further investigate a selected client is available. ('Open' button). By opening a specific client, user access the FVT's home page, which was mentioned in section 4.2.2.



Nephrology Clinic
Security Risk Level : -
RAMA Score :

Critical Events : 0
Identified Heartbleeds : 0
App Vulnerabilities : 0
Total Findings : 0
SIEM Critical Events : 0
Attacks : 0
Exploits : 0
OS Vulnerabilities : 0
Misconfigurations : 0
SIEM High Severity Events: 0

General surgery Clinic
Security Risk Level : -
RAMA Score :

Critical Events : 0
Identified Heartbleeds : 0
App Vulnerabilities : 0
Total Findings : 0
SIEM Critical Events : 0
Attacks : 0
Exploits : 0
OS Vulnerabilities : 0
Misconfigurations : 0
SIEM High Severity Events: 0

Pulmonology Clinic
Security Risk Level : Medium
RAMA Score : 64.9

Critical Events : 0
Identified Heartbleeds : 0
App Vulnerabilities : 55
Total Findings : 0
SIEM Critical Events : 0
Attacks : 3
Exploits : 0
OS Vulnerabilities : 1
Misconfigurations : 14
SIEM High Severity Events: 2

Gastroenterology Clinic
Security Risk Level : -
RAMA Score :

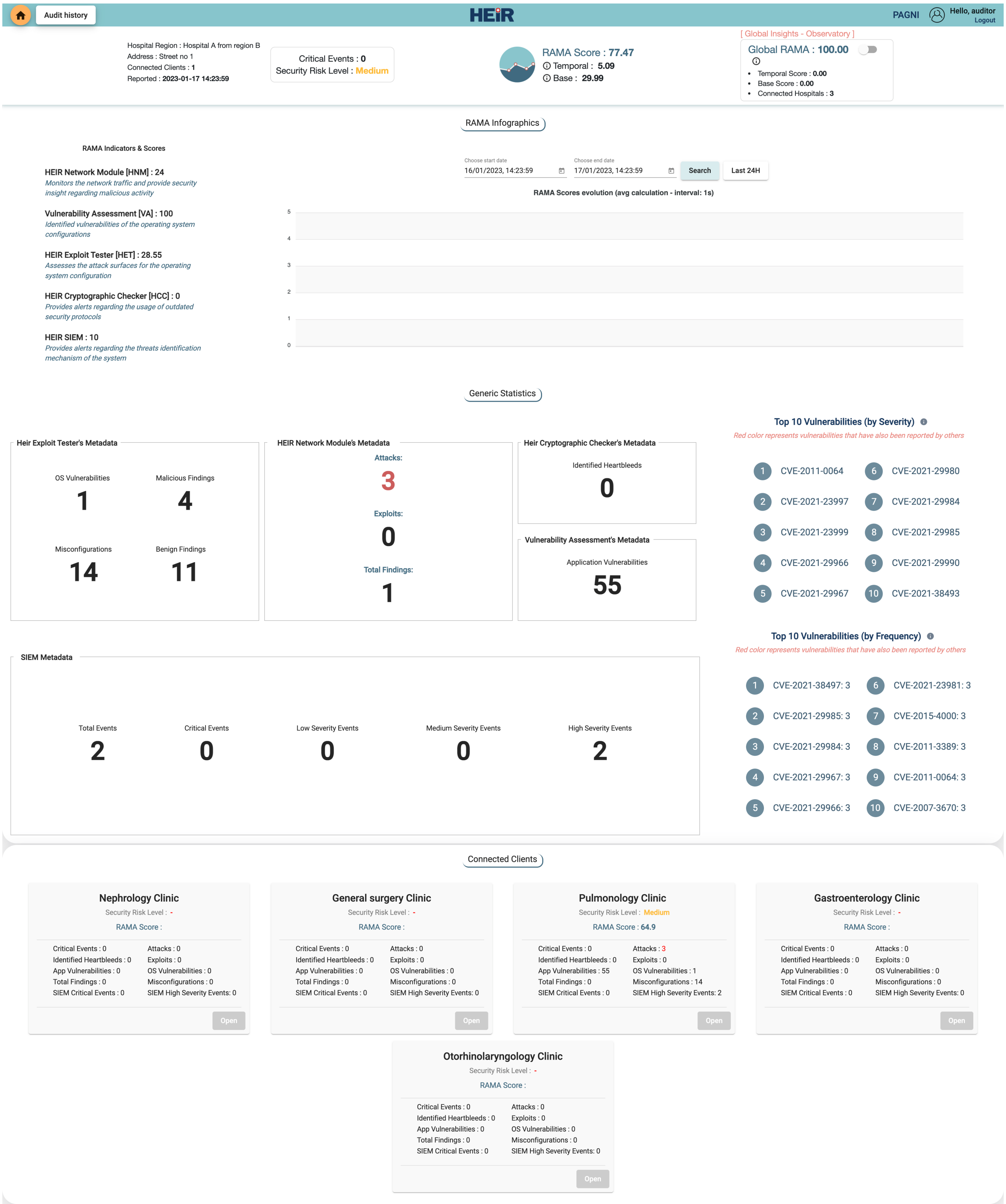
Critical Events : 0
Identified Heartbleeds : 0
App Vulnerabilities : 0
Total Findings : 0
SIEM Critical Events : 0
Attacks : 0
Exploits : 0
OS Vulnerabilities : 0
Misconfigurations : 0
SIEM High Severity Events: 0

Figure 12: Connected Clients

The complete HCG page is presented in **Erreur ! Source du renvoi introuvable.** below.

5.2.4 Conclusion

The visualization updates made to the 1st Layer GUI have improved its functionality and usability, so to compose a robust security dashboard for the hospital’s staff. The new features enhance the GUI's overall performance and users experience. The additions of the Audit History screen and the local with global comparison capability, provide extra tools in the bucket of HEIR services and also integrate the outcomes of different services into a single dashboard.



Hospital Region : Hospital A from region B
Address : Street no 1
Connected Clients : **1**
Reported : **2023-01-17 14:23:59**

Critical Events : **0**
Security Risk Level : **Medium**

RAMA Score : **77.47**
Temporal : **5.09**
Base : **29.99**

[Global Insights - Observatory]

Global RAMA : **100.00**

- Temporal Score : **0.00**
- Base Score : **0.00**
- Connected Hospitals : **3**

RAMA Infographics

RAMA Indicators & Scores

HEIR Network Module [HNM] : 24
Monitors the network traffic and provide security insight regarding malicious activity

Vulnerability Assessment [VA] : 100
Identified vulnerabilities of the operating system configurations

HEIR Exploit Tester [HET] : 28.55
Assesses the attack surfaces for the operating system configuration

HEIR Cryptographic Checker [HCC] : 0
Provides alerts regarding the usage of outdated security protocols

HEIR SIEM : 10
Provides alerts regarding the threats identification mechanism of the system

16/01/2023, 14:23:59
17/01/2023, 14:23:59

RAMA Scores evolution (avg calculation - interval: 1s)

Generic Statistics

Heir Exploit Tester's Metadata

OS Vulnerabilities	Malicious Findings
1	4
Misconfigurations	Benign Findings
14	11

HEIR Network Module's Metadata

Attacks: 3

Exploits: 0

Total Findings: 1

Heir Cryptographic Checker's Metadata

Identified Heartbleeds
0

Vulnerability Assessment's Metadata

Application Vulnerabilities
55

SIEM Metadata

Total Events	Critical Events	Low Severity Events	Medium Severity Events	High Severity Events
2	0	0	0	2

Top 10 Vulnerabilities (by Severity)

Red color represents vulnerabilities that have also been reported by others

1	CVE-2011-0064	6	CVE-2021-29980
2	CVE-2021-23997	7	CVE-2021-29984
3	CVE-2021-23999	8	CVE-2021-29985
4	CVE-2021-29966	9	CVE-2021-29990
5	CVE-2021-29967	10	CVE-2021-38493

Top 10 Vulnerabilities (by Frequency)

Red color represents vulnerabilities that have also been reported by others

1	CVE-2021-38497: 3	6	CVE-2021-23981: 3
2	CVE-2021-29985: 3	7	CVE-2015-4000: 3
3	CVE-2021-29984: 3	8	CVE-2011-3389: 3
4	CVE-2021-29967: 3	9	CVE-2011-0064: 3
5	CVE-2021-29966: 3	10	CVE-2007-3670: 3

Connected Clients

Nephrology Clinic
Security Risk Level : -
RAMA Score :

Critical Events : 0	Attacks : 0
Identified Heartbleeds : 0	Exploits : 0
App Vulnerabilities : 0	OS Vulnerabilities : 0
Total Findings : 0	Misconfigurations : 0
SIEM Critical Events : 0	SIEM High Severity Events: 0

General surgery Clinic
Security Risk Level : -
RAMA Score :

Critical Events : 0	Attacks : 0
Identified Heartbleeds : 0	Exploits : 0
App Vulnerabilities : 0	OS Vulnerabilities : 0
Total Findings : 0	Misconfigurations : 0
SIEM Critical Events : 0	SIEM High Severity Events: 0

Pulmonology Clinic
Security Risk Level : Medium
RAMA Score : 64.9

Critical Events : 0	Attacks : 3
Identified Heartbleeds : 0	Exploits : 0
App Vulnerabilities : 55	OS Vulnerabilities : 1
Total Findings : 0	Misconfigurations : 14
SIEM Critical Events : 0	SIEM High Severity Events: 2

Gastroenterology Clinic
Security Risk Level : -
RAMA Score :

Critical Events : 0	Attacks : 0
Identified Heartbleeds : 0	Exploits : 0
App Vulnerabilities : 0	OS Vulnerabilities : 0
Total Findings : 0	Misconfigurations : 0
SIEM Critical Events : 0	SIEM High Severity Events: 0

Otorhinolaryngology Clinic
Security Risk Level : -
RAMA Score :

Critical Events : 0	Attacks : 0
Identified Heartbleeds : 0	Exploits : 0
App Vulnerabilities : 0	OS Vulnerabilities : 0
Total Findings : 0	Misconfigurations : 0
SIEM Critical Events : 0	SIEM High Severity Events: 0

Figure 13: Complete page of HEIR Client GUI

6. The HEIR Aggregator

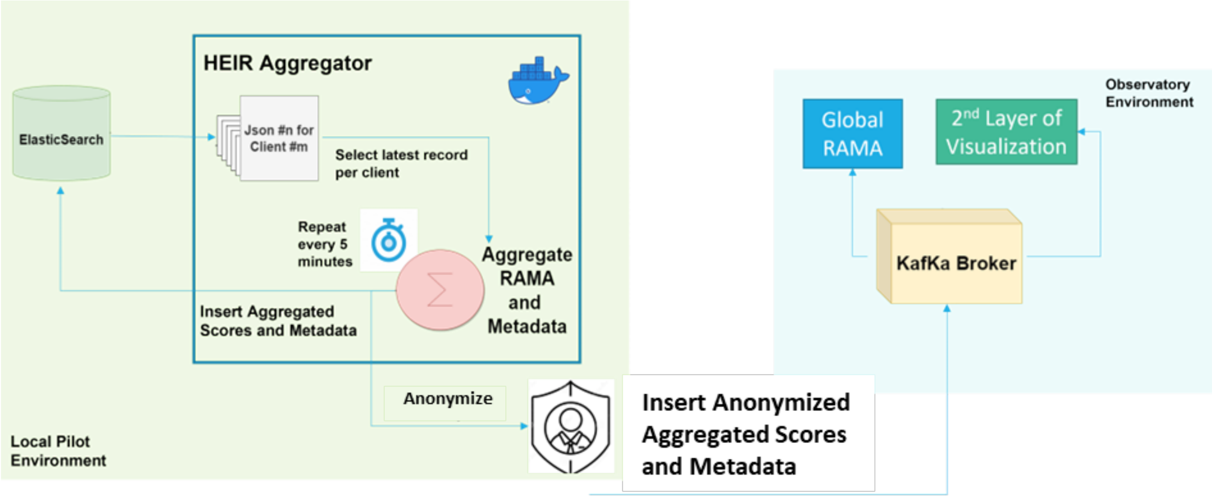

HEIR Aggregator
ElasticSearch
Json #n for Client #m
Select latest record per client
Repeat every 5 minutes
Aggregate RAMA and Metadata
Insert Aggregated Scores and Metadata
Anonymize
Insert Anonymized Aggregated Scores and Metadata
Local Pilot Environment
Observatory Environment
Global RAMA
2nd Layer of Visualization
KafKa Broker

Figure 14: HEIR Aggregator flow. The Aggregator produces locally aggregated (weighted by Department "severity) RAMA score and metadata (blue square). The Aggregator also generates the Global aggregated (no weights) and anonymized RAMA score and metadata and sends it to the Observatory(light blue box).

The HEIR Aggregator is the component that makes the liaison between the HEIR client and RAMA calculator on the one hand and the HEIR's 1st layer of services GUI, and the Observatory on the other. The HEIR Aggregator was initially conceived for medical institutions with multiple departments for which individual HEIR clients and RAMA calculators were deployed, with the Aggregator collecting and producing combined scored and metadata statistics.

Over the course of the project the purpose of the Aggregator has evolved into a connecting component that performs the transfer of detected activity at the local level by the HEIR Clients and the RAMA calculator to the HEIR local GUI and to the HEIR Observatory, and it is now deployed to all participant Pilots of the HEIR project, regardless of the number of departments they have.

In the Months 19-30 of the HEIR project, the HEIR Aggregator has been changed to illustrate the changes presented above (Sections 4 and 5) in the HEIR client and RAMA calculator, updating all the modified metadata and RAMA score information.

One of the main features of Aggregator v3 (25.01.2023) is that it now computes two versions of the Aggregated RAMA score:

1. **Locally** Aggregated RAMA Score (LARS) that follows the formula:

$$\textbf{LARS} = \frac{\sum_{i=1}^{n} \boldsymbol{LRS * S_i}}{\sum_{i=1}^{n} \boldsymbol{S_i}},$$

with **n** the number of HEIR clients deployed for the specific Health Institution, ***LRS*** described in Section 4, and $\boldsymbol{S_i}$ standing for the "**severity**" assigned to department ***i*** by the Health Institution IT experts.

The updated LARS is now present in the HEIR platform as a need to illustrate and reflect the different severity (priority) a hospital might give to a specific department included in the HEIR detection platform.

2. **Globally** Aggregated RAMA Score (GARS) to be sent to the **Observatory** with the anonymized associated metadata with the following formula:

$$\boldsymbol{GARS = 0.7 \ * \sum_i^n \mathbf{BaseScore}_i \ + \ 0.3 \ * \ \sum_i^n \mathbf{TemporalScore}_i,}$$

with i, associated to the departments where HEIR clients have been deployed.

The ***GARS*** no longer contains the severity components, in order to comply with anonymization rules, with no identifiable information on the local IT systems being transmitted to the Observatory.

7. Conclusions

Deliverable D3.3 has continued the work started in deliverables D3.1 and D3.2. Considerable progress was achieved in the months M19-M30 for the technical development of the components of WP3, i.e., HEIR client, RAMA calculator, RAMA Aggregator and the GUI for the 1st layer of services. The current status of the WP3 components make the final version of the complete 1st layer of HEIR services fully functional and in accordance with the HEIR project proposal and Grand Agreement.

All the components developed in WP3 have been successfully deployed and tested on the premises of all 4 participant pilots of the HEIR project, with the execution scenarios, user stories, and deployment procedures fully described in Deliverables 5.4 and 6.3.

8. Bibliography

Mihaila, O. V. (2022). *D3.2: The HEIR 1st layer of services package: 1st complete version.* Retrieved from Zenodo: https://zenodo.org/record/6389732

Zacharakis, A. L. (2021). *D3.1: The HEIR 1st layer of services package for the MVP*. Retrieved from Zenodo: https://doi.org/10.5281/zenodo.6389713

Grant Agreement number: 883275 — HEIR — H2020-SU-DS-2018-2019-2020 / H2020-SU-DS-2019. https://doi.org/10.3030/883275

9. Annex A - HEIR client sample JSON output

```
    {
        "clientId": 5,
        "client_name": "Some client",
        "hospitalId": 1,
        "hospital_address": "Street no 1",
        "hospital_region": "PAGNI",
        "hcc": [
            {
                "ssltest": {
                    "description": "",
                    "host": "10.104.14.22",
                    "sniname": "10.104.14.22",
                    "port": "2379",
                    "protocol": [
                        {
                            "type": "tls",
                            "version": "1.2",
                            "enabled": "1"
                        }
                    ],
                    "heartbleed": []
                },
                "triggered": true
            }
        ],
        "scan_id": "a06beae7-f742-3285-e74e83b6a7008a72",
        "connected_clients": 3,
        "vulnerabilityAssessment": [
            {
                "triggered": true,
                "events": [
                    {
                        "application_name": "Mozilla Firefox",
                        "cves": [
                            {
                                "cve": "CVE-2007-3670",
                                "description": "Argument injection vulnerability in Microsoft
Internet Explorer, when running on systems with Firefox installed and certain URIs registered,
allows remote attackers to conduct cross-browser scripting attacks and execute arbitrary commands
via shell metacharacters in a (1) FirefoxURL or (2) FirefoxHTML URI, which are inserted into the
command line that is created when invoking firefox.exe.  NOTE: it has been debated as to whether
the issue is in Internet Explorer or Firefox. As of 20070711, it is CVE's opinion that IE appears
to be failing to properly delimit the URL argument when invoking Firefox, and this issue could
arise with other protocol handlers in IE as well. However, Mozilla has stated that it will
address the issue with a \\\\\\\\\\\\\\\"defense in depth\\\\\\\\\\\\\\\" fix that will
\\\\\\\\\\\\\\\"prevent IE from sending Firefox malicious data.\\\\\\\\\\\\\\\"",
                                "publish_date": "2007-07-10T19:30Z",
                                "score": 42
                            },
                            {
                                "cve": "CVE-2011-0064",
                                "description": "The hb_buffer_ensure function in hb-buffer.c in
HarfBuzz, as used in Pango 1.28.3, Firefox, and other products, does not verify that memory
reallocations succeed, which allows remote attackers to cause a denial of service (NULL pointer
dereference and application crash) or possibly execute arbitrary code via crafted OpenType font
data that triggers use of an incorrect index.",
                                "publish_date": "2011-03-07T21:00Z",
                                "score": 67
                            },
                            {
                                "cve": "CVE-2011-3389",
                                "description": "The SSL protocol, as used in certain
configurations in Microsoft Windows and Microsoft Internet Explorer, Mozilla Firefox, Google
Chrome, Opera, and other products, encrypts data by using CBC mode with chained initialization
vectors, which allows man-in-the-middle attackers to obtain plaintext HTTP headers via a
blockwise chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with JavaScript code
```

```
that uses (1) the HTML5 WebSocket API, (2) the Java URLConnection API, or (3) the Silverlight
WebClient API, aka a \\\\\\\\\\\\\\\"BEAST\\\\\\\\\\\\\\\" attack.",
                                "publish_date": "2011-09-06T19:55Z",
                                "score": 42
                            },
                            {
                                "cve": "CVE-2015-4000",
                                "description": "The TLS protocol 1.2 and earlier, when a
DHE_EXPORT ciphersuite is enabled on a server but not on a client, does not properly convey a
DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks
by rewriting a ClientHello with DHE replaced by DHE_EXPORT and then rewriting a ServerHello with
DHE_EXPORT replaced by DHE, aka the \\\\\\\\\\\\\\\"Logjam\\\\\\\\\\\\\\\" issue.",
                                "publish_date": "2015-05-21T00:59Z",
                                "score": 42
                            },
                            {
                                "cve": "CVE-2021-23987",
                                "description": "Mozilla developers and community members reported
memory safety bugs present in Firefox 86 and Firefox ESR 78.8. Some of these bugs showed evidence
of memory corruption and we presume that with enough effort some of these could have been
exploited to run arbitrary code. This vulnerability affects Firefox ESR < 78.9, Firefox < 87, and
Thunderbird < 78.9.",
                                "publish_date": "2021-03-31T14:15Z",
                                "score": 67
                            },
                            {
                                "cve": "CVE-2021-23988",
                                "description": "Mozilla developers reported memory safety bugs
present in Firefox 86. Some of these bugs showed evidence of memory corruption and we presume
that with enough effort some of these could have been exploited to run arbitrary code. This
vulnerability affects Firefox < 87.",
                                "publish_date": "2021-03-31T14:15Z",
                                "score": 67
                            },
                            {
                                "cve": "CVE-2021-23984",
                                "description": "A malicious extension could have opened a popup
window lacking an address bar. The title of the popup lacking an address bar should not be fully
controllable, but in this situation was. This could have been used to spoof a website and attempt
to trick the user into providing credentials. This vulnerability affects Firefox ESR < 78.9,
Firefox < 87, and Thunderbird < 78.9.",
                                "publish_date": "2021-03-31T14:15Z",
                                "score": 42
                            },
                            {
                                "cve": "CVE-2021-23986",
                                "description": "A malicious extension with the 'search'
permission could have installed a new search engine whose favicon referenced a cross-origin URL.
The response to this cross-origin request could have been read by the extension, allowing a same-
origin policy bypass by the extension, which should not have cross-origin permissions. This
cross-origin request was made without cookies, so the sensitive information disclosed by the
violation was limited to local-network resources or resources that perform IP-based
authentication. This vulnerability affects Firefox < 87.",
                                "publish_date": "2021-03-31T14:15Z",
                                "score": 42
                            },
                            {
                                "cve": "CVE-2021-23981",
                                "description": "A texture upload of a Pixel Buffer Object could
have confused the WebGL code to skip binding the buffer used to unpack it, resulting in memory
corruption and a potentially exploitable information leak or crash. This vulnerability affects
Firefox ESR < 78.9, Firefox < 87, and Thunderbird < 78.9.",
                                "publish_date": "2021-03-31T14:15Z",
                                "score": 57
                            },
                            {
                                "cve": "CVE-2021-23982",
                                "description": "Using techniques that built on the slipstream
research, a malicious webpage could have scanned both an internal network's hosts as well as
```

```
services running on the user's local machine utilizing WebRTC connections. This vulnerability
affects Firefox ESR < 78.9, Firefox < 87, and Thunderbird < 78.9.",
                                "publish_date": "2021-03-31T14:15Z",
                                "score": 42
                            },
                            {
                                "cve": "CVE-2021-23983",
                                "description": "By causing a transition on a parent node by
removing a CSS rule, an invalid property for a marker could have been applied, resulting in
memory corruption and a potentially exploitable crash. This vulnerability affects Firefox < 87.",
                                "publish_date": "2021-03-31T14:15Z",
                                "score": 42
                            },
                            {
                                "cve": "CVE-2021-23985",
                                "description": "If an attacker is able to alter specific
about:config values (for example malware running on the user's computer), the Devtools remote
debugging feature could have been enabled in a way that was unnoticable to the user. This would
have allowed a remote attacker (able to make a direct network connection to the victim) to
monitor the user's browsing activity and (plaintext) network traffic. This was addressed by
providing a visual cue when Devtools has an open network socket. This vulnerability affects
Firefox < 87.",
                                "publish_date": "2021-03-31T14:15Z",
                                "score": 42
                            },
                            {
                                "cve": "CVE-2021-29968",
                                "description": "When drawing text onto a canvas with WebRender
disabled, an out of bounds read could occur. *This bug only affects Firefox on Windows. Other
operating systems are unaffected.*. This vulnerability affects Firefox < 89.0.1.",
                                "publish_date": "2021-06-24T14:15Z",
                                "score": 57
                            },
                            {
                                "cve": "CVE-2021-29967",
                                "description": "Mozilla developers reported memory safety bugs
present in Firefox 88 and Firefox ESR 78.11. Some of these bugs showed evidence of memory
corruption and we presume that with enough effort some of these could have been exploited to run
arbitrary code. This vulnerability affects Thunderbird < 78.11, Firefox < 89, and Firefox ESR <
78.11.",
                                "publish_date": "2021-06-24T14:15Z",
                                "score": 67
                            },
                            {
                                "cve": "CVE-2021-29966",
                                "description": "Mozilla developers reported memory safety bugs
present in Firefox 88. Some of these bugs showed evidence of memory corruption and we presume
that with enough effort some of these could have been exploited to run arbitrary code. This
vulnerability affects Firefox < 89.",
                                "publish_date": "2021-06-24T14:15Z",
                                "score": 67
                            },
                            {
                                "cve": "CVE-2021-29947",
                                "description": "Mozilla developers and community members reported
memory safety bugs present in Firefox 87. Some of these bugs showed evidence of memory corruption
and we presume that with enough effort some of these could have been exploited to run arbitrary
code. This vulnerability affects Firefox < 88.",
                                "publish_date": "2021-06-24T14:15Z",
                                "score": 67
                            },
                            {
                                "cve": "CVE-2021-29946",
                                "description": "Ports that were written as an integer overflow
above the bounds of a 16-bit integer could have bypassed port blocking restrictions when used in
the Alt-Svc header. This vulnerability affects Firefox ESR < 78.10, Thunderbird < 78.10, and
Firefox < 88.",
                                "publish_date": "2021-06-24T14:15Z",
                                "score": 67
                            },
                            {
                                "cve": "CVE-2021-29964",
                                "description": "A locally-installed hostile program could send
`WM_COPYDATA` messages that Firefox would process incorrectly, leading to an out-of-bounds read.
*This bug only affects Firefox on Windows. Other operating systems are unaffected.*. This
vulnerability affects Thunderbird < 78.11, Firefox < 89, and Firefox ESR < 78.11.",
                                "publish_date": "2021-06-24T14:15Z",
                                "score": 57
                            },
                            {
                                "cve": "CVE-2021-29961",
                                "description": "When styling and rendering an oversized
`<select>` element, Firefox did not apply correct clipping which allowed an attacker to paint
over the user interface. This vulnerability affects Firefox < 89.",
                                "publish_date": "2021-06-24T14:15Z",
                                "score": 42
                            },
                            {
                                "cve": "CVE-2021-29960",
                                "description": "Firefox used to cache the last filename used for
printing a file. When generating a filename for printing, Firefox usually suggests the web page
title. The caching and suggestion techniques combined may have lead to the title of a website
visited during private browsing mode being stored on disk. This vulnerability affects Firefox <
89.",
                                "publish_date": "2021-06-24T14:15Z",
                                "score": 42
                            },
                            {
                                "cve": "CVE-2021-29959",
                                "description": "When a user has already allowed a website to
access microphone and camera, disabling camera sharing would not fully prevent the website from
re-enabling it without an additional prompt. This was only possible if the website kept recording
with the microphone until re-enabling the camera. This vulnerability affects Firefox < 89.",
                                "publish_date": "2021-06-24T14:15Z",
                                "score": 42
                            },
                            {
                                "cve": "CVE-2021-29955",
                                "description": "A transient execution vulnerability, named
Floating Point Value Injection (FPVI) allowed an attacker to leak arbitrary memory addresses and
may have also enabled JIT type confusion attacks. (A related vulnerability, Speculative Code
Store Bypass (SCSB), did not affect Firefox.). This vulnerability affects Firefox ESR < 78.9 and
Firefox < 87.",
                                "publish_date": "2021-06-24T14:15Z",
                                "score": 26
                            },
                            {
                                "cve": "CVE-2021-29951",
                                "description": "The Mozilla Maintenance Service granted
SERVICE_START access to BUILTIN|Users which, in a domain network, grants normal remote users
access to start or stop the service. This could be used to prevent the browser update service
from operating (if an attacker spammed the 'Stop' command); but also exposed attack surface in
the maintenance service. *Note: This issue only affected Windows operating systems older than Win
10 build 1709. Other operating systems are unaffected.*. This vulnerability affects Thunderbird <
78.10.1, Firefox < 87, and Firefox ESR < 78.10.1.",
                                "publish_date": "2021-06-24T14:15Z",
                                "score": 64
                            },
                            {
                                "cve": "CVE-2021-29944",
                                "description": "Lack of escaping allowed HTML injection when a
webpage was viewed in Reader View. While a Content Security Policy prevents direct code
execution, HTML injection is still possible. *Note: This issue only affected Firefox for Android.
Other operating systems are unaffected.*. This vulnerability affects Firefox < 88.",
                                "publish_date": "2021-06-24T14:15Z",
                                "score": 42
                            },
                            {
                                "cve": "CVE-2021-24002",
                                "description": "When a user clicked on an FTP URL containing
encoded newline characters (%0A and %0D), the newlines would have been interpreted as such and
allowed arbitrary commands to be sent to the FTP server. This vulnerability affects Firefox ESR <
78.10, Thunderbird < 78.10, and Firefox < 88.",
                                "publish_date": "2021-06-24T14:15Z",
                                "score": 67
                            },
                            {
                                "cve": "CVE-2021-24001",
                                "description": "A compromised content process could have
performed session history manipulations it should not have been able to due to testing
infrastructure that was not restricted to testing-only configurations. This vulnerability affects
Firefox < 88.",
                                "publish_date": "2021-06-24T14:15Z",
                                "score": 42
                            },
                            {
                                "cve": "CVE-2021-24000",
                                "description": "A race condition with requestPointerLock() and
setTimeout() could have resulted in a user interacting with one tab when they believed they were
on a separate tab. In conjunction with certain elements (such as &lt;input
type=\\\\\\\\\\\\\\\"file\\\\\\\\\\\\\\\"&gt;) this could have led to an attack where a user was
confused about the origin of the webpage and potentially disclosed information they did not
intend to. This vulnerability affects Firefox < 88.",
                                "publish_date": "2021-06-24T14:15Z",
                                "score": 26
                            },
                            {
                                "cve": "CVE-2021-23999",
                                "description": "If a Blob URL was loaded through some unusual
user interaction, it could have been loaded by the System Principal and granted additional
privileges that should not be granted to web content. This vulnerability affects Firefox ESR <
78.10, Thunderbird < 78.10, and Firefox < 88.",
                                "publish_date": "2021-06-24T14:15Z",
                                "score": 67
                            },
                            {
                                "cve": "CVE-2021-23998",
                                "description": "Through complicated navigations with new windows,
an HTTP page could have inherited a secure lock icon from an HTTPS page. This vulnerability
affects Firefox ESR < 78.10, Thunderbird < 78.10, and Firefox < 88.",
                                "publish_date": "2021-06-24T14:15Z",
                                "score": 42
                            },
                            {
                                "cve": "CVE-2021-23996",
                                "description": "By utilizing 3D CSS in conjunction with
Javascript, content could have been rendered outside the webpage's viewport, resulting in a
spoofing attack that could have been used for phishing or other attacks on a user. This
vulnerability affects Firefox < 88.",
                                "publish_date": "2021-06-24T14:15Z",
                                "score": 42
                            },
                            {
                                "cve": "CVE-2021-23997",
                                "description": "Due to unexpected data type conversions, a use-
after-free could have occurred when interacting with the font cache. We presume that with enough
effort this could have been exploited to run arbitrary code. This vulnerability affects Firefox <
88.",
                                "publish_date": "2021-06-24T14:15Z",
                                "score": 67
                            },
                            {
                                "cve": "CVE-2021-23995",
                                "description": "When Responsive Design Mode was enabled, it used
references to objects that were previously freed. We presume that with enough effort this could
have been exploited to run arbitrary code. This vulnerability affects Firefox ESR < 78.10,
Thunderbird < 78.10, and Firefox < 88.",
                                "publish_date": "2021-06-24T14:15Z",
                                "score": 50
                            },
                            {
                                "cve": "CVE-2021-23994",
                                "description": "A WebGL framebuffer was not initialized early
enough, resulting in memory corruption and an out of bound write. This vulnerability affects
Firefox ESR < 78.10, Thunderbird < 78.10, and Firefox < 88.",
                                "publish_date": "2021-06-24T14:15Z",
                                "score": 67
                            },
                            {
                                "cve": "CVE-2021-29989",
                                "description": "Mozilla developers reported memory safety bugs
present in Firefox 90 and Firefox ESR 78.12. Some of these bugs showed evidence of memory
corruption and we presume that with enough effort some of these could have been exploited to run
arbitrary code. This vulnerability affects Thunderbird < 78.13, Firefox ESR < 78.13, and Firefox
< 91.",
                                "publish_date": "2021-08-17T20:15Z",
                                "score": 67
                            },
                            {
                                "cve": "CVE-2021-29988",
                                "description": "Firefox incorrectly treated an inline list-item
element as a block element, resulting in an out of bounds read or memory corruption, and a
potentially exploitable crash. This vulnerability affects Thunderbird < 78.13, Thunderbird < 91,
Firefox ESR < 78.13, and Firefox < 91.",
                                "publish_date": "2021-08-17T20:15Z",
                                "score": 67
                            },
                            {
                                "cve": "CVE-2021-29987",
                                "description": "After requesting multiple permissions, and
closing the first permission panel, subsequent permission panels will be displayed in a different
position but still record a click in the default location, making it possible to trick a user
into accepting a permission they did not want to. *This bug only affects Firefox on Linux. Other
operating systems are unaffected.*. This vulnerability affects Firefox < 91 and Thunderbird <
91.",
                                "publish_date": "2021-08-17T20:15Z",
                                "score": 42
                            },
                            {
                                "cve": "CVE-2021-29986",
                                "description": "A suspected race condition when calling
getaddrinfo led to memory corruption and a potentially exploitable crash. *Note: This issue only
affected Linux operating systems. Other operating systems are unaffected.* This vulnerability
affects Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91.",
                                "publish_date": "2021-08-17T20:15Z",
                                "score": 67
                            },
                            {
                                "cve": "CVE-2021-29985",
                                "description": "A use-after-free vulnerability in media channels
could have led to memory corruption and a potentially exploitable crash. This vulnerability
affects Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91.",
                                "publish_date": "2021-08-17T20:15Z",
                                "score": 67
                            },
                            {
                                "cve": "CVE-2021-29984",
                                "description": "Instruction reordering resulted in a sequence of
instructions that would cause an object to be incorrectly considered during garbage collection.
This led to memory corruption and a potentially exploitable crash. This vulnerability affects
Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91.",
                                "publish_date": "2021-08-17T20:15Z",
                                "score": 67
                            },
                            {
                                "cve": "CVE-2021-29983",
                                "description": "Firefox for Android could get stuck in fullscreen
mode and not exit it even after normal interactions that should cause it to exit. *Note: This
```

```
issue only affected Firefox for Android. Other operating systems are unaffected.*. This
vulnerability affects Firefox < 91.",
                                "publish_date": "2021-08-17T20:15Z",
                                "score": 42
                            },
                            {
                                "cve": "CVE-2021-29982",
                                "description": "Due to incorrect JIT optimization, we incorrectly
interpreted data from the wrong type of object, resulting in the potential leak of a single bit
of memory. This vulnerability affects Firefox < 91 and Thunderbird < 91.",
                                "publish_date": "2021-08-17T20:15Z",
                                "score": 42
                            },
                            {
                                "cve": "CVE-2021-29981",
                                "description": "An issue present in lowering/register allocation
could have led to obscure but deterministic register confusion failures in JITted code that would
lead to a potentially exploitable crash. This vulnerability affects Firefox < 91 and Thunderbird
< 91.",
                                "publish_date": "2021-08-17T20:15Z",
                                "score": 67
                            },
                            {
                                "cve": "CVE-2021-29980",
                                "description": "Uninitialized memory in a canvas object could
have caused an incorrect free() leading to memory corruption and a potentially exploitable crash.
This vulnerability affects Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and
Firefox < 91.",
                                "publish_date": "2021-08-17T20:15Z",
                                "score": 67
                            },
                            {
                                "cve": "CVE-2021-29990",
                                "description": "Mozilla developers and community members reported
memory safety bugs present in Firefox 90. Some of these bugs showed evidence of memory corruption
and we presume that with enough effort some of these could have been exploited to run arbitrary
code. This vulnerability affects Firefox < 91.",
                                "publish_date": "2021-08-17T20:15Z",
                                "score": 67
                            },
                            {
                                "cve": "CVE-2021-38501",
                                "description": "Mozilla developers reported memory safety bugs
present in Firefox 92 and Firefox ESR 91.1. Some of these bugs showed evidence of memory
corruption and we presume that with enough effort some of these could have been exploited to run
arbitrary code. This vulnerability affects Firefox < 93, Thunderbird < 91.2, and Firefox ESR <
91.2.",
                                "publish_date": "2021-11-03T01:15Z",
                                "score": 67
                            },
                            {
                                "cve": "CVE-2021-38500",
                                "description": "Mozilla developers reported memory safety bugs
present in Firefox 92 and Firefox ESR 91.1. Some of these bugs showed evidence of memory
corruption and we presume that with enough effort some of these could have been exploited to run
arbitrary code. This vulnerability affects Thunderbird < 78.15, Thunderbird < 91.2, Firefox ESR <
91.2, Firefox ESR < 78.15, and Firefox < 93.",
                                "publish_date": "2021-11-03T01:15Z",
                                "score": 67
                            },
                            {
                                "cve": "CVE-2021-38499",
                                "description": "Mozilla developers reported memory safety bugs
present in Firefox 92. Some of these bugs showed evidence of memory corruption and we presume
that with enough effort some of these could have been exploited to run arbitrary code. This
vulnerability affects Firefox < 93.",
                                "publish_date": "2021-11-03T01:15Z",
                                "score": 67
                            },
                            {
                                "cve": "CVE-2021-38498",
                                "description": "During process shutdown, a document could have
caused a use-after-free of a languages service object, leading to memory corruption and a
potentially exploitable crash. This vulnerability affects Firefox < 93, Thunderbird < 91.2, and
Firefox ESR < 91.2.",
                                "publish_date": "2021-11-03T01:15Z",
                                "score": 50
                            },
                            {
                                "cve": "CVE-2021-38497",
                                "description": "Through use of reportValidity() and
window.open(), a plain-text validation message could have been overlaid on another origin,
leading to possible user confusion and spoofing attacks. This vulnerability affects Firefox < 93,
Thunderbird < 91.2, and Firefox ESR < 91.2.",
                                "publish_date": "2021-11-03T01:15Z",
                                "score": 42
                            },
                            {
                                "cve": "CVE-2021-38494",
                                "description": "Mozilla developers reported memory safety bugs
present in Firefox 91. Some of these bugs showed evidence of memory corruption and we presume
that with enough effort some of these could have been exploited to run arbitrary code. This
vulnerability affects Firefox < 92.",
                                "publish_date": "2021-11-03T01:15Z",
                                "score": 67
                            },
                            {
                                "cve": "CVE-2021-38493",
                                "description": "Mozilla developers reported memory safety bugs
present in Firefox 91 and Firefox ESR 78.13. Some of these bugs showed evidence of memory
corruption and we presume that with enough effort some of these could have been exploited to run
arbitrary code. This vulnerability affects Firefox ESR < 78.14, Thunderbird < 78.14, and Firefox
< 92.",
                                "publish_date": "2021-11-03T01:15Z",
                                "score": 67
                            },
                            {
                                "cve": "CVE-2021-38492",
                                "description": "When delegating navigations to the operating
system, Firefox would accept the `mk` scheme which might allow attackers to launch pages and
execute scripts in Internet Explorer in unprivileged mode. *This bug only affects Firefox for
Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox < 92,
Thunderbird < 91.1, Thunderbird < 78.14, Firefox ESR < 78.14, and Firefox ESR < 91.1.",
                                "publish_date": "2021-11-03T01:15Z",
                                "score": 42
                            },
                            {
                                "cve": "CVE-2021-38491",
                                "description": "Mixed-content checks were unable to analyze
opaque origins which led to some mixed content being loaded. This vulnerability affects Firefox <
92.",
                                "publish_date": "2021-11-03T01:15Z",
                                "score": 42
                            },
                            {
                                "cve": "CVE-2021-29991",
                                "description": "Firefox incorrectly accepted a newline in a
HTTP/3 header, interpretting it as two separate headers. This allowed for a header splitting
attack against servers using HTTP/3. This vulnerability affects Firefox < 91.0.1 and Thunderbird
< 91.0.1.",
                                "publish_date": "2021-11-03T01:15Z",
                                "score": 57
                            },
                            {
                                "cve": "CVE-2021-38496",
                                "description": "During operations on MessageTasks, a task may
have been removed while it was still scheduled, resulting in memory corruption and a potentially
exploitable crash. This vulnerability affects Thunderbird < 78.15, Thunderbird < 91.2, Firefox
ESR < 91.2, Firefox ESR < 78.15, and Firefox < 93.",
                                "publish_date": "2021-11-03T01:15Z",
                                "score": 67
                            }
                        ],
                        "version": "85.0.1"
                    }
                ]
            }
        ],
        "het": [
            {
                "triggered": true,
                "events": [
                    {
                        "availability": "None",
                        "confidentiality": "None",
                        "description": "Verifies the local group policy settings for User
Configuration\\Administrative Templates\\System\\Ctrl+Alt+Del Options\\Remove Task Manager. When
Remove Task Manager is enabled, the endpoint is vulnerable to security threats. Since Task
Manager can list and terminate currently running processes, some malware may disable it to
prevent themselves from being closed.",
                        "integrity": "High",
                        "name": "Task Manager",
                        "score": 25,
                        "triggered": true,
                        "type": "MisConfiguration"
                    },
                    {
                        "availability": "None",
                        "confidentiality": "Medium",
                        "description": "Verifies if Windows requires account sign-in. When the
user accounts sign-in is disabled, Windows stores the user passwords in the registry database,
making possible to bypass the password screen during logon.",
                        "integrity": "None",
                        "name": "Auto Logon",
                        "score": 25,
                        "triggered": false,
                        "type": "MisConfiguration"
                    },
                    {
                        "availability": "None",
                        "confidentiality": "Low",
                        "description": "Verifies the local security policy option User Account
Control: Run all administrators in Admin Approval Mode. This setting controls the behavior of all
UAC policy settings for the endpoint. UAC (User Account Control) is a security feature that helps
preventing unauthorized changes to the OS by potentially harmful programs. UAC requires
administrator authorization for actions like installing a program or modifying system settings.
When UAC is set to Never notify, the system is more vulnerable to malware.",
                        "integrity": "Low",
                        "name": "UAC Off",
                        "score": 50,
                        "triggered": false,
                        "type": "MisConfiguration"
                    },
                    {
                        "availability": "None",
                        "confidentiality": "Low",
                        "description": "Verifies the configuration for User Account Control
policy and registry settings, to check if these comply with the default recommended settings. The
policy settings are located in Security Settings\\Local Policies\\Security Options, in the Local
Security Policy app.",
                        "integrity": "Low",
                        "name": "UAC Insecure",
                        "score": 30,
                        "triggered": true,
                        "type": "MisConfiguration"
                    },
                    {
                        "availability": "None",
                        "confidentiality": "None",
                        "description": "Verifies the local group policy Turn off Data Execution
Prevention for Explorer, located in Computer Configuration\\Administrative Templates\\Windows
Components\\File Explorer. Disabling data execution prevention can allow certain legacy plug-in
applications to function without terminating Explorer.",
                        "integrity": "Low",
                        "name": "Explorer Data Execution Prevention",
                        "score": 50,
                        "triggered": false,
                        "type": "MisConfiguration"
                    },
                    {
                        "availability": "None",
                        "confidentiality": "None",
                        "description": "Verifies the local group policy Turn off heap termination
on corruption, located in Computer Configuration\\Administrative Templates\\Windows
Components\\File Explorer. Disabling heap termination on corruption can allow certain legacy
plug-in applications to function without terminating Explorer immediately, although Explorer may
still terminate unexpectedly later.",
                        "integrity": "Low",
                        "name": "Heap Termination on Corruption",
                        "score": 50,
                        "triggered": false,
                        "type": "MisConfiguration"
                    },
                    {
                        "availability": "None",
                        "confidentiality": "Medium",
                        "description": "Verifies the local group policy Do not allow passwords to
be saved, located in Computer Configuration\\Administrative Templates\\Windows Components\\Remote
Desktop Services\\Remote Desktop Connection Client. This policy controls whether passwords can be
saved on this computer from Remote Desktop Connection.  - If you enable this setting, the
password saving checkbox in Remote Desktop Connection will be disabled and users will no longer
be able to save passwords. When a user opens an RDP file using Remote Desktop Connection and
saves his settings, any password that previously existed in the RDP file will be deleted.",
                        "integrity": "Low",
                        "name": "Save Passwords from RDP",
                        "score": 50,
                        "triggered": false,
                        "type": "MisConfiguration"
                    },
                    {
                        "availability": "None",
                        "confidentiality": "Medium",
                        "description": "Verifies the local group policy Do not allow drive
redirection, located in Computer Configuration\\Administrative Templates\\Windows
Components\\Remote Desktop Services\\Remote Desktop Session Host\\Device and Resource
Redirection. This policy setting specifies whether to prevent the mapping of client drives in a
Remote Desktop Services session (drive redirection). By default, an RD Session Host server maps
client drives automatically upon connection. Mapped drives appear in the session folder tree in
File Explorer or Computer in the format &lt;driveletter&gt; on &lt;computername&gt;. You can use
this policy setting to override this behavior.  - If you enable this policy setting, client drive
redirection is not allowed in Remote Desktop Services sessions, and Clipboard file copy
redirection is not allowed on computers running Windows Server 2003, Windows 8, and Windows XP.",
                        "integrity": "Low",
                        "name": "Drive Redirection",
                        "score": 50,
                        "triggered": true,
                        "type": "MisConfiguration"
                    },
                    {
                        "availability": "None",
                        "confidentiality": "None",
                        "description": "Checks the Macro settings for Office Word 16, located in
File\\Options\\Trust Center\\Trust Center Settings\\Macro Settings. Disable all macros without
notification - Macros and security alerts about macros are disabled. Disable all macros with
notification - Macros are disabled, but security alerts will be triggered if macros are present.
Disable all macros except digitally signed macros - Macros are disabled, but security alerts will
be triggered if macros are present. However, for macros digitally signed by a trusted publisher,
these will run if the trust access for that publisher has been enabled. Enable all macros (not
recommended, potentially dangerous code can run) - All macros run. This setting makes your
```

```
computer vulnerable to potentially malicious code. Trust access to the VBA project object
model.",
                        "integrity": "Medium",
                        "name": "Office Word 16 Macro",
                        "score": 55,
                        "triggered": false,
                        "type": "MisConfiguration"
                    },
                    {
                        "availability": "None",
                        "confidentiality": "None",
                        "description": "Checks the Macro settings for Office Excel 16, located in
File\\Options\\Trust Center\\Trust Center Settings\\Macro Settings. Disable all macros without
notification - Macros and security alerts about macros are disabled. Disable all macros with
notification - Macros are disabled, but security alerts will be triggered if macros are present.
Disable all macros except digitally signed macros - Macros are disabled, but security alerts will
be triggered if macros are present. However, for macros digitally signed by a trusted publisher,
these will run if the trust access for that publisher has been enabled. Enable all macros (not
recommended, potentially dangerous code can run) - All macros run. This setting makes your
computer vulnerable to potentially malicious code. Trust access to the VBA project object
model.",
                        "integrity": "Medium",
                        "name": "Office Excel 16 Macro",
                        "score": 55,
                        "triggered": false,
                        "type": "MisConfiguration"
                    },
                    {
                        "availability": "None",
                        "confidentiality": "Medium",
                        "description": "Checks the Macro settings for Office Outlook 16, located
in File\\Options\\Trust Center\\Trust Center Settings\\Macro Settings. Disable all macros without
notification - Macros and security alerts about macros are disabled. Disable all macros with
notification - Macros are disabled, but security alerts will be triggered if macros are present.
Disable all macros except digitally signed macros - Macros are disabled, but security alerts will
be triggered if macros are present. However, for macros digitally signed by a trusted publisher,
these will run if the trust access for that publisher has been enabled. Enable all macros (not
recommended, potentially dangerous code can run) - All macros run. This setting makes your
computer vulnerable to potentially malicious code. Trust access to the VBA project object
model.",
                        "integrity": "Medium",
                        "name": "Office Outlook 16 Macro",
                        "score": 55,
                        "triggered": false,
                        "type": "MisConfiguration"
                    },
                    {
                        "availability": "None",
                        "confidentiality": "Low",
                        "description": "Checks the number of local administrators on the
machine.",
                        "integrity": "None",
                        "name": "Too many local administrators",
                        "score": 40,
                        "triggered": false,
                        "type": "MisConfiguration"
                    },
                    {
                        "availability": "None",
                        "confidentiality": "High",
                        "description": "Checks the existence of shared folders with read access
for the Everyone group. The Everyone group includes all users who have logged in with a password
(members of the Authenticated Users group) as well as built-in, non-password protected accounts
such as Guest, and several other built-in security accounts like SERVICE, LOCAL_SERVICE,
NETWORK_SERVICE, and others. A Guest account is a built-in account on a Windows system that is
disabled by default.  - If enabled, it allows anyone to login without a password.",
                        "integrity": "None",
                        "name": "SMB Shared Everyone Read",
                        "score": 20,
                        "triggered": true,
                        "type": "MisConfiguration"
                    },
                    {
                        "availability": "None",
                        "confidentiality": "None",
                        "description": "Checks the existence of shared folders with write access
for the Everyone group. The Everyone group includes all users who have logged in with a password
(members of the Authenticated Users group) as well as built-in, non-password protected accounts
such as Guest, and several other built-in security accounts like SERVICE, LOCAL_SERVICE,
NETWORK_SERVICE, and others. A Guest account is a built-in account on a Windows system that is
disabled by default.  - If enabled, it allows anyone to login without a password.",
                        "integrity": "Medium",
                        "name": "SMB Shared Everyone Write",
                        "score": 25,
                        "triggered": false,
                        "type": "MisConfiguration"
                    },
                    {
                        "availability": "None",
                        "confidentiality": "High",
                        "description": "Verifies if regular users are allowed to read the
Security Account Manager (SAM) data. Non-admin users should not be allowed to read critical
files, but a vulnerability (known as HiveNightmare or SeriousSam) has been discovered in Windows
11 and Windows 10 version 1809 and above, which involved a \"bad\" ACL being set on the
%SystemRoot%\\System32\\Config folder, making it possible for regular users to acces the SAM,
SYSTEM, SECURITY and other critical files.",
                        "integrity": "Medium",
                        "name": "SAM File readable by users",
                        "score": 80,
                        "triggered": false,
                        "type": "Vulnerability"
                    }
                ]
            }
        ],
        "host_name": "HEIR-WIN10-2",
        "host_os": "Windows 10",
        "machine_id":
"0102CC3601029F9E0102DE280102BB9F010280F30102E8B30102D9B8010280570102CF370102C0FB0102AA4A0102A1AA
0102B6E20102EA600102C9D00102B962",
        "scan_status": "finished",
        "hnm": [
            {
                "triggered": true,
                "events": [
                    {
                        "DestinationMAC": "00:0c:29:68:24:5a",
                        "DestinationPort": 50975,
                        "AlertType": "ATTACK",
                        "GMID": "984a2797-190b-4d28-a5b8-d97597a5bb11",
                        "Description": "Network Probe has prevented a suspicious DNS request to a
public server that could contain private data. This is a potential data exfiltration marker. Data
exfiltration is a form of a security breach that occurs when an individual's or company's data is
copied, transferred, or retrieved from a computer or server without authorization.",
                        "DestinationIp": "192.168.198.204",
                        "SourceIp": "192.168.198.203",
                        "event_name": "detection",
                        "AlertName": "Exploit.DNS.ExfiltrationQuery",
                        "TimeCreated": 1637750665615,
                        "SourceMAC": "00:0c:29:a3:01:b7",
                        "SourcePort": 445
                    },
                    {
                        "DestinationMAC": "00:50:56:b7:57:4f",
                        "DestinationPort": 49671,
                        "AlertType": "ATTACK",
                        "Description": "Network probe has detected a request to a suspicious DNS
domain.",
                        "DestinationIp": "10.18.139.78",
                        "SourceIp": "10.18.139.58",
                        "event_name": "alert",
                        "AlertName": "Alert.DNS.DGA.SuspiciousDomain",
                        "TimeCreated": 1637750665616,
                        "SourceMAC": "00:50:56:b7:5e:a9",
                        "SourcePort": 35168
                    },
                    {
                        "DestinationMAC": "00:50:56:b7:57:4f",
                        "DestinationPort": 222,
                        "AlertType": "ATTACK",
                        "Description": "Network probe has detected a request to a suspicious DNS
domain.",
                        "DestinationIp": "10.18.139.78",
                        "SourceIp": "10.18.139.58",
                        "event_name": "alert",
                        "AlertName": "Alert.DNS.DGA.SuspiciousDomain",
                        "TimeCreated": 1637750665616,
                        "SourceMAC": "00:50:56:b7:5e:a9",
                        "SourcePort": 35168
                    }
                ]
            }
        ],
        "tdm": [
            {
                "triggered": false,
                "events": [
                    {
                        "ScannedObject": "C:/test/samples.",
                        "ObjectType": "File",
                        "AlertType": "Malware",
                        "event_name": "detection",
                        "AlertName": "Trojan.NG.Test.1",
                        "TimeCreated": 1670944872
                    }
                ]
            }
        ],
        "siem": [
            {
                "triggered": true,
                "events": [
                    {
                        "description": "Windows Defender: ERROR: BAD INPUT DATA",
                        "severity": "12",
                        "timestamp": "1671191952"
                    },
                    {
                        "description": "Windows Defender: ERROR: BAD CONFIGURATION",
                        "severity": "12",
                        "timestamp": "1671191952"
                    }
                ]
            }
        ],
        "received": null,
        "facilitators": null,
        "severity": 60}
```

10. Annex B – Local RAMA Score Calculator sample JSON output

```
{
    "temporalScore": {
        "temporalScore": 5.1,
        "hnmScore": 24,
        "siemScore": 10
    },
    "metadata": {
        "severity": 80,
        "hospital_region": "Hospital A from region B",
        "numberOfCriticalEvents": 0,
        "clientId": 4,
        "connected_clients": "1",
        "machine_id":
"3119BFD93119E3AB3119D0123119960B3119B2ED3119FDE63119DF543119C5BB3119FC35311994B33119DB3C3119D9C2
3119A1363119BCC73119BDB63119F25A",
        "hetMetadata": {
            "numberOfMaliciousFindings": 4,
            "percentageOfBenignFindings": 73.33333333333333,
            "noOfOSVulnerabilities": 1,
            "percentageOfMaliciousFindings": 26.666666666666668,
            "id": 0,
            "noOfMisconfigurations": 14,
            "numberOfBenignFindings": 11,
            "hetVector": "C:L/I:L/A:N"
        },
        "indicators": {
            "vaScore": 100,
            "hnmScore": 24,
            "hetScore": 28.55,
            "hccScore": 0,
            "siemScore": 10
        },
        "siemMetadata": {
            "lastTriggered": "2023-01-10 11:33:10.53",
            "numberOfMediumEvents": 0,
            "numberOfCriticalEvents": 0,
            "numberOfHighEvents": 2,
            "numberOfLowEvents": 0,
            "id": 0,
            "totalNumberOfEvents": 2
        },
        "vulnerabilityAssessmentAggregatedMetadata": {
            "top10MostFrequentVulnerabilities": {
                "CVE-2011-0064": 3,
                "CVE-2021-38497": 3,
                "CVE-2021-29985": 3,
                "CVE-2011-3389": 3,
                "CVE-2007-3670": 3,
                "CVE-2021-29984": 3,
                "CVE-2015-4000": 3,
                "CVE-2021-23981": 3,
                "CVE-2021-29967": 3,
                "CVE-2021-29966": 3
            },
            "id": 0,
            "vulnerabilityAssessmentMetadata": [{
                "application_name": "Mozilla Firefox 85.0.1",
                "noOfVulnerabilities": 55,
                "vulnerabilities": [
                    "CVE-2011-3389",
                    "CVE-2007-3670",
                    "CVE-2011-0064",
                    "CVE-2015-4000",
                    "CVE-2021-29984",
                    "CVE-2021-38497",
                    "CVE-2021-29985",
                    "CVE-2021-29967",
                    "CVE-2021-29966",
                    "CVE-2021-23981",
                    "CVE-2021-29964",
                    "CVE-2021-23996",
                    "CVE-2021-23985",
                    "CVE-2021-29980",
                    "CVE-2021-29987",
                    "CVE-2021-38498",
                    "CVE-2021-38493",
                    "CVE-2021-29982",
                    "CVE-2021-23999",
                    "CVE-2021-29983",
                    "CVE-2021-23983",
                    "CVE-2021-23998",
                    "CVE-2021-29960",
                    "CVE-2021-23997",
                    "CVE-2021-29990",
                    "CVE-2021-29944",
                    "CVE-2021-38491",
                    "CVE-2021-23986",
                    "CVE-2021-29986",
                    "CVE-2021-29951",
                    "CVE-2021-38501",
                    "CVE-2021-29991",
                    "CVE-2021-29946",
                    "CVE-2021-24000",
                    "CVE-2021-29989",
                    "CVE-2021-23987",
                    "CVE-2021-24002",
                    "CVE-2021-24001",
                    "CVE-2021-38494",
                    "CVE-2021-29947",
                    "CVE-2021-29955",
                    "CVE-2021-29988",
                    "CVE-2021-38499",
                    "CVE-2021-29959",
                    "CVE-2021-29961",
                    "CVE-2021-29981",
                    "CVE-2021-38496",
                    "CVE-2021-38500",
                    "CVE-2021-23995",
                    "CVE-2021-23988",
                    "CVE-2021-29968",
                    "CVE-2021-23982",
                    "CVE-2021-38492",
                    "CVE-2021-23984",
                    "CVE-2021-23994"
                ],
                "id": 0
            }],
            "totalNoOfVulnerabilities": 55,
            "top10Vulnerabilities": {
                "CVE-2021-23997": 67,
                "CVE-2021-23999": 67,
                "CVE-2021-38493": 67,
                "CVE-2021-29980": 67,
                "CVE-2021-29990": 67,
                "CVE-2011-0064": 67,
                "CVE-2021-29985": 67,
                "CVE-2021-29984": 67,
                "CVE-2021-29967": 67,
                "CVE-2021-29966": 67
            }
        },
        "hnmMetadata": {
            "numberOfExploits": 0,
            "hnmMetadata": [
                {
                    "destinationPort": 49671,
                    "destinationIp": "[removed]",
                    "sourcePort": 35168,
                    "sourceIp": "[removed]",
                    "description": "Network probe has detected a request to a suspicious DNS
domain.",
                    "id": 0
                },
                {
                    "destinationPort": 222,
                    "destinationIp": "[removed]",
                    "sourcePort": 35168,
                    "sourceIp": "10.18.139.58",
                    "description": "Network probe has detected a request to a suspicious DNS
domain.",
                    "id": 0
                },
                {
                    "destinationPort": 50975,
                    "destinationIp": "[removed]",
                    "sourcePort": 445,
                    "sourceIp": "[removed]”
                    "description": "Network Probe has prevented a suspicious DNS request to a
public server that could contain private data. This is a potential data exfiltration marker. Data
exfiltration is a form of a security breach that occurs when an individual's or company's data is
copied, transferred, or retrieved from a computer or server without authorization.",
                    "id": 0
                }
            ],
            "numberOfAttacks": 3,
            "id": 0,
            "totalHNMFindings": 1
        },
        "hospitalId": 5678,
        "hccMetadata": {
            "identifiedHeartbleeds": [],
            "numberOfIdentifiedHeartbleeds": 0,
            "id": 0
        },
        "hospital_address": "Street no 1",
        "host_name": "X-L2"
    },
    "clientId": [removed],
    "hospitalId": [removed],
    "ramaScore": 64.905,
    "created": "2023-01-09 11:32:17.286",
    "clientStatus": "Medium",
    "baseScore": {
        "vulnerabilityAssessmentScore": 100,
        "hetScore": 28.55,
        "hccScore": 0,
        "baseScore": 29.994999
    },
    "updated": "2023-01-09 11:32:28.714"
}
```

11. Annex C - HEIR Aggregator sample Json outputs

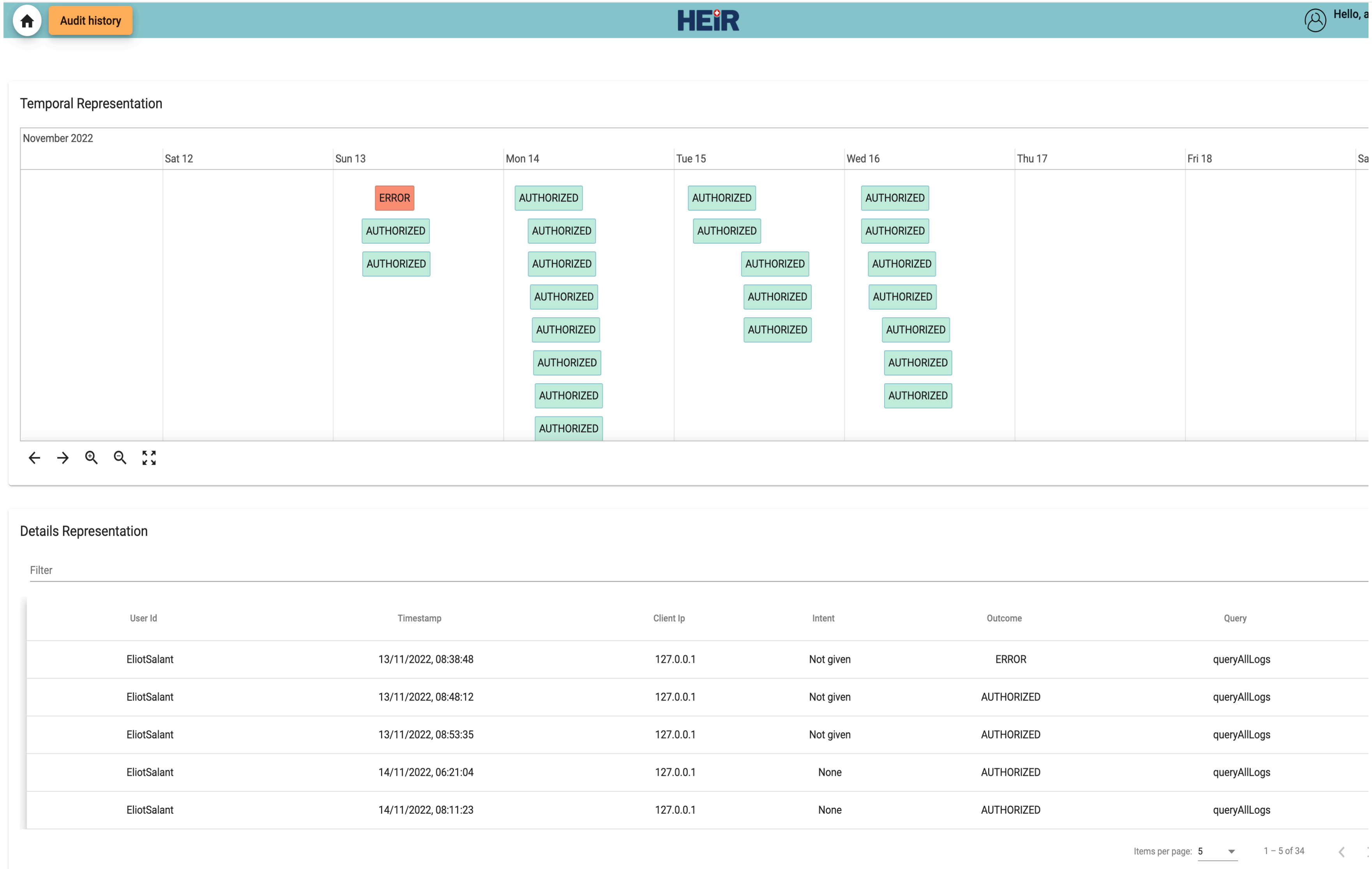
11.1 HEIR Aggregator JSON sent to HEIR's 1st Layer of services GUI

```
{
    "hospitalId": 3212,
    "clientIdList":
    [
        1
    ],
    "noOfClients": 1,
    "globalTemporalScore": 5.1,
    "hnmScore": 24.0,
    "siemScore": 10.0,
    "globalBaseScore": 29.994999,
    "vulnerabilityAssessmentScore": 100.0,
    "hccScore": 0.0,
    "hetScore": 28.55,
    "numberOfCriticalEvents": 0,
    "numberOfIdentifiedHeartbleeds": 0,
    "noOfOSVulnerabilities": 1,
    "noOfMisconfigurations": 14,
    "numberOfBenignFindings": 11,
    "numberOfMaliciousFindings": 4,
    "percentageOfBenignFindings": 73.33333333333333,
    "percentageOfMaliciousFindings": 26.666666666666668,
    "noOfAppVulnerabilities": 55,
    "totalHNMFindings": 1,
    "numberOfAttacks": 3,
    "numberOfExploits": 0,
    "top10Vulnerabilities":
    {
        "CVE-2021-38500": 67,
        "CVE-2021-38493": 67,
        "CVE-2021-29986": 67,
        "CVE-2021-29985": 67,
        "CVE-2021-24002": 67,
        "CVE-2021-23999": 67,
        "CVE-2021-23997": 67,
        "CVE-2021-23994": 67,
        "CVE-2021-23988": 67,
        "CVE-2011-0064": 67
    },
    "numberOfSIEMCriticalEvents": 0,
    "numberOfSIEMMediumEvents": 0,
    "numberOfSIEMHighEvents": 2,
    "numberOfSIEMLowEvents": 0,
    "totalNumberOfSIEMEvents": 2,
    "globalRamaScore": 77.47350069999999,
    "created": "2023-01-06 13:09:35",
    "localTemporalScore": 5.1,
    "localBaseScore": 29.994999000000004,
    "localRamaScore": 77.47350069999999,
    "cyberSecurityStatus": "Medium",
    "hospital_address": "Street no 1",
    "hospital_region": "Hospital A from region B",
    "clientJsonList": "[{\"temporalScore\": {\"temporalScore\": 5.1, \"hnmScore\": 24,
\"siemScore\": 10}, \"metadata\": {\"severity\": 90, \"hospital_region\": \"Hospital A from
region B\", \"clientId\": 1, \"numberOfCriticalEvents\": 0, \"connected_clients\": \"1\",
\"machine_id\":
\"3119BFD93119E3AB3119D0123119960B3119B2ED3119FDE63119DF543119C5BB3119FC35311994B33119DB3C3119D9C
23119A1363119BCC73119BDB63119F25A\", \"hetMetadata\": {\"numberOfMaliciousFindings\": 4,
\"percentageOfBenignFindings\": 1100, \"noOfOSVulnerabilities\": 1,
\"percentageOfMaliciousFindings\": 400, \"noOfMisconfigurations\": 14,
\"numberOfBenignFindings\": 11, \"hetVector\": \"C:L/I:L/A:N\"}, \"indicators\": {\"vaScore\":
100, \"hnmScore\": 24, \"hetScore\": 28.55, \"hccScore\": 0, \"siemScore\": 10},
\"vulnerabilityAssessmentAggregatedMetadata\": {\"totalNoOfVulnerabilities\": 55,
\"vulnerabilityAssessmentMetadata\": [{\"application_name\": \"Mozilla Firefox 85.0.1\",
\"noOfVulnerabilities\": 55, \"vulnerabilities\": [\"CVE-2021-23997\", \"CVE-2007-3670\", \"CVE-
2011-0064\", \"CVE-2021-24001\", \"CVE-2021-24000\", \"CVE-2021-29991\", \"CVE-2021-29983\",
\"CVE-2021-23984\", \"CVE-2021-29964\", \"CVE-2021-38491\", \"CVE-2021-23999\", \"CVE-2021-
29961\", \"CVE-2021-23988\", \"CVE-2021-29982\", \"CVE-2021-29985\", \"CVE-2021-23998\", \"CVE-
2021-38492\", \"CVE-2021-23983\", \"CVE-2021-24002\", \"CVE-2021-38493\", \"CVE-2011-3389\",
\"CVE-2021-38500\", \"CVE-2021-23994\", \"CVE-2021-29986\", \"CVE-2021-29989\", \"CVE-2015-
4000\", \"CVE-2021-23986\", \"CVE-2021-23981\", \"CVE-2021-29990\", \"CVE-2021-29947\", \"CVE-
2021-23996\", \"CVE-2021-29987\", \"CVE-2021-38499\", \"CVE-2021-29944\", \"CVE-2021-29981\",
\"CVE-2021-29968\", \"CVE-2021-29946\", \"CVE-2021-29966\", \"CVE-2021-23987\", \"CVE-2021-
29955\", \"CVE-2021-38494\", \"CVE-2021-29988\", \"CVE-2021-38496\", \"CVE-2021-29984\", \"CVE-
2021-29959\", \"CVE-2021-38501\", \"CVE-2021-38498\", \"CVE-2021-29967\", \"CVE-2021-38497\",
\"CVE-2021-23995\", \"CVE-2021-23985\", \"CVE-2021-29951\", \"CVE-2021-23982\", \"CVE-2021-
29980\", \"CVE-2021-29960\"]}], \"top10Vulnerabilities\": {\"CVE-2021-23997\": 67, \"CVE-2021-
23999\": 67, \"CVE-2021-23988\": 67, \"CVE-2021-38493\": 67, \"CVE-2011-0064\": 67, \"CVE-2021-
29986\": 67, \"CVE-2021-29985\": 67, \"CVE-2021-24002\": 67, \"CVE-2021-38500\": 67, \"CVE-2021-
23994\": 67}}, \"siemMetadata\":
….
}
```

11.2 HEIR Aggregator JSON sent to HEIR's Observatory

```
{
    "hospitalId": 3212,
    "clientIdList":
    [
        1
    ],
    "noOfClients": 1,
    "globalTemporalScore": 5.1,
    "hnmScore": 24.0,
    "siemScore": 10.0,
    "globalBaseScore": 29.994999,
    "vulnerabilityAssessmentScore": 100.0,
    "hccScore": 0.0,
    "hetScore": 28.55,
    "numberOfCriticalEvents": 0,
    "numberOfIdentifiedHeartbleeds": 0,
    "noOfOSVulnerabilities": 1,
    "noOfMisconfigurations": 14,
    "numberOfBenignFindings": 11,
    "numberOfMaliciousFindings": 4,
    "percentageOfBenignFindings": 73.33333333333333,
    "percentageOfMaliciousFindings": 26.666666666666668,
    "noOfAppVulnerabilities": 55,
    "totalHNMFindings": 1,
    "numberOfAttacks": 3,
    "numberOfExploits": 0,
    "top10Vulnerabilities":
    {
        "CVE-2021-38500": 67,
        "CVE-2021-38493": 67,
        "CVE-2021-29986": 67,
        "CVE-2021-29985": 67,
        "CVE-2021-24002": 67,
        "CVE-2021-23999": 67,
        "CVE-2021-23997": 67,
        "CVE-2021-23994": 67,
        "CVE-2021-23988": 67,
        "CVE-2011-0064": 67
    },
    "numberOfSIEMCriticalEvents": 0,
    "numberOfSIEMMediumEvents": 0,
    "numberOfSIEMHighEvents": 2,
    "numberOfSIEMLowEvents": 0,
    "totalNumberOfSIEMEvents": 2,
    "globalRamaScore": 77.47350069999999,
    "created": "2023-01-06 13:09:35"
}
```

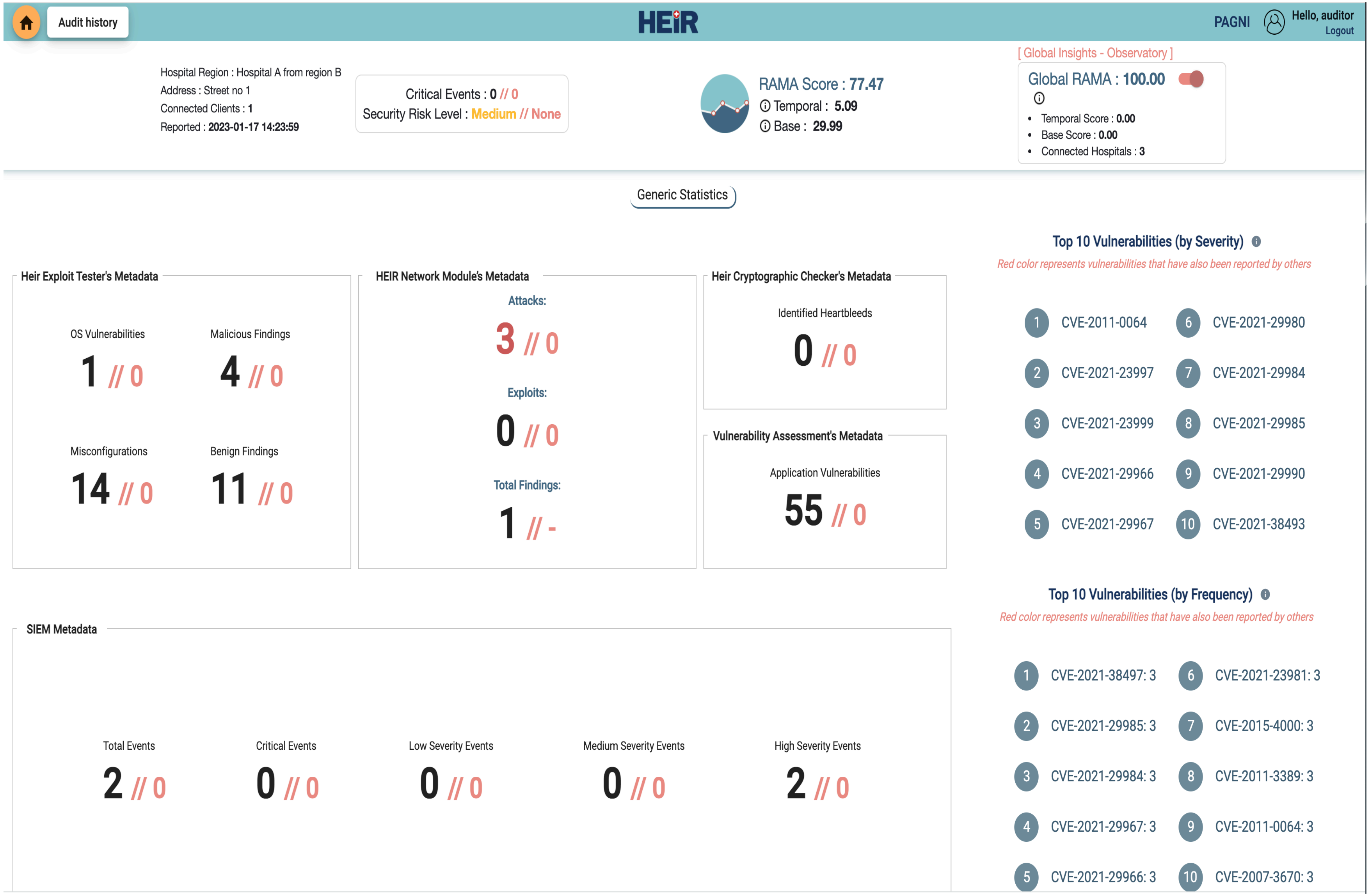
12. Annex D – HEIR 1st layer of services GUI Screenshots



User Id	Timestamp	Client Ip	Intent	Outcome	Query
EliotSalant	13/11/2022, 08:38:48	127.0.0.1	Not given	ERROR	queryAllLogs
EliotSalant	13/11/2022, 08:48:12	127.0.0.1	Not given	AUTHORIZED	queryAllLogs
EliotSalant	13/11/2022, 08:53:35	127.0.0.1	Not given	AUTHORIZED	queryAllLogs
EliotSalant	14/11/2022, 06:21:04	127.0.0.1	None	AUTHORIZED	queryAllLogs
EliotSalant	14/11/2022, 08:11:23	127.0.0.1	None	AUTHORIZED	queryAllLogs

Items per page: 5 1 – 5 of 34

Figure 15: Audit History page (logged in as Auditor)-Full size capture



Hospital Region : Hospital A from region B
Address : Street no 1
Connected Clients : 1
Reported : 2023-01-17 14:23:59

Critical Events : 0 // 0
Security Risk Level : Medium // None

RAMA Score : 77.47
Temporal : 5.09
Base : 29.99

[Global Insights - Observatory]

Global RAMA : 100.00

- Temporal Score : 0.00
- Base Score : 0.00
- Connected Hospitals : 3

Generic Statistics

Heir Exploit Tester's Metadata

OS Vulnerabilities	Malicious Findings
1 // 0	4 // 0
Misconfigurations	Benign Findings
14 // 0	11 // 0

HEIR Network Module's Metadata

Attacks: 3 // 0

Exploits: 0 // 0

Total Findings: 1 // -

Heir Cryptographic Checker's Metadata

Identified Heartbleeds: 0 // 0

Vulnerability Assessment's Metadata

Application Vulnerabilities: 55 // 0

SIEM Metadata

Total Events	Critical Events	Low Severity Events	Medium Severity Events	High Severity Events
2 // 0	0 // 0	0 // 0	0 // 0	2 // 0

Top 10 Vulnerabilities (by Severity)

Red color represents vulnerabilities that have also been reported by others

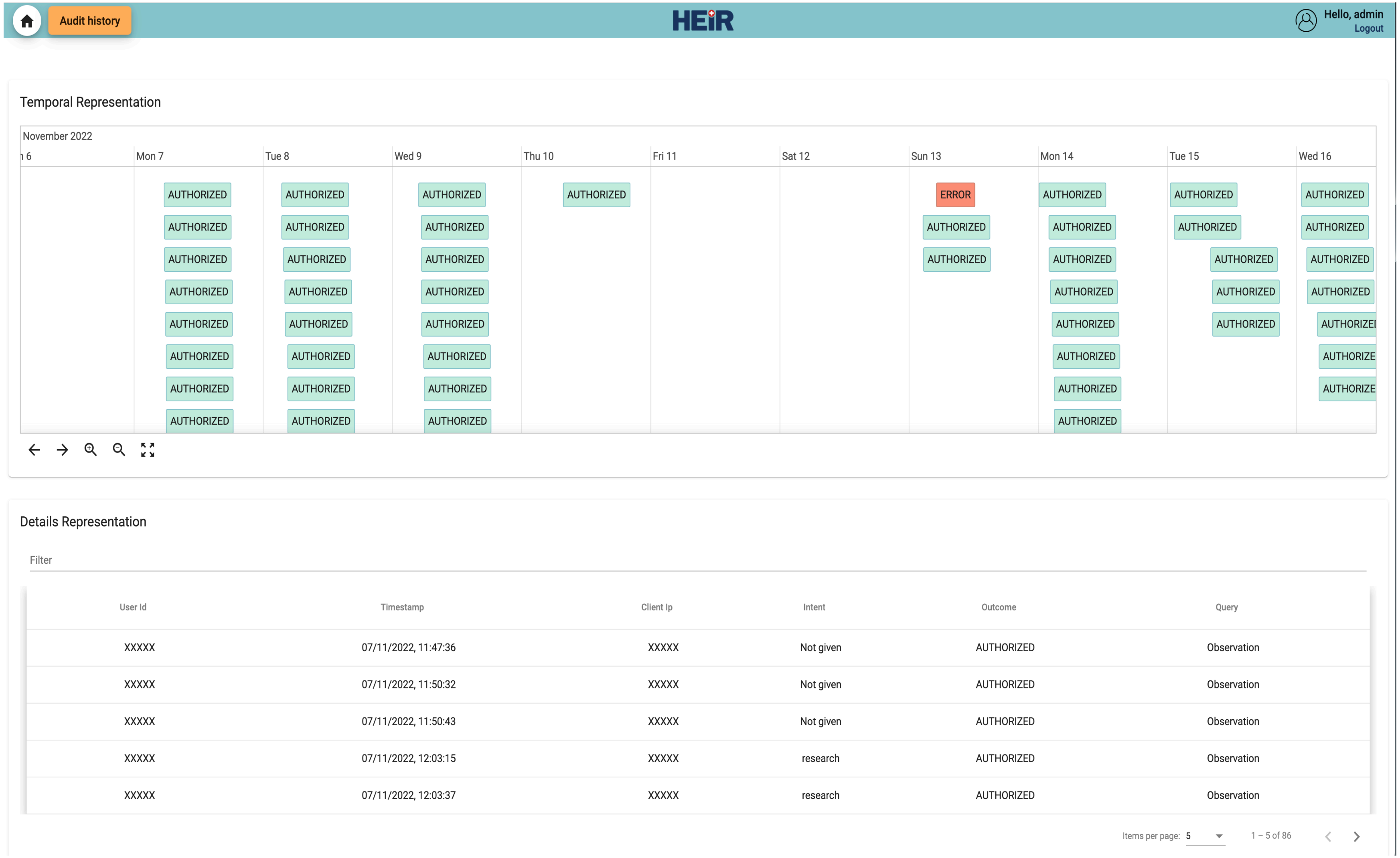
1	CVE-2011-0064	6	CVE-2021-29980
2	CVE-2021-23997	7	CVE-2021-29984
3	CVE-2021-23999	8	CVE-2021-29985
4	CVE-2021-29966	9	CVE-2021-29990
5	CVE-2021-29967	10	CVE-2021-38493

Top 10 Vulnerabilities (by Frequency)

Red color represents vulnerabilities that have also been reported by others

1	CVE-2021-38497: 3	6	CVE-2021-23981: 3
2	CVE-2021-29985: 3	7	CVE-2015-4000: 3
3	CVE-2021-29984: 3	8	CVE-2011-3389: 3
4	CVE-2021-29967: 3	9	CVE-2011-0064: 3
5	CVE-2021-29966: 3	10	CVE-2007-3670: 3

Figure 16: Audit History page (logged in as Admin), full size capture



Temporal Representation

Details Representation

Filter

User Id	Timestamp	Client Ip	Intent	Outcome	Query
XXXXX	07/11/2022, 11:47:36	XXXXX	Not given	AUTHORIZED	Observation
XXXXX	07/11/2022, 11:50:32	XXXXX	Not given	AUTHORIZED	Observation
XXXXX	07/11/2022, 11:50:43	XXXXX	Not given	AUTHORIZED	Observation
XXXXX	07/11/2022, 12:03:15	XXXXX	research	AUTHORIZED	Observation
XXXXX	07/11/2022, 12:03:37	XXXXX	research	AUTHORIZED	Observation

Items per page: 5 1 – 5 of 86

Figure 17: HEIR Client GUI page with comparisons and SIEM metrics, full size capture