Deliverable 6.2 - HEIR Demonstration – Final Execution

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.	D6.2
Workpackage	WP6
Due date	07-2022-M35
Actual submission date	31.07.2023

Deliverable lead	NSE
Editors	Rouven Besters (NSE)
Contributors	NSE, CUH, HYGEIA, PAGNI
Reviewers	STS
Dissemination level	Public
Revision	Final - 2.0
Keywords	Real-Life Demonstration, Playbook, Development

Abstract

Deliverable D6.2 focuses on the deployment of demonstrators as well as the execution in the set-up healthcare test environment. This deliverable contains background information on the pilots, the development of the use cases, the playbooks to demonstrate the HEIR functionalities per pilot and an overview of the technical status at the time of this deliverable.

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 four pilots HYGEIA; PAGNI, NSE/NOKLUS and CUH have worked closely with the technical partners to implement the HEIR solution in their technical environment and create the so-called playbooks, scripts that depict the demonstration process of the individual components for each pilot.

This deliverable will describe all the playbooks created throughout HEIR's lifecycle. However, the final year demonstrations per pilot have different focuses, which were set as follows:

1. HYGEIA aims to demonstrate the so-called Cryptographic Checker (HCC) and how this will impact the base part of the Local RAMA score. The HCC is part of HEIR's Threat Hunting Module and its task is to establish connections to check the cryptographic capabilities of every interconnected system in the IT infrastructure supporting the "*my-Ygeia*" application.
2. PAGNI aims to demonstrate HEIR's Threat Detection (TDM) and the SIEM modules. The Threat Detection Module is part of the Threat Hunting Module of the HEIR Project, which focuses on the Hospital Information System and access to the patient data held therein. Unlike the HCC, the TDM impacts the temporal part of the Local RAMA score.
3. NSE/NOKLUS aim to demonstrate the function of the so-called Privacy-Aware Framework, which focuses on facilitating policy-driven access and redaction of healthcare data.
4. CUH's objective is to showcase the Machine Learning (ML)-based Anomaly Detection capability of HEIR. To achieve this, HEIR closely monitors data flows originating from medical devices and entering the medical facility's infrastructure. The primary focus is on identifying abnormal data flows that indicate potential malfunctions in medical devices, signaling possible compromises due to malware presence. Through this demonstration, HEIR aims to highlight its ability to detect and respond to such anomalies, enhancing the overall cybersecurity posture of the medical facility.

Overall, the goal of the four different use cases is to present and demonstrate the various functionalities of the HEIR solution. So that on the one hand, a comprehensive impression of the various functions can be gained, and on the other hand, it can be proven that the developed components work as intended.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

ACL	Access Control List
CGM	Continuous glucose monitoring
CI/CD	Continuous integration and continuous delivery
CUH	Croydon University Hospital
DPO	Data Protection Officer
GUI	Graphical User Interface
HCC	HEIR Cryptographic Checker
HIS	Hospital Information System
JWT	JSON Web Token
LIS	Laboratory Information System
PACS	Picture Archiving and Communication System
PAF	Privacy-Aware Framework
PHR	Personal Health Record
PII	Personally Identifiable Information
RAMA	Risk Assessment of Medical Applications
SIEM	Security Information and Event Management
TIR	Time in range
TDM	Threat Detection Module
UI	Users Interface
UiT	University in Tromsø

1. Overview

The four end users HYGEIA Hospital (HYGEIA), the General University Hospital of Heraklion (PAGNI), the Norwegian Centre for E-Health Research (NSE) in cooperation with the Norwegian Diabatesregister for Adults (NOKLUS) and the Croydon University Hospital (CUH) have been demonstrating and carrying out the HEIR framework on four diverse, real-life health pilots in sensitive medical environments.

1.1 Scope and Objective

The aim of this deliverable and the associated task T6.2 is firstly to provide the framework conditions for the development and use of the HEIR solution and the underlying components - i.e., the technical and real-life infrastructure - and secondly to develop a detailed script - the so-called Playbooks - to execute the HEIR solution and its components in a realistic and practical healthcare environment.

The execution of the trials was an iterative process which took place over a period of time. While early versions of the HEIR solution had limited functionality, more functionalities were added over time. Although input (both physical and remote) from HEIR technical partners was needed during the operation of the testing phase, the system today can be run and controlled entirely by the four end users.

1.2 Deliverable Structure

This Deliverable is divided into a total of six parts. The second chapter is intended to provide a brief but comprehensible overview of the individual use cases, the institutions behind them and their respective background.

Building on this, the third chapter examines the developments of the individual cases in detail. The aim is to show how the cases were conceived at the beginning and which changes and adjustments were made over time before the final state was reached in July 2023.

This final state is then described in chapter four and contains the so-called *"Playbooks"*, documents that contain and describe the exact procedure for demonstrating the implemented components and functionalities of the HEIR project.

The fifth chapter provides a summary of the current technical status of the individual use cases and the technical components behind them before Chapter 6 summarizes and concludes this Deliverable.

2. The institutions behind the four use cases

2.1 HYGEIA Hospital

HYGEIA Hospital (HYGEIA) is a member of the Hellenic Healthcare Group (HHG) which is the largest private healthcare provider in Greece and Cyprus. HHG owns 8 hospitals in Greece and Cyprus and several Diagnostic Centres. It serves more than 1.5 million patients per year collaborating with more than 6.500 doctors, with 1.700 beds. HYG is the first private clinic in Greece which was accredited by the Joint Commission International (JCI) accreditation, the world's leading accreditation for quality and safety in healthcare services. In its 50 years of operation, HYGEIA has been driving the development of private healthcare in Greece and has been continuously enhancing its services both on an infrastructure and organization level. It also ensures its alignment with technological developments in medical science, standing out as a point of reference in Greece and Europe.

HYGEIA's interest in the technologies and outcomes of the HEIR project results is grounded in its continuous efforts to ensure the highest levels of quality, safety, and security for the offered healthcare services. HYGEIA's holistic Quality, Health, Safety and Environmental Policy is based on specific values which govern all operations around the entire range of services offered, and the hospital infrastructure.

To this end, HYGEIA supported the definition of the requirements and needs for the HEIR technologies and built its use case for the proactive management of vulnerabilities that can compromise the security and data privacy of the IT infrastructure supporting the "*my-Ygeia*" mobile application, that the patients use to access, manage, track, and share data, contained in their Personal Health Records (PHRs).

2.2 University Hospital of Heraklion - PAGNI

The University Hospital of Heraklion (PAGNI) is the largest hospital facility in Crete and one of the largest public hospitals in the country, with 760 beds and more than 1900 employees. Currently, PAGNI is using an integrated information system called the *«OPSI platform»*. This is an eHealth IT infrastructure that currently links the hospital medical care, the pharmacy, the patient flows and records.

The OPSI platform is an effective means for the smooth operation and easy management of the PAGNI IT system as the PAGNI's personnel (i.e., doctors, nurses, administrative staff and the IT department) uses the OPSI platform daily offering numerous services.

Despite the implemented cyber infrastructure, the OPSI platform is currently facing several cybersecurity and data privacy issues such as malware (including Ransomware) and phishing attempts, internal users having access to patient files, external attackers/hackers, mechanical failures etc., problems with third-party vendors (e.g., problems with the database administrator or cloud provider) resulting several serious system failures like: (a) loss of confidentiality (e.g. in the electronic health records), (b) loss of availability (e.g. the web interfaces of the OPSI's system) and (c) loss of integrity (e.g. clinical records).

HEIR aimed to enhance the OPSI platform with respect to its data privacy and cybersecurity by measuring and evaluating the overall security status of the hospital IT system. In particular, the operation of the OPSI platform will be boosted via the provision of a HEIR vulnerability analysis module, SIEM monitoring tools and forensics analysis, advanced visualization tools and a RAMA calculator. Furthermore, the consortium will install the Blockchain service components and work with the PAGNI team to define the use cases and procedures that are necessary to maintain the distributed health services.

2.3 Norwegian Center for e-health research and Noklus

The Norwegian Centre for E-health Research (NSE) was created in 2016 to contribute to the national development of e-health. The center is multidisciplinary and by 2019 it had 79 employees. NSEs aim is to acquire and manage a complete overview of relevant experience and knowledge regarding e-health.

The Norwegian Diabetesregister for Adults (Noklus) is a national non-profit organization that provides quality improvement services for point-of-care testing. Noklus is also responsible for the development and day-to-day running of the Norwegian diabetes register for Adults, which is a National Quality Register. Its main aim is to improve the quality of treatment for people with diabetes. The register also provides data for research on diabetes and diabetes-related conditions. In addition, Noklus hosts an annual meeting in Clinical Chemistry for Biomedical laboratory scientists and Specialists in laboratory medicine in secondary health care.

The primary objective is to make the exchange of medical data between patients' wearable devices and researchers/clinicians more secure as well as give patients the opportunity to freely decide which data they want to share with whom.

This use case will therefore mainly examine the cross-domain aspect of data exchange between patient representatives (NSE), health data register representatives (NOKLUS) and researchers. Data is being gathered by the patient on their mobile devices and sensors, and further shared between them and their clinicians for clinical purposes, with the help of the so-called *"Privacy Aware Framework"* (PAF)[1]. The PAF was built on top of the Open-Source project, Fybrik[2] and enables users to define a set of privacy policies which describe who is entitled to access the data in their medical profile.

Additionally, as part of the demonstration, NSE/NOKLUS defined a consent management system for patient-generated health data gathered via the Sensotrend[3] solution using HL7 FHIR[4]. Furthermore, NSE/NOKLUS works on a proof-of-concept that allows Noklus and/or third-party researchers to request data on a patient representatives (NSE) server, subject to the policy-defined data constraints.

2.4 Croydon University Hospital - CUH

Croydon University Hospital (CUH) is a large integrated organization located in Southwest London. There are over 380,000 patient populations under the care of the Trust, with an annual budget of over £260 Million. In Croydon health Services there are two separate healthcare systems under one roof: the acute hospital trust and community services, including primary care.

The R&D department has worked on telehealth projects in the past and the Trust has a system of virtual wards in place, to help manage patients in the community using telemedicine.

[1] https://medium.com/fybrik/using-fybrik-to-create-a-privacy-aware-framework-to-access-fhir-data-245aa1a4a6a4

[2] https://fybrik.io/v1.3/

[3] https://www.sensotrend.com

[4] https://www.hl7.org/fhir/

The HEIR project aims to demonstrate benchmarking of the current IT infrastructure (local and global RAMA score[5]) as well as the utilization of machine learning for monitoring a medical device, in this case, the chosen example is a so-called team 3 device, used within the labour ward settings, for monitoring the health of the mother and baby during labour. The idea is that the machine learning would pick up abnormal behavior in the device, indicative of a compromised device, thus enabling system isolation and if needed shut down, to ensure the security of the system as a whole from a potential cyber-attack. The aim is the increasing use of telehealth medicine delivering healthcare is becoming more reliant on remote monitoring, an increasing attack surface for cyberattacks, for which we would wish to mitigate against such intrusions.

[5] For more information see Deliverables D3.1, D3.2 and D3.3

3. Development of the Use Cases

The goal of this section is to show the evolution of each use case over the duration of the project so that a comprehensive understanding of the cases′ changes over time can be developed. This chapter will additionally serve to explain the differences between the mid-term review as well as the final demonstration, before the subsequent chapter then contains the actual playbooks for the final demonstrations.

3.1 HYGEIA

From the beginning of the project, HYGEIA aimed to use the HEIR Framework to enhance/supplement the security and data privacy of its IT architecture supporting the "***my-Ygeia***"[6] mobile application, that the patients use to access, manage, track, and share data, contained in their Personal Health Records (PHRs). This is because "*my-Ygeia*" is a relatively recent application that is constantly being enriched with new features that will not only allow patients to access their health data, but also for HYGEIA to offer extended homecare services. Since at this moment "*my-Ygeia*" is already used by tens of thousands of users, the maximum assurance of security and data integrity are imperative.

To this end, the demonstration will take place in the test environment that accurately replicates the sub-section of the IT infrastructure responsible for the operation of the *"my-Ygeia"* application. For compliance purposes, the data therein will be test/pseudonymised data that conform to regulatory requirements.

It was deemed as the most appropriate but also useful use case, for HYGEIA to demonstrate the use of the HEIR Framework for the proactive management of system vulnerabilities that can compromise the IT infrastructure.

During the first period of the project, the HYGEIA use case was built around the detection of any outdated software or missing security patch, that could be maliciously exploited. The demonstration involved the PHR Backend System Administrator using the 1st Layer GUI[7] of HEIR for:

- Checking the RAMA score for any significant reduction,
- Spotting the client reporting a vulnerability incident and checking the provided details,
- Resolving the vulnerability by updating the software, outside the HEIR environment,
- Rechecking the RAMA score, confirming that the issue has been resolved and no other vulnerability is reported.

3.1.1 Cryptographic protocol issue detection using the HCC Module

For the final demonstration, HYGEIA aims to demonstrate one of the tools comprising the HEIR Core Framework, namely the so-called Cryptographic Checker (HCC)[8]. The HCC will try to establish connections and check the cryptographic capabilities of every interconnected system in the IT infrastructure supporting the *"my-Ygeia"* application. It will then verify if devices or servers are susceptible to cryptographic attacks and modify the RAMA score accordingly, providing the necessary information to the PHR Backend System Administrator.

[6] https://www.hygeia.gr/en/my-hygeia-personal-health-record/

[7] For more information see Deliverables D3.1, D3.2 and D3.3

[8] For more information see Deliverables D3.1, D3.2 and D3.3

3.2 PAGNI

PAGNI’s use case focuses on the Hospital Information System (HIS), which allows healthcare providers (physicians, nurses, etc.) to access patient data stored in the system during their regular activity in the clinic.

The objective was to protect the “PANAKIA” HIS system from cyberattacks. Healthcare providers can register patient information, request or view exams from the Laboratory Information System and the Picture Archiving and Communication System, and access data from the Surgery List through this platform.

The primary intention was to secure the system by either protecting the workstation or utilizing machine learning techniques to detect anomalies in the platform’s daily use by medical personnel. PAGNI divided the use case into the four scenarios described below.

3.2.1 Identification of outdated software

This scenario foresees the use of HEIR’s 1st Layer GUI to check the local RAMA score and identify that a workstation at the clinic has malicious findings. The vulnerabilities details for the specific client and the HEIR system informs that a client uses an outdated version of the Mozilla Firefox browser.

3.2.2 Threat hunting using HEIR'S Threat Detection Module and SIEM system

In this scenario – which was demonstrated at the midterm review - an end user of the hospital uses the workstation at the office and opens an email. The email - from a patient - contains a malicious URL. The Threat Detection Module of HEIR identifies the threat and reports to the HEIR platform.

3.2.3 Threat detection using HEIR'S Threat Detection Module and SIEM system

In an additional scenario, an external storage device and a malware that attempts to escalate privileges and try a lateral movement tactic are involved. In this additional case the malicious application is copied from the external storage and then executed unwittingly by the end-user.

3.2.4 Anomaly Detection based on HEIR´s Machine Learning

For this specific scenario, the HEIR technical team utilized the retrospective logs to train a machine learning model specifically for the circumstance. The pre-trained model is linked to the real-time logs and monitors the logs coming from HIS. When a non-expected behavior has been identified in the real-time logs of HIS from the ML module, the FVT / Events Analysis page of the department, provides an alert about the HIS logs.

3.3 NSE and NOKLUS

The overall aim of this use case is to make the exchange of data between diabetes patients and databases/registries more secure for the parties involved.

Initially, the so-called “Diabetes Diary App”[9] was to be used for gathering the required patient data. This application allows diabetics to record – among other values and functionalities – glucose values, insulin doses and carbohydrate intake.

[9] https://play.google.com/store/apps/details?hl=no&id=no.telemed.diabetesdiary

However, it became apparent in the early stages of the project that this application would not be the optimal choice, as the data it contained was self-reported and had to be maintained manually by its users.

Against this background, it was decided to collect the data directly from the patient's diabetes devices and then transfer the data to the registries in a secure way. However, as the data transfer was not easily feasible, a suitable platform for collecting and managing the patient's data had to be found. It is important to note at this point that no real patient data were collected, processed or stored as part of the HEIR project.

The choice initially fell on *"Tidepool"*[10], a platform where all the diabetes data collected by a device comes together in a dashboard in the internet browser.

The platform enables the patients – among other functionalities – to monitor the hourly, daily, and weekly patterns, discover trends, and add notes to their diabetes management. Additionally, the platform is supposed to simplify sharing patient data with physicians, nurses, and family and control how these parties interact with the data.

However, the challenge with this solution was that the application was comparatively complex, and the scope and functions went beyond the needs of the project. Therefore, an alternative had to be found, which was identified in cooperation with the Finnish company Sensotrend.

On request, Sensotrend provided its own Dashboard- and Uploadersoftware[11] – based on the open-source components of Tidepool – against licensing. Besides being easier to use, the Finnish solution offered another advantage; the processed data was stored in the HL7 FHIR standard. This simplifies the communication and transmission of data in this projects context.

Once these baseline conditions were established – the use of the devices to gather the relevant data as well as the Finnish platform – NSE and Noklus were actively involved in the design of the use cases by autumn 2021.

Regarding the transfer of the collected data to NOKLUS; the choice fell on the so-called *"DIPS Communicator"*[12], a tool that is used by multiple actors in the healthcare sector to communicate patient-sensitive information. DIPS Communicator is – as of the date of this deliverable – the most widespread communication solution in the health sector in Norway. The decision was made, since the DIPS Communicator was at this stage already used by NOKLUS and thus integrated in their system.

Due to security guidelines, it was not possible to accommodate the components of the HEIR solution in the technical infrastructure of NSE. In close cooperation with the University in Tromsø (UiT), it was agreed to house the individual components in Microsoft's Azure, while the necessary licenses were also provided by the UiT.

After the technical framework conditions within the use case had been clarified, it was agreed within the overall project that NSE and NOKLUS should implement and demonstrate the functionalities of the PAF – a secure data transfer from the patient to various recipients in their use case.

[10] https://www.tidepool.org

[11] https://www.sensotrend.com/uploader.html

[12] https://www.dips.com/sykehus/losninger/samhandling/connectivity-suite

3.3.1 Policy-dictated data transformation to an S3 object store bucket

The first use case – which was demonstrated at the midterm review - demonstrates how data from an FHIR-compatible end device (e.g. CGM) is sent to the FHIR server, and from there, the PAF transparently exports the data with a transformation (statistical analysis) to an S3 store that NOKLUS has access to.

3.3.2 Consent management through the PAF`s privacy policy

The second use-case is about the permission to access patient data for research purposes, demonstrated through different entities such as for example hospitals or universities which require access to the patient's data within a certain time frame.

3.3.3 Distributed data registries using PAF and blockchain technology

The use case depicts the use of blockchain technology for the logging of data access actions and demonstrates how the PAF can provide role-based access to information.

3.3.4 Auditing with the PAF using blockchain technology

For accountability purposes, the PAF logs information about received data requests – who requested the information, when it was requested, the actions performed on the returned data (for example, anonymization) and other parameters to a blockchain ledger. This functionality was previously demonstrated at the midterm review.

3.4 CUH

At the start of the HEIR project, the decision was made to secure a medical application system, that can be hosted in a separate stand-alone virtual machine, upon which the HEIR-trial software could be installed to assess its functionality.

A selection of medical applications that were used at Croydon at that time was therefore assessed, and the initial concept intended to use the imaging software for ultrasound scanning.

CUH settled on the "TEAM 3 device, a Fetal/maternal monitor" which has multiple modalities such as – heart rates of fetus and mother, pulse oximetry, blood pressure, as well as uterine muscle activity – uterine contractions (i.e., sound, light, electrical and mechanical means that needed to be recorded.) The output of the device was routed to a central Sonicaid server, and the entire system could be duplicated. Furthermore, there was already a live database that was available for review as the benchmark.

A VM machine and laptops were secured, with the loan of a Team 3 device and the sonicaid server networked to provide a secure repository for the HEIR agent to be installed. It also replicated the current working environment found within the labour ward. Additionally, an agreement with the third-party vendor for assistance and support as well as permission to use their device in such a manner was secured.

Ports were opened in the Trust Firewall to enable the technical partners to access the server and install the HEIR clients into a segregated network built specifically for this project.

The proposal was thus established that CUH would run the TEAM 3 system, mimicking real-time usage in the simulated labour ward setting, then subject the system to a simulated attack to see if the HEIR solution does indeed detect attacks and can afford protection as outlined. As the whole setup was isolated, the risks to the live patient system and potential risk of software failure were mitigated.

Over the duration of the project, it became apparent that real data from a live database would be needed to help train the machine learning component of the HEIR solution from which the anomaly detection tool could be developed. The regulatory authorities were informed, and the required agreements regarding the ethical utilization of historic team 3 data in place to secure totally anonymized data from the working live team 3 device database to be anonymized for training the machine learning component.

Additionally, a standard proforma of defined abnormal recordings, that could not have naturally arisen, was generated to simulate a real cyberattack, culminating in a corrupted output from an imitated infected team3 device. This was also used to help train the machine learning needed to detect abnormal compared to normal profiles.

The testing of other aspects of the system, namely the anomaly detection and threat hunting, were discarded as they were already demonstrated at the midterm review, and had been developed at the PAGNI site – the HEIR components for local and global RAMA score, with links to the Observatory were installed at all sites, and does detect outdated software locally, as was also seen in changes in HEIR local RAMA scores at Croydon.

3.4.1 Team 3 device infection and Threat detection through HEIR´s Machine Learning

For the final demonstration, the current playbook aims to demonstrate the function of the HEIR components which monitors data flows from medical devices into the infrastructure of a medical facility, focusing on the detection of aberrant data flows indicative of a malfunctioning medical device that is intended to represent a medical device compromised by malware.

4. Execution of real-life demonstrations

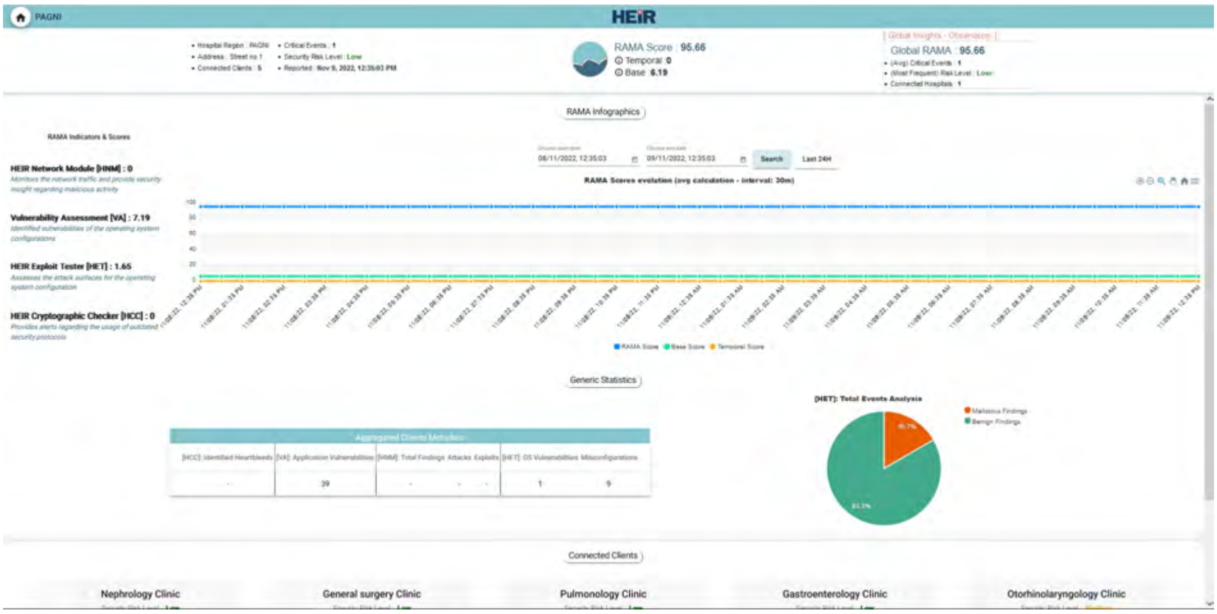
Playbooks are generally intended to specify actions according to predefined framework conditions. With the help of these playbooks, the following demonstrations of the pilot partners are to be presented in a coherent and easily understandable way.

4.1 PAGNI

PAGNI aims to demonstrate the function of the Threat (Anomaly) Detection components of the HEIR Project, which focuses on the Hospital Information System (HIS) and access to the patient data held therein. Healthcare providers (physicians, nurses etc.) have access to the HIS during their daily practice in the clinic. From that system, called PANAKIA, the Healthcare providers can record information about the patient, request, or view exams from the Laboratory Information System (LIS) and the Picture Archiving and Communication System (PACS) and retrieve data from the Surgery List.

4.1.1 Data gathering and collection

The HEIR 1st layer GUI has been deployed and operates in the premises of PAGNI at the dedicated environment for HEIR. HEIR's Threat Hunting Module is a web-based platform that collects, analyses and correlates the results of all tests run by the HEIR Client in any device or system, facilitating the work of IT professionals in medical environments as it can display their current security status in terms of adaptation of good practices. Main components of the HEIR Threat Hunting Module are: (a) the Novel HEIR Client, (b) the Local RAMA Score Calculator, (d) the 1st Layer GUI and the HEIR Aggregator. Figure 1 presents the HEIR 1st Layer GUI at the PAGNI environment.



- Hospital Region : PAGNI
- Address : Street no 1
- Connected Clients : 5
- Critical Events : 1
- Security Risk Level : Low
- Reported : Nov 9, 2022, 12:35:03 PM

RAMA Score : 95.66
Temporal : 0
Base : 6.19

[Global Insights - Observation]
Global RAMA : 95.66
- (Avg) Critical Events : 1
- (Most Frequent) Risk Level : Low
- Connected Hospitals : 1

08/11/2022, 12:35:03
09/11/2022, 12:35:03

HEIR Network Module [HNM] : 0
Monitors the network traffic and provide security insight regarding malicious activity

Vulnerability Assessment [VA] : 7.19
Identified vulnerabilities of the operating system configurations

HEIR Exploit Tester [HET] : 1.65
Assesses the attack surfaces for the operating system configuration

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

Aggregated Clients Metadata

[HCC]: Identified Heartbleeds	[VA]: Application Vulnerabilities	[HNM]: Total Findings	Attacks	Exploits	[HET]: OS Vulnerabilities	Misconfigurations
-	39	-	-	-	1	9

Nephrology Clinic
General surgery Clinic
Pulmonology Clinic
Gastroenterology Clinic
Otorhinolaryngology Clinic

Figure 1: HEIR 1st Layer GUI at PAGNI

4.1.2 Infrastructure and Architecture

The PAGNI HEIR environment consists of two dedicated Servers 2 Desktop VMs, Virtual Machines (with the same configuration as the existing PCs in the Hospital), along with four productive workstations from different departments of the hospital that the HEIR components are deployed.

The main actors are the IT SysAdmins (System Administrators) of the hospital. Furthermore, the IT SysAdmins manage the Roles, Rights and the Users of the system. The system is also accessible from the Primary Care Units in the region of Heraklion (outside of the hospital) using a VPN connection. The overall architecture is presented in Figure 2.

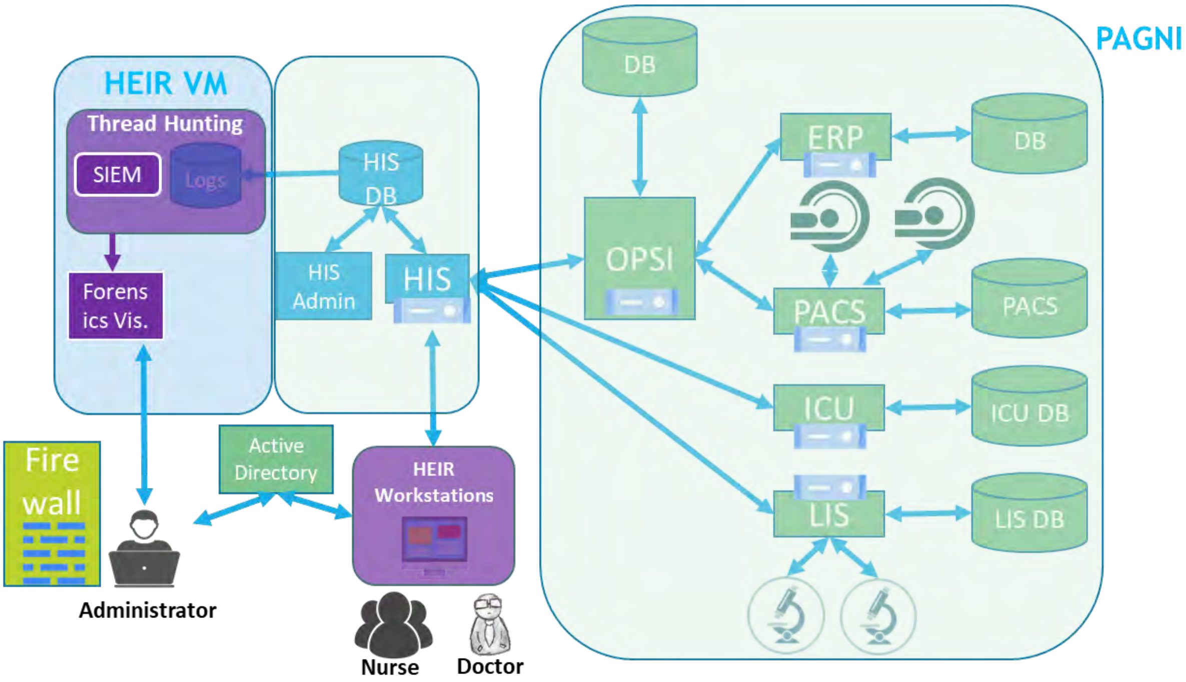


Figure 2: PAGNI Use Case – Overall Architecture

4.1.3 Playbook Scenarios

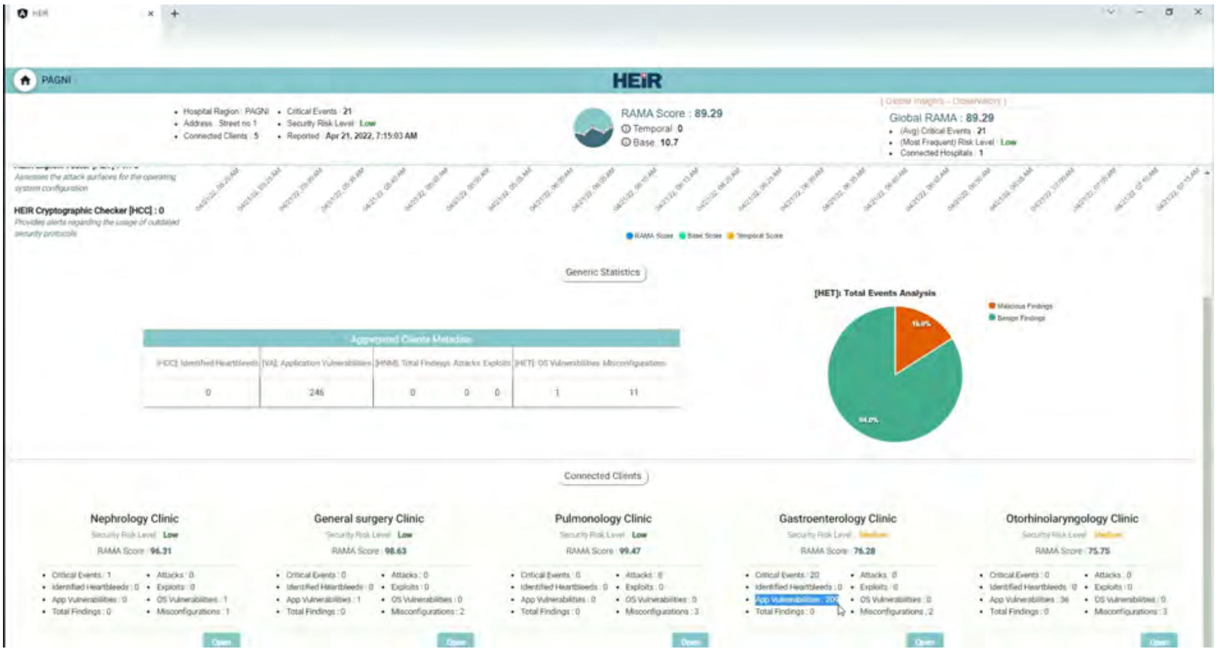
The following section explains the three scenarios foreseen in the playbook, namely the Identification of outdated software, Threat hunting using HEIR' Threat Detection Module and SIEM system, Threat detection using HEIR'S Threat Detection Module and SIEM system and the Machine learning-based Anomaly Detection.

4.1.3.1 Identification of outdated software

Involved components: HEIR's Vulnerability Assessment module, HEIR's 1st Layer GUI, HEIR's Local RAMA

In this scenario, the administrator of the hospital uses the HEIR's 1st Layer GUI to check whether any outdated software exists within the organization. More specifically, the administrator first checks the local RAMA score and identifies that one of the connected clients (a workstation at a clinic) has reported vulnerabilities. The administrator then proceeds to further examine the metadata for the specific client, as reported through HEIR's Vulnerability

Assessment. The reported metadata informs the user that a client has an outdated version of the Mozilla Firefox browser.



PAGNI

HEiR

- Hospital Region : PAGNI
- Address : Street no 1
- Connected Clients : 5
- Critical Events : 21
- Security Risk Level : Low
- Reported : Apr 21, 2022, 7:15:03 AM

RAMA Score : 89.29
Temporal : 0
Base : 10.7

(Global Insights – Observatory)
Global RAMA : 89.29
- (Avg) Critical Events : 21
- (Most Frequent) Risk Level : Low
- Connected Hospitals : 1

Assesses the attack surfaces for the operating system configuration

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

Generic Statistics

Aggregated Clients Metadata

[HCC]: Identified Heartbleeds	[VA]: Application Vulnerabilities	[HNM]: Total Findings	Attacks	Exploits	[HET]: OS Vulnerabilities	Misconfigurations
0	246	0	0	0	1	11

[HET]: Total Events Analysis

Connected Clients

Nephrology Clinic
Security Risk Level : Low
RAMA Score : 96.31
- Critical Events : 1
- Identified Heartbleeds : 0
- App Vulnerabilities : 0
- Total Findings : 0
- Attacks : 0
- Exploits : 0
- OS Vulnerabilities : 1
- Misconfigurations : 1

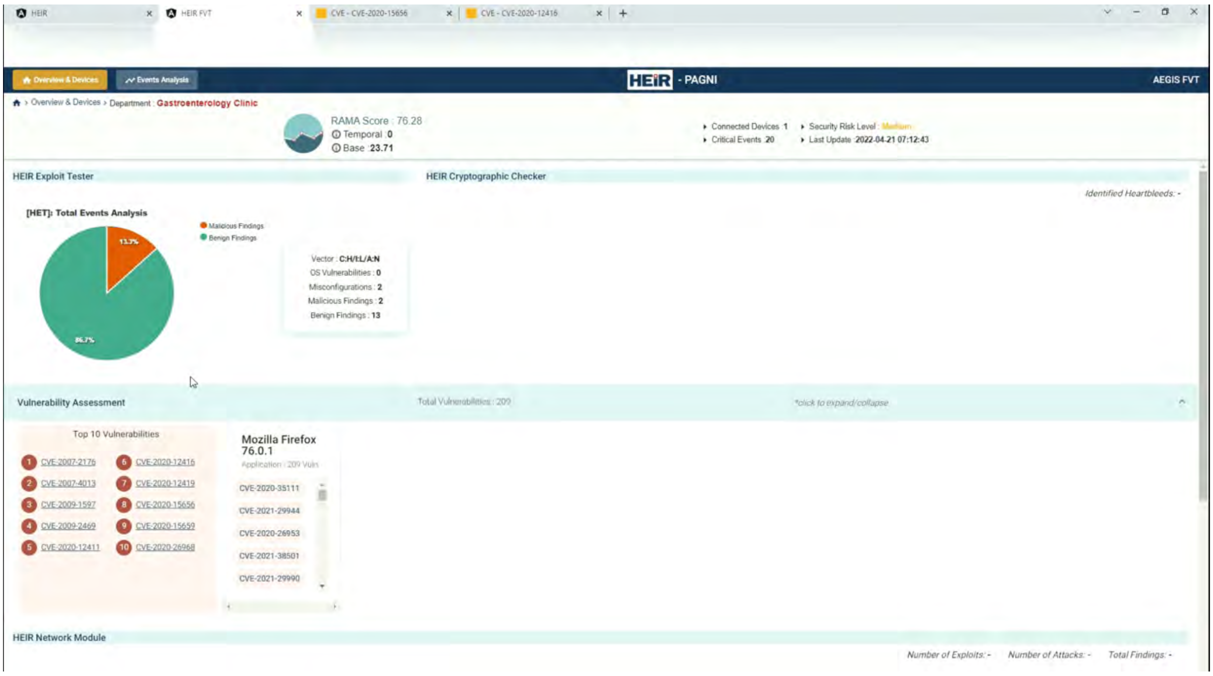
General surgery Clinic
Security Risk Level : Low
RAMA Score : 98.63
- Critical Events : 0
- Identified Heartbleeds : 0
- App Vulnerabilities : 1
- Total Findings : 0
- Attacks : 0
- Exploits : 0
- OS Vulnerabilities : 0
- Misconfigurations : 2

Pulmonology Clinic
Security Risk Level : Low
RAMA Score : 99.47
- Critical Events : 0
- Identified Heartbleeds : 0
- App Vulnerabilities : 0
- Total Findings : 0
- Attacks : 0
- Exploits : 0
- OS Vulnerabilities : 0
- Misconfigurations : 3

Gastroenterology Clinic
Security Risk Level : Medium
RAMA Score : 76.28
- Critical Events : 20
- Identified Heartbleeds : 0
- App Vulnerabilities : 209
- Total Findings : 0
- Attacks : 0
- Exploits : 0
- OS Vulnerabilities : 0
- Misconfigurations : 2

Otorhinolaryngology Clinic
Security Risk Level : Medium
RAMA Score : 75.75
- Critical Events : 0
- Identified Heartbleeds : 0
- App Vulnerabilities : 36
- Total Findings : 0
- Attacks : 0
- Exploits : 0
- OS Vulnerabilities : 0
- Misconfigurations : 3

Figure 3: Outdated software detected (1)



HEiR - PAGNI

AEGIS FVT

Overview & Devices › Department : Gastroenterology Clinic

RAMA Score : 76.28
Temporal : 0
Base : 23.71

- Connected Devices : 1
- Critical Events : 20
- Security Risk Level : Medium
- Last Update : 2022-04-21 07:12:43

HEIR Exploit Tester

HEIR Cryptographic Checker

Identified Heartbleeds: -

[HET]: Total Events Analysis

Vector : C:H/I:L/A:N
OS Vulnerabilities : 0
Misconfigurations : 2
Malicious Findings : 2
Benign Findings : 13

Vulnerability Assessment

Total Vulnerabilities : 209

*click to expand/collapse

Top 10 Vulnerabilities

1. CVE-2007-2176
2. CVE-2007-4013
3. CVE-2009-1597
4. CVE-2009-2469
5. CVE-2020-12411
6. CVE-2020-12416
7. CVE-2020-12419
8. CVE-2020-15656
9. CVE-2020-15659
10. CVE-2020-26968

Mozilla Firefox 76.0.1
Application : 209 Vuln

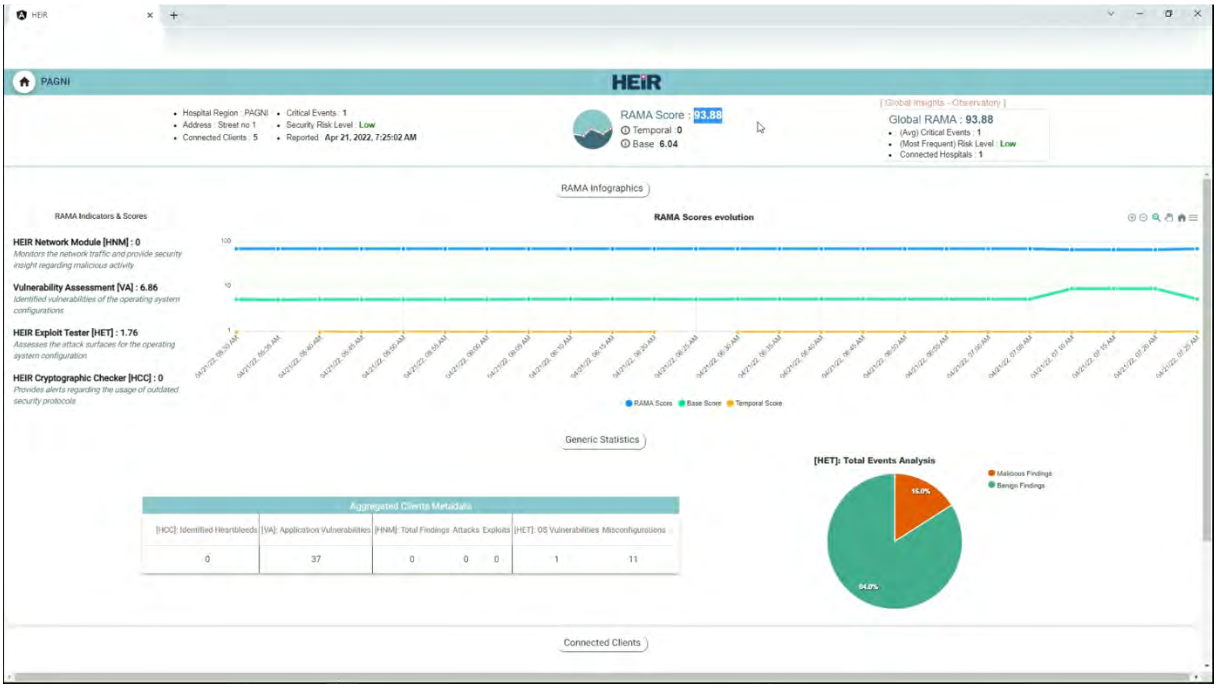
CVE-2020-35111
CVE-2021-29944
CVE-2020-26953
CVE-2021-38501
CVE-2021-29990

HEIR Network Module

Number of Exploits: - Number of Attacks: - Total Findings: -

Figure 4: Outdated software detected (2)

The administrator updates the software (Mozilla) to the specific workstation using remote connection or with physical access at the department/clinic. Then, back at the office, opens again the 1st Layer GUI of HEIR and identifies that there are no vulnerabilities anymore (Figure 5) for the specific client and that the local RAMA score has been increased.



- Hospital Region : PAGNI
- Address : Street no 1
- Connected Clients : 5
- Critical Events : 1
- Security Risk Level : Low
- Reported : Apr 21, 2022, 7:25:02 AM

RAMA Score : 93.88
Temporal : 0
Base : 6.04

[Global Insights - Observatory]

Global RAMA : 93.88

- (Avg) Critical Events : 1
- (Most Frequent) Risk Level : Low
- Connected Hospitals : 1

RAMA Indicators & Scores

HEIR Network Module [HNM] : 0
Monitors the network traffic and provide security insight regarding malicious activity

Vulnerability Assessment [VA] : 6.86
Identified vulnerabilities of the operating system configurations

HEIR Exploit Tester [HET] : 1.76
Assesses the attack surfaces for the operating system configuration

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

Aggregated Clients Metadata

[HCC]: Identified Heartbleeds	[VA]: Application Vulnerabilities	[HNM]: Total Findings	Attacks	Exploits	[HET]: OS Vulnerabilities	Misconfigurations
0	37	0	0	0	1	11

Figure 5: Increased RAMA score after software update

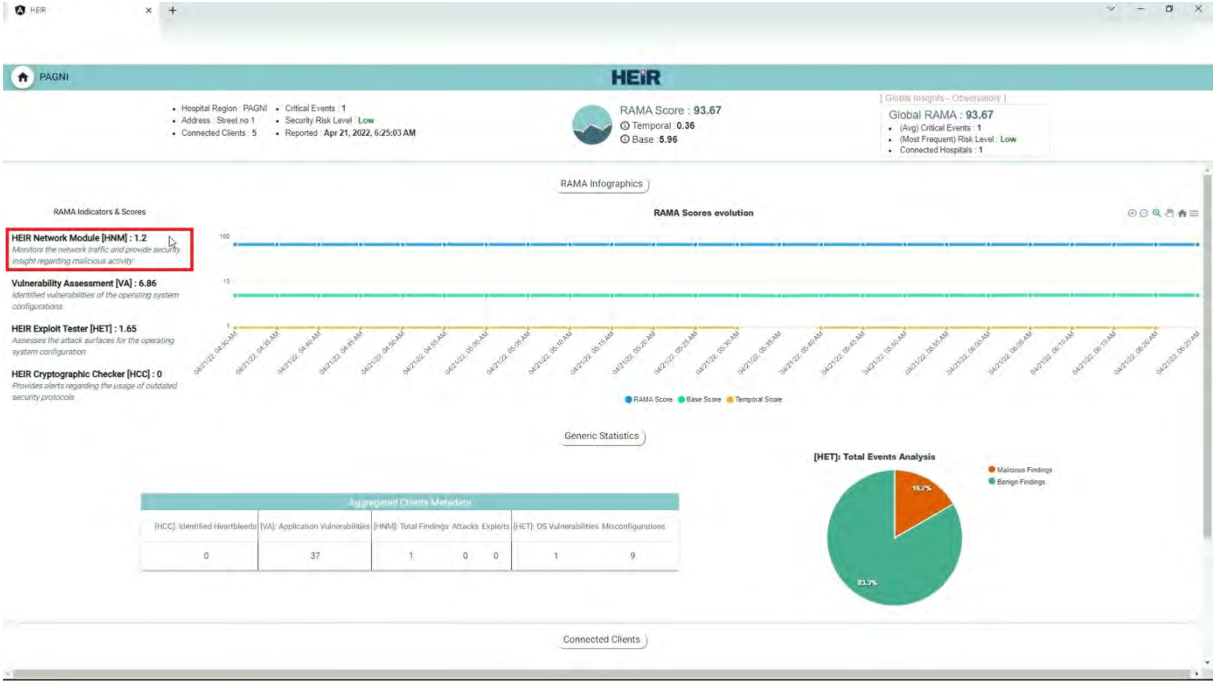
4.1.3.2 Threat hunting using HEIR' Threat Detection Module and SIEM system

Involved components: HEIR’s Network module, HEIR’s Threat Detection Module, HEIR’s SIEM system

For the smooth operation of the hospital IT systems, a threat detection and mitigation system that acts quickly and efficiently is crucial. HEIR security mechanisms can detect threats to the servers and workstations that belong to the hospital, neutralize them and inform the IT department for the issues and the actions needed.

In such a scenario, which was demonstrated at the midterm review, an end user of the hospital e.g., a physician uses the workstation at the office and opens an email. The email - from a patient - contains a URL and the sender claims that this is an MRI exam for evaluation. The physician opens the URL that is actually a malicious URL. The threat detection module of HEIR identifies the threat and reports to the HEIR platform.

On parallel the administrator of PAGNI views at the 1st Layer GUI of HEIR a threat detection. Checks the local RAMA score and identifies that one of the connected clients (a workstation at a clinic) has malicious findings as shown in Figure 6.



- Hospital Region : PAGNI
- Address : Street no 1
- Connected Clients : 5
- Critical Events : 1
- Security Risk Level : Low
- Reported : Apr 21, 2022, 6:25:03 AM

RAMA Score : 93.67
Temporal : 0.36
Base : 5.96

[Global Insights - Observatory]
Global RAMA : 93.67
- (Avg) Critical Events : 1
- (Most Frequent) Risk Level : Low
- Connected Hospitals : 1

RAMA Indicators & Scores

HEIR Network Module [HNM] : 1.2
Monitors the network traffic and provide security insight regarding malicious activity

Vulnerability Assessment [VA] : 6.86
Identified vulnerabilities of the operating system configurations

HEIR Exploit Tester [HET] : 1.65
Assesses the attack surfaces for the operating system configuration

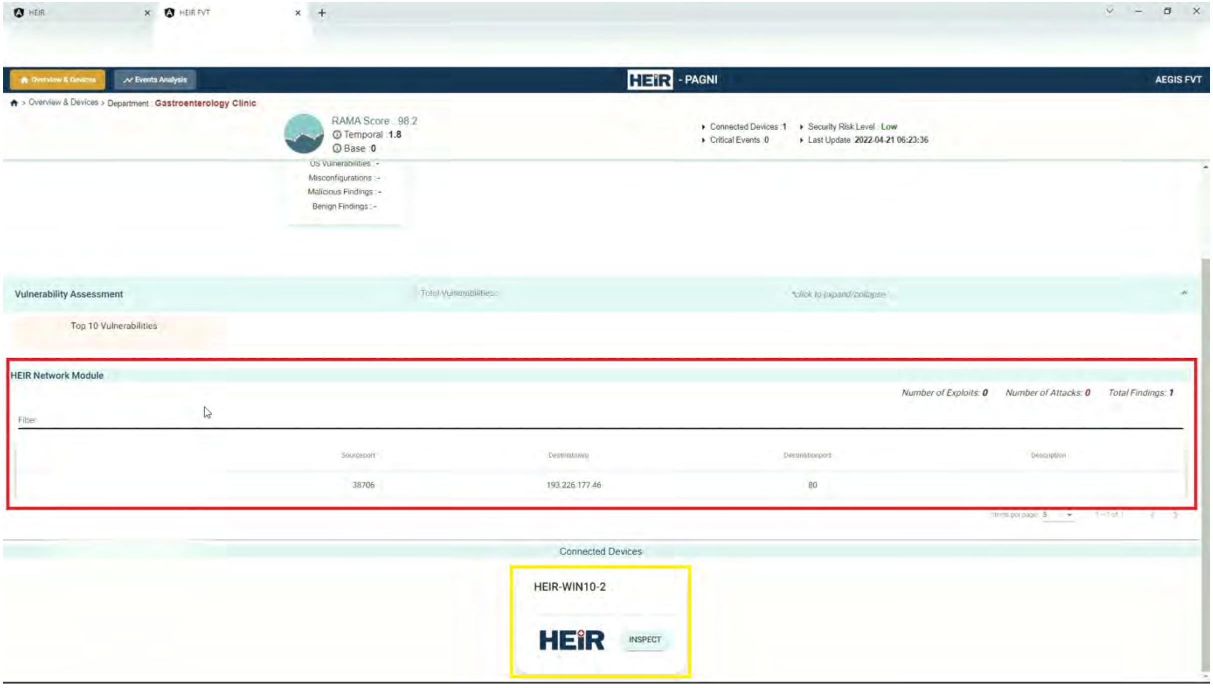
HEIR Cryptographic Checker [HCC] : 0
Provides alerts regarding the usage of outdated security protocols

Aggregated Clients Metadata

[HCC]: Identified Heartbleeds	[VA]: Application Vulnerabilities	[HNM]: Total Findings	Attacks	Exploits	[HET]: OS Vulnerabilities	Misconfigurations
0	37	1	0	0	1	9

Figure 6: Local RAMA score reduced

The administrator opens the vulnerabilities details for the specific client and the system informs the administrator that the HEIR threat detection module identified a malicious network traffic as shown in Figure 7.



Overview & Devices > Department : Gastroenterology Clinic

RAMA Score : 98.2
Temporal : 1.8
Base : 0

OS Vulnerabilities : -
Misconfigurations : -
Malicious Findings : -
Benign Findings : -

- Connected Devices : 1
- Critical Events : 0
- Security Risk Level : Low
- Last Update : 2022-04-21 06:23:36

HEIR Network Module

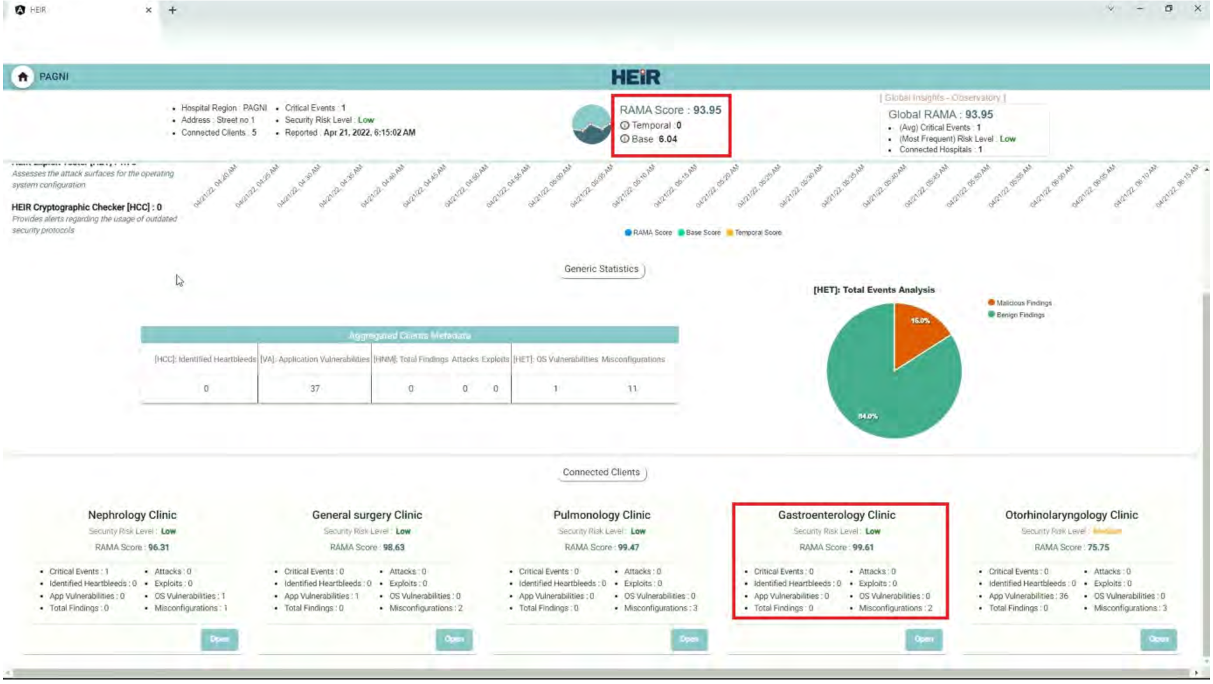
Number of Exploits: ***0*** *Number of Attacks:* ***0*** *Total Findings:* ***1***

Filter

Sourceport	Destinationip	Destinationport	Description
38706	193.226.177.46	80	

Figure 7: Malicious network traffic detected

The administrator subsequently uses the specific workstation and runs a threat scan and mitigation efforts are enacted to properly neutralize the threat, opens again the 1st Layer GUI of HEIR and identifies that there are no vulnerabilities any more for the specific client and that the local RAMA score has been increased as shown in Figure 8.



HEIR

PAGNI

- Hospital Region : PAGNI
- Address : Street no 1
- Connected Clients : 5

- Critical Events : 1
- Security Risk Level : Low
- Reported : Apr 21, 2022, 6:15:02 AM

RAMA Score : 93.95
Temporal : 0
Base : 6.04

| Global Insights - Observatory |

Global RAMA : 93.95

- (Avg) Critical Events : 1
- (Most Frequent) Risk Level : Low
- Connected Hospitals : 1

Assesses the attack surfaces for the operating system configuration

HEIR Cryptographic Checker [HCC] : 0

Provides alerts regarding the usage of outdated security protocols

Generic Statistics

Aggregated Clients Metadata

[HCC]: Identified Heartbleeds	[VA]: Application Vulnerabilities	[HNM]: Total Findings	Attacks	Exploits	[HET]: OS Vulnerabilities	Misconfigurations
0	37	0	0	0	1	11

[HET]: Total Events Analysis

Connected Clients

Nephrology Clinic
Security Risk Level : Low
RAMA Score : 96.31

- Critical Events : 1
- Identified Heartbleeds : 0
- App Vulnerabilities : 0
- Total Findings : 0
- Attacks : 0
- Exploits : 0
- OS Vulnerabilities : 1
- Misconfigurations : 1

General surgery Clinic
Security Risk Level : Low
RAMA Score : 98.63

- Critical Events : 0
- Identified Heartbleeds : 0
- App Vulnerabilities : 1
- Total Findings : 0
- Attacks : 0
- Exploits : 0
- OS Vulnerabilities : 0
- Misconfigurations : 2

Pulmonology Clinic
Security Risk Level : Low
RAMA Score : 99.47

- Critical Events : 0
- Identified Heartbleeds : 0
- App Vulnerabilities : 0
- Total Findings : 0
- Attacks : 0
- Exploits : 0
- OS Vulnerabilities : 0
- Misconfigurations : 3

Gastroenterology Clinic
Security Risk Level : Low
RAMA Score : 99.61

- Critical Events : 0
- Identified Heartbleeds : 0
- App Vulnerabilities : 0
- Total Findings : 0
- Attacks : 0
- Exploits : 0
- OS Vulnerabilities : 0
- Misconfigurations : 2

Otorhinolaryngology Clinic
Security Risk Level : Medium
RAMA Score : 75.75

- Critical Events : 0
- Identified Heartbleeds : 0
- App Vulnerabilities : 36
- Total Findings : 0
- Attacks : 0
- Exploits : 0
- OS Vulnerabilities : 0
- Misconfigurations : 3

Figure 8: Increased local RAMA (good condition)

4.1.3.3 Threat detection using HEIR'S Threat Detection Module and SIEM system

Involved components: HEIR’s Threat Detection Module, HEIR’s SIEM system, HEIR’s RAMA

This scenario involves an external storage device and malware that attempts to escalate privileges and try a lateral movement tactic. In this case the malicious application is copied from the external storage and then executed unwittingly by the end-user. The threat detection module can detect the malware and reports it to the HEIR platform. The SIEM component is also able to detect critical events performed by an entity, be it user, attacker, or process. In this case the malware - after its execution - modifies the user groups to obtain some privilege escalation. Additionally, it tries several predefined logins to obtain a lateral movement. As the logins do not work, they will generate failed login events that will be considered as an indicator of a compromise, for a SIEM point of view. This type of events, depending on their severity will be submitted to the HEIR platform to be visible and the RAMA score will be decreased. The SIEM and Threat Detection Module work in a complementary way.

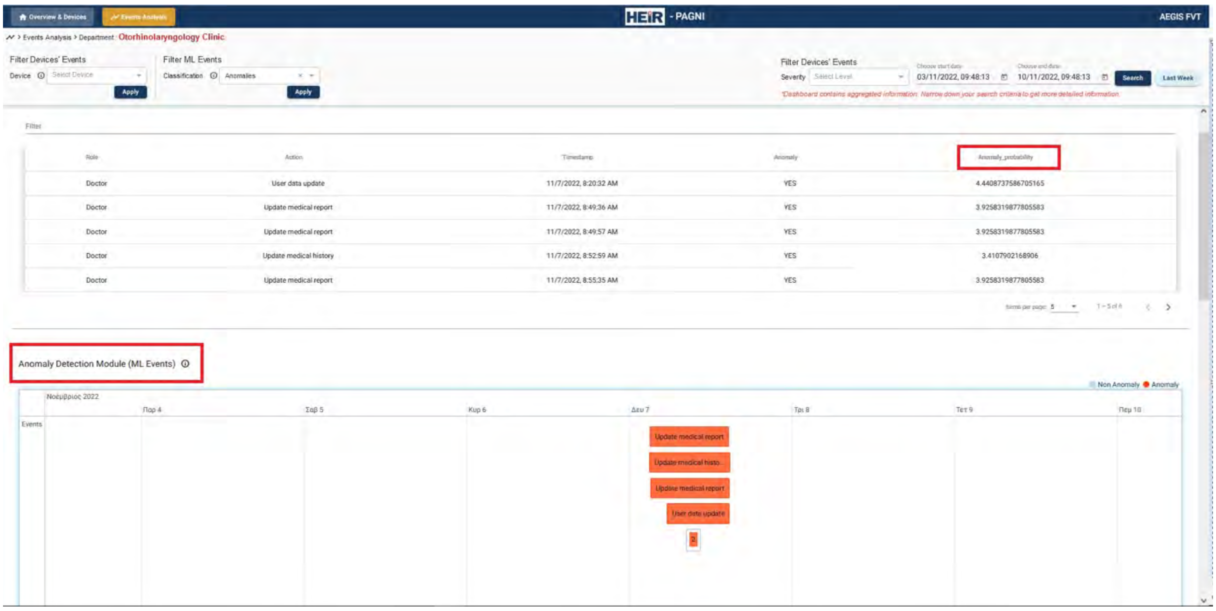
Let us presume that the detection for the malware was not available, the SIEM high severity events would be reported providing a clear indication that an attack or malicious action are active in the indicated endpoint. On the other hand, the reports from Threat Detection Module to the SIEM can also increase the importance of maybe not important action but they may provide context into the administrator analysis.

4.1.3.4 Machine learning-based Anomaly Detection

Involved components: HEIR’s ML-based Anomaly Detection Module, HEIR’s 1st Layer GUI

Retrospective and anonymized log data are available for the training of machine learning algorithms developed by the technical partners of HEIR. The main components of the IT infrastructure of the hospital (Hospital Information System, Laboratory Information System and Picture Archiving and Communication System) fed the HEIR environment with about 2.5 million records (logs/actions) anonymized logs that cover a period of 20 months. The records contain information about the user, the case/admission the action (e.g. medical action, medical report, medical history (update), exit report, document upload, surgery report, physiotherapy, request lab exams, etc.) and the connection type (VPN or not). The aim is to identify not typical behavior of the users and alert the IT department.

For the specific scenario the HEIR technical team trained a machine learning model with the retrospective logs. The pre-trained model is linked to the real time logs and monitors the logs coming from HIS. When a non-expected behavior has been identified in the real-time logs of HIS from the ML module the 1st Layer GUI of HEIR provides an alert about the HIS logs. The administrator gets a notification for the suspicious behavior from the log files of HIS and opens the 1st Layer GUI of HEIR and at the devices overview, selects the HIS server. Then, checks the temporal representation and the details representation as shown in Figure 9. To get more details, the administrator navigates to the events analysis part and uses the UI of the HEIR platform to filter and view selected time ranges Figure 10.



> Events Analysis > Department: Otorhinolaryngology Clinic

Filter Devices' Events
Device: Select Device

Filter ML Events
Classification: Anomalies

Filter Devices' Events
Severity: Select Level
Choose start date: 03/11/2022, 09:48:13
Choose end date: 10/11/2022, 09:48:13

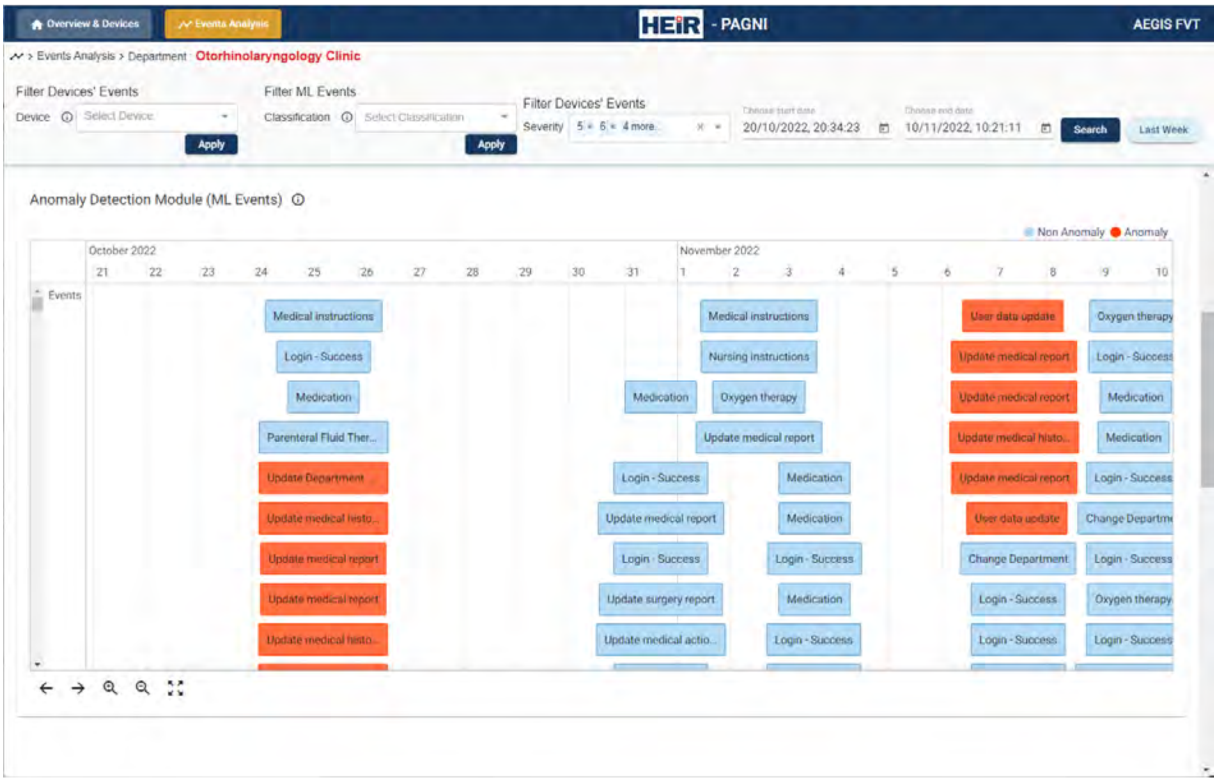
*Dashboard contains aggregated information. Narrow down your search criteria to get more detailed information.

Role	Action	Timestamp	Anomaly	Anomaly_probability
Doctor	User data update	11/7/2022, 8:20:32 AM	YES	4.4408737586705165
Doctor	Update medical report	11/7/2022, 8:49:36 AM	YES	3.9258319877805583
Doctor	Update medical report	11/7/2022, 8:49:57 AM	YES	3.9258319877805583
Doctor	Update medical history	11/7/2022, 8:52:59 AM	YES	3.4107902168906
Doctor	Update medical report	11/7/2022, 8:55:35 AM	YES	3.9258319877805583

Items per page: 5 1 – 5 of 6

Anomaly Detection Module (ML Events)

Figure 9: Anomaly detection



Events Analysis > Department : Otorhinolaryngology Clinic

Filter Devices' Events
Device: Select Device

Filter ML Events
Classification: Select Classification

Filter Devices' Events
Severity: 5 × 6 × 4 more
Choose start date: 20/10/2022, 20:34:23
Choose end date: 10/11/2022, 10:21:11

Figure 10: Anomaly detection, filtering

If the system's activity looks abnormal and other conditions like Memory and CPU usage for the server have been increased, the support team of HIS is informed about the incident for further actions if needed.

4.2 HYGEIA

HYGEIA aims to demonstrate the use of the HEIR Framework and specifically of the HEIR Cryptographic Checker (HCC) module, for the proactive managing of system vulnerabilities that can compromise the security and data privacy of its IT infrastructure, especially of the components supporting the "***my-hygeia***" mobile application, that the patients use to access, manage, track, and share data, contained in their Personal Health Records (PHRs).

The demonstration will take place in the test environment that accurately replicates the sub-section of the IT infrastructure responsible for the operation of the "*my-hygeia*" application. For compliance purposes, the data therein will be pseudonymized data conform to regulatory requirements.

4.2.1 Infrastructure & Architecture

The PHR application architecture consists of the components displayed in Figure 11 and is accessed (from the mobile device application) via the API Connect Cloud (IBM) and Secure Gateway Client (IBM). More information on the architecture can be found in deliverable *D6.1 – HEIR Demonstrations – Initial Execution and Evaluation,* section 3.3.

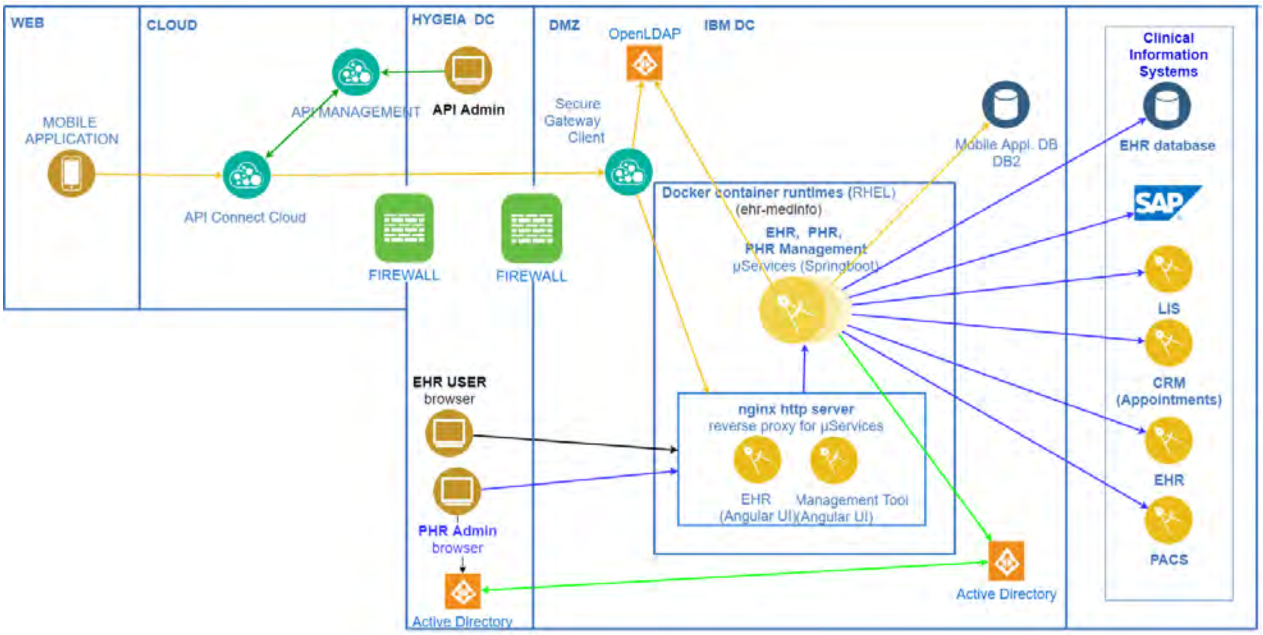


Figure 11: Hygeia Hospital Use Case Architecture – Logical Diagram

The following HEIR components have been installed to support the HYGEIA use case:

SIEM
Elastic Connector
Message Broker
SIEM Agents
Forensics Visualization Toolkit (FVT)

Visualization Level 1 – (Local RAMA)
Dynamic Vulnerability & Monitoring
HNM (Network Module)
HET (Exploit Tester)
HCC (Cryptographic Checker)
HEIR client
HEIR Agent
HEIR Aggregator
Local RAMA Score Calculator
ML

Table 1 – HYGEIA use case Components.

4.2.2 Playbook Scenario

The following section explains the scenario foreseen in the playbook, namely the Cryptographic protocol issue detection using HCC and the RAMA score.

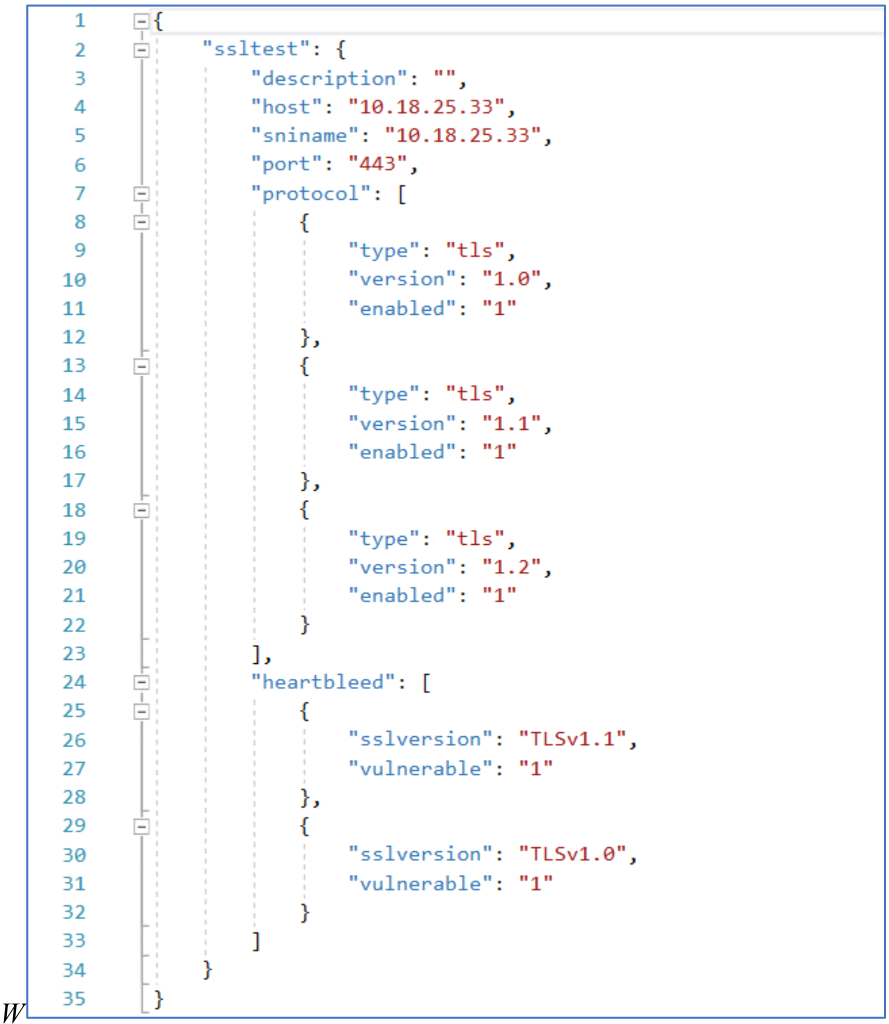
4.2.2.1 Cryptographic protocol issue detection using the HCC Module

Involved components: HEIR's Vulnerability Assessment module, HEIR's 1st Layer GUI, HEIR's Local RAMA, HEIR's Cryptographic Checker

The key objective of the HYGEIA use case is for the key actor involved, namely, the PHR Backend System Administrator, to timely detect any devices or servers that are susceptible to cryptographic attacks, and use the information provided by the HCC to resolve the vulnerability.

To this end, the use case will be demonstrated as follows:

- The Backend System Administrator opens the 1st Layer GUI of HEIR and checks the local RAMA score for any significant reduction.
- In such an occasion, the Administrator detects – through the 1st Layer GUI – the client reporting a vulnerability and checks its details. The Administrator checks the HCC reports (Figure 12) for the port and address of the vulnerable application, and which protocols are affected by the *Heartbleed* vulnerability.
- The Administrator updates the OpenSSL library or the application opening the vulnerable port, depending on which one exposed the vulnerability. This is done outside HEIR environment.
- The Administrator rechecks the local RAMA score, waiting for a new HCC scan to take place, and confirms that the issue has been resolved and no other vulnerability is reported.



```
{
    "ssltest": {
        "description": "",
        "host": "10.18.25.33",
        "sniname": "10.18.25.33",
        "port": "443",
        "protocol": [
            {
                "type": "tls",
                "version": "1.0",
                "enabled": "1"
            },
            {
                "type": "tls",
                "version": "1.1",
                "enabled": "1"
            },
            {
                "type": "tls",
                "version": "1.2",
                "enabled": "1"
            }
        ],
        "heartbleed": [
            {
                "sslversion": "TLSv1.1",
                "vulnerable": "1"
            },
            {
                "sslversion": "TLSv1.0",
                "vulnerable": "1"
            }
        ]
    }
}
```

W

Figure 12: HCC report (JSON format), detecting the Heartbleed vulnerability

4.3 NSE and NOKLUS

NSE/NOKLUS aim to demonstrate the function of the so-called Privacy-Aware Framework, which focuses on facilitating policy-driven access and redaction of healthcare data. The work is based on the HL7 FHIR[13] standard which dictates the rules for digital exchange of medical data. It will be demonstrated how the PAF can work with data stored either in a FHIR server, or in FHIR JSON format in a PostgreSQL database.

For the actual demonstrations, the following four cases are presented:

- The transfer of data with policy-dictated data transformation to an S3 object store bucket owned by the Norwegian Diabetes Register for Adults (located at NOKLUS).
- How the PAF can work in conjunction with the FHIR Consent resource to enforce time-limited patient consent to data sharing.
- How the PAF can gather data from distributed data registries, to allow seamless, privacy-regulated control to the federated FHIR resources.
- How the PAF can be used to provide role-based access to the metadata stored in the blockchain.

In addition, a professional video was produced as part of the project to provide a basic overview of this use case: https://www.youtube.com/watch?v=Pu2U2-U4iNs

4.3.1 Data gathering and collection

Involved components: Sensotrend Uploader

The demonstration starts by depicting a patient in her home, plugging in the Continuous glucose monitoring (CGM) transmitter into the laptop (see Figure 13). The video then switches into screen recording mode.

Figure 13: Sensotrend Uploader – Patient connect CGM transmitter

[13] https://www.hl7.org/fhir/

4.3.2 Data transfer

Involved components: Sensotrend Uploader, Sensotrend Dashboard

The following screen shows the Sensotrend uploader, where the patient uses her credentials to log in. The upcoming front end displays a selection of devices that can be used with the Sensotrend Uploader and requires the user to pick the device she owns. Subsequently, she triggers uploading all the data gathered (see Figure 14).

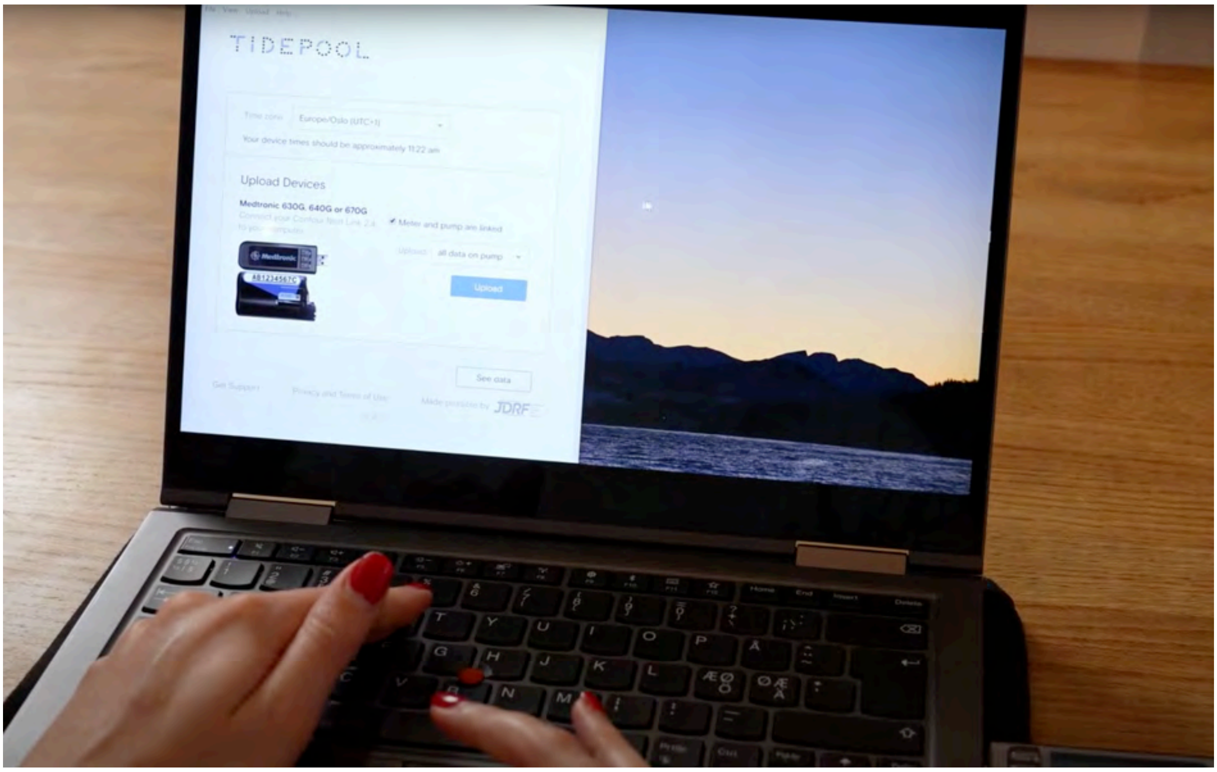
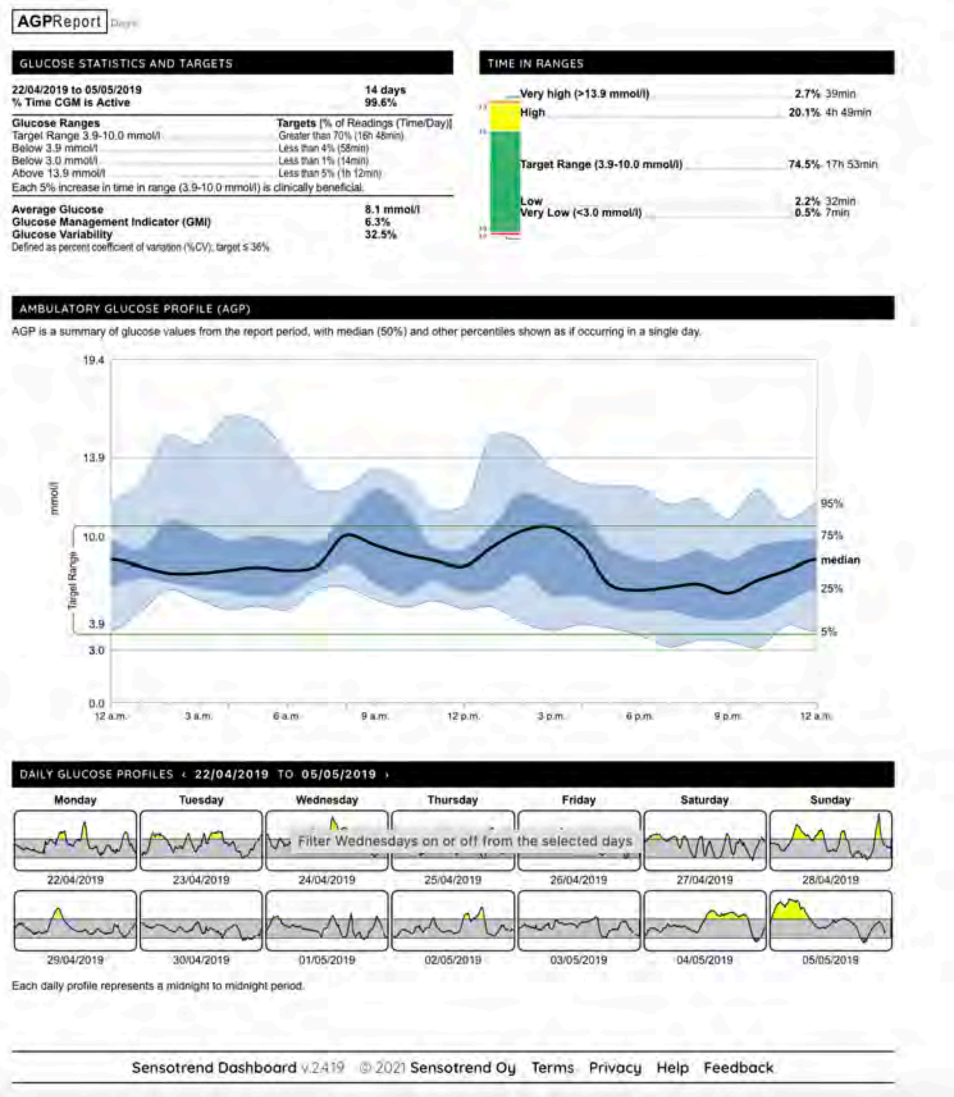


Figure 14: Sensotrend Uploader – Patient upload CGM device via the laptop

Once the upload is completed, the patient opens a web browser (this happens in screen recording mode) and logs into the Sensotrend dashboard. The collected and uploaded data is visible in the Dashboard with updated statistics such as – for example – the Glucose Ranges, and the average Glucose and Glucose Variability.

The demonstration foresees a brief presentation of the Sensotrend Dashboard (see Figure 15).



AGPReport Days

GLUCOSE STATISTICS AND TARGETS

22/04/2019 to 05/05/2019 — 14 days
% Time CGM is Active — 99.6%

Glucose Ranges	Targets [% of Readings (Time/Day)]
Target Range 3.9-10.0 mmol/l	Greater than 70% (16h 48min)
Below 3.9 mmol/l	Less than 4% (58min)
Below 3.0 mmol/l	Less than 1% (14min)
Above 13.9 mmol/l	Less than 5% (1h 12min)

Each 5% increase in time in range (3.9-10.0 mmol/l) is clinically beneficial.

Average Glucose	8.1 mmol/l
Glucose Management Indicator (GMI)	6.3%
Glucose Variability	32.5%

Defined as percent coefficient of variation (%CV); target ≤ 36%

TIME IN RANGES

Very high (>13.9 mmol/l)	2.7%	39min
High	20.1%	4h 49min
Target Range (3.9-10.0 mmol/l)	74.5%	17h 53min
Low	2.2%	32min
Very Low (<3.0 mmol/l)	0.5%	7min

AMBULATORY GLUCOSE PROFILE (AGP)

AGP is a summary of glucose values from the report period, with median (50%) and other percentiles shown as if occurring in a single day.

DAILY GLUCOSE PROFILES ‹ 22/04/2019 TO 05/05/2019 ›

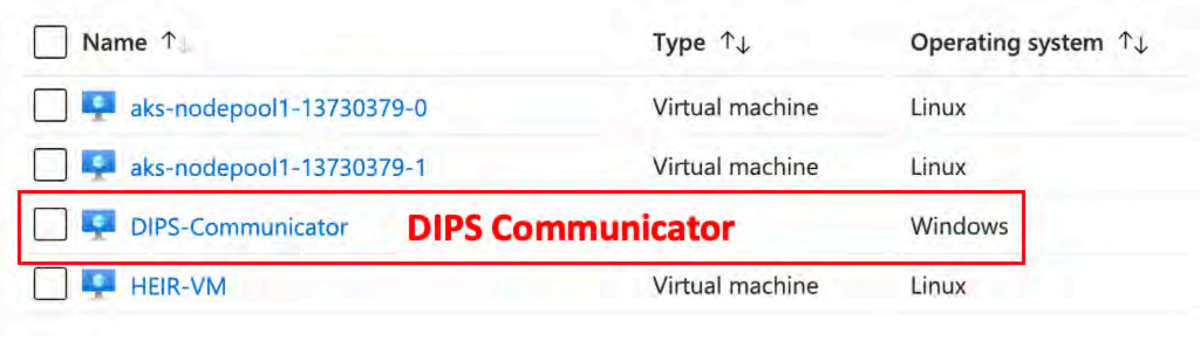
Each daily profile represents a midnight to midnight period.

Sensotrend Dashboard v.2.4.19 © 2021 Sensotrend Oy Terms Privacy Help Feedback

Figure 15: Sensotrend Dashboard

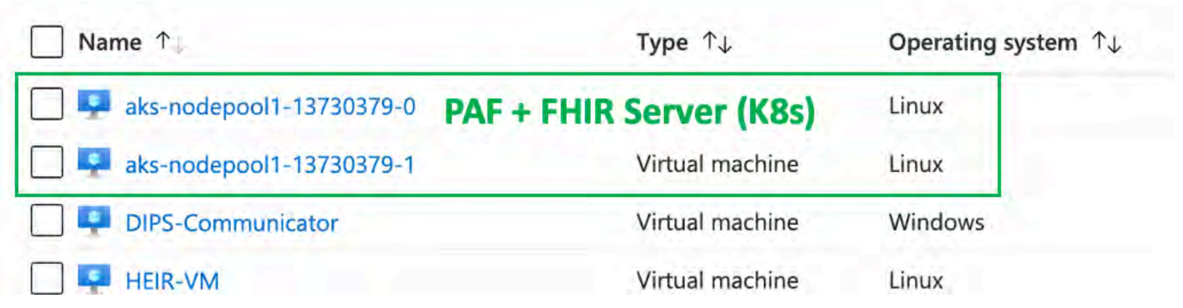
4.3.3 Infrastructure and Architecture

From here on, the demonstration switches from the Patients´ to the Developer's perspective in Microsoft Azure, where the demonstrators guide through the Cloud User Interface (UI) that shows individual servers like DIPS Communicator (see Figure 16), Kubernetes nodes (see Figure 17) and HEIR components (see Figure 18) as well as how they are being set up and the communication between them.



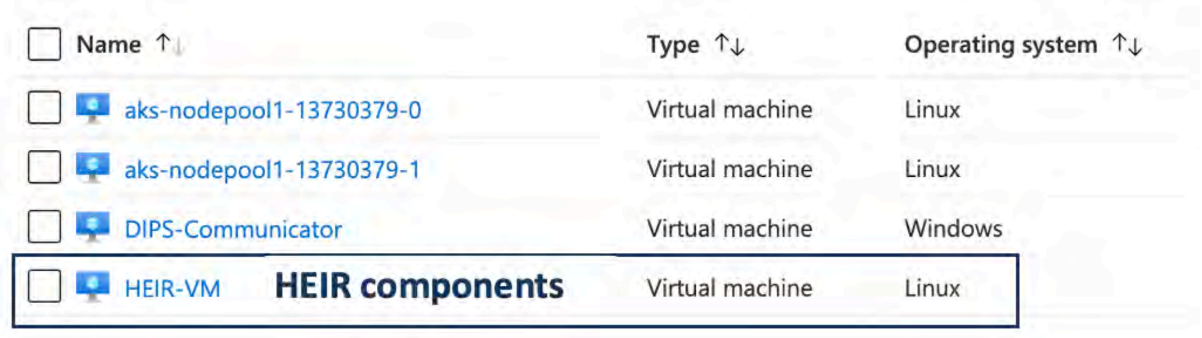
□ Name ↑	Type ↑↓	Operating system ↑↓
□ aks-nodepool1-13730379-0	Virtual machine	Linux
□ aks-nodepool1-13730379-1	Virtual machine	Linux
□ DIPS-Communicator	DIPS Communicator	Windows
□ HEIR-VM	Virtual machine	Linux

Figure 16: Azure Infrastructure – DIPS Communicator



□ Name ↑	Type ↑↓	Operating system ↑↓
□ aks-nodepool1-13730379-0	PAF + FHIR Server (K8s)	Linux
□ aks-nodepool1-13730379-1	Virtual machine	Linux
□ DIPS-Communicator	Virtual machine	Windows
□ HEIR-VM	Virtual machine	Linux

Figure 17: Azure Infrastructure – PAF and FHIR Sever in Kubernetes



□ Name ↑	Type ↑↓	Operating system ↑↓
□ aks-nodepool1-13730379-0	Virtual machine	Linux
□ aks-nodepool1-13730379-1	Virtual machine	Linux
□ DIPS-Communicator	Virtual machine	Windows
□ HEIR-VM HEIR components	Virtual machine	Linux

Figure 18: Azure Infrastructure – HEIR components

The first two virtual machines are hosting the PAF and the FHIR-Server. Fast Healthcare Interoperability Resources is a standard that defines the way healthcare information can be exchanged between different computer systems.

The third machine runs the DIPS-Communicator, a software that communicates via health-network and transfers aggregated data in this use-case to NOKLUS.

The fourth machine contains the different HEIR components such as – for example – the Threat Hunting Module, the Heir Client, or the Local RAMA Score Calculator.

4.3.4 Playbook Scenarios

The following section explains the four scenarios foreseen in the playbook, namely the Policy-Dictated Data Transformation to an S3 object Store Bucket, Consent management through the

PAF´s privacy policy, Distributed data registries using PAF and blockchain technology and Auditing with the PAF using blockchain technology.

Within the scenarios, the HEIR Observatory queries open policy agent (OPA) directly for all of the loaded policies (rules) and presents those.

4.3.4.1 Policy-dictated data transformation to an S3 object store bucket

Components: PAF, HEIR's Observatory

The first use case – which was demonstrated at the midterm review - demonstrates how data from a FHIR-compatible end device (e.g. CGM) is sent to the FHIR server, and from there, the PAF transparently exports the data with a transformation (statistical analysis) to an S3 store that NOKLUS has access to.

The demonstrators will log in to the MinIO S3, explore the MinIO S3 content and identify the newly redacted data (XML file). In a second step, the XML file that has just been computed based on newly processed data will be downloaded and further verified regarding the content inside of the file (e.g., mean, std, and time in range (TIR) glucose values). The file is then picked up by the DIPS-Communicator and transferred to NOKLUS.

In case the file cannot be verified, the transfer does not proceed and the process is stopped.

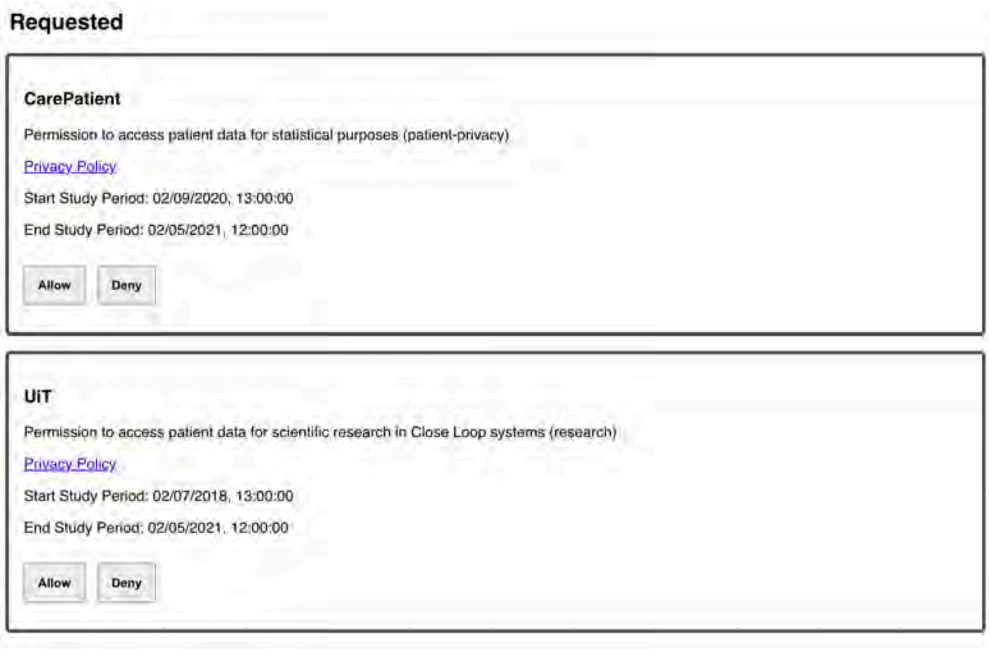
The Policy that dictates the data transformation can be easily configured. In the demonstration an example of a policy defined in the so called REGO-language that defines a statistical analysis on top of blood glucose measurements and calculates values such as Time-In-Range, Mean, Standard Deviation etc. will be displayed.

4.3.4.2 Consent management through the PAF`s privacy policy

Components: PAF, HEIR's Observatory, Sensotrend Dashboard

The second use-case, is about the permission to access patient data for research purposes, demonstrated through different entities such as for example hospitals or universities which require access to the patient's data within a certain time frame.

To demonstrate the PAF implementation, the User interface (UI) as depicted in Figure 7 was prepared. This UI lists the consents to share non-anonymized data, that have been previously granted by patients, and additionally allows patients to manage these consents.



Requested

CarePatient

Permission to access patient data for statistical purposes (patient-privacy)

Privacy Policy

Start Study Period: 02/09/2020, 13:00:00

End Study Period: 02/05/2021, 12:00:00

UiT

Permission to access patient data for scientific research in Close Loop systems (research)

Privacy Policy

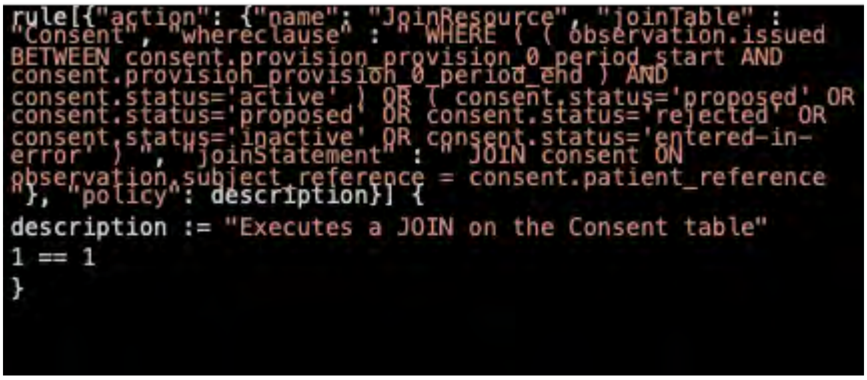
Start Study Period: 02/07/2018, 13:00:00

End Study Period: 02/05/2021, 12:00:00

Figure 19: Consent Management interface implemented in a Sensotrend Dashboard

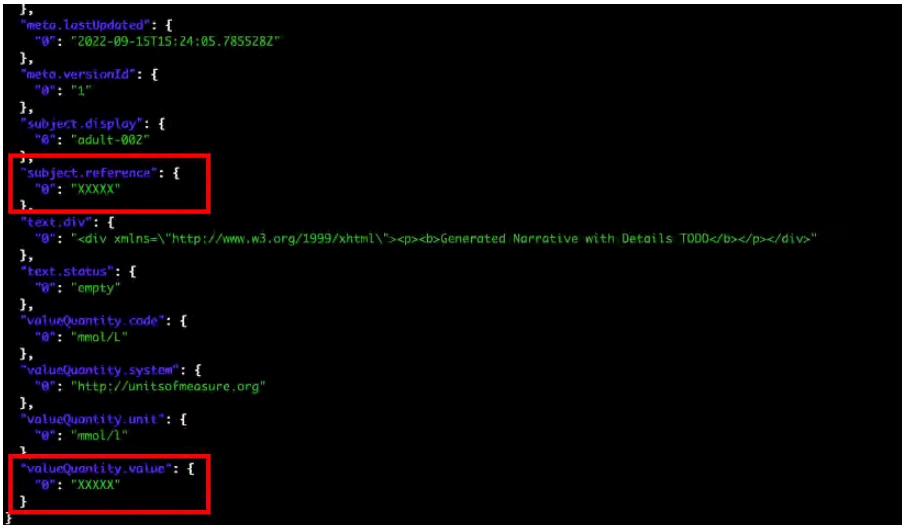
The patient now has the opportunity, to grant or deny access to his data per requestor such as for example the UiT or NOKLUS.

In case the patient allows the access, the requesting entity will be provided with the data requested within the specified timeframe.



```
rule[{"action": {"name": "JoinResource", "joinTable" :
"Consent", "whereclause" : " WHERE ( ( observation.issued
BETWEEN consent.provision_provision_0_period_start AND
consent.provision_provision_0_period_end ) AND
consent.status='active' ) OR ( consent.status='proposed' OR
consent.status='proposed' OR consent.status='rejected' OR
consent.status='inactive' OR consent.status='entered-in-
error' ) ", "joinStatement" : " JOIN consent ON
observation.subject_reference = consent.patient_reference
"}, "policy": description}] {
description := "Executes a JOIN on the Consent table"
1 == 1
}
```

Figure 20: PAF - Policy Definition



```
  },
  "meta.lastUpdated": {
    "0": "2022-09-15T15:24:05.785528Z"
  },
  "meta.versionId": {
    "0": "1"
  },
  "subject.display": {
    "0": "adult-002"
  },
  "subject.reference": {
    "0": "XXXXX"
  },
  "text.div": {
    "0": "<div xmlns=\"http://www.w3.org/1999/xhtml\"><p><b>Generated Narrative with Details TODO</b></p></div>"
  },
  "text.status": {
    "0": "empty"
  },
  "valueQuantity.code": {
    "0": "mmol/L"
  },
  "valueQuantity.system": {
    "0": "http://unitsofmeasure.org"
  },
  "valueQuantity.unit": {
    "0": "mmol/l"
  },
  "valueQuantity.value": {
    "0": "XXXXX"
  }
}
```

Figure 21: Consenting mechanism – data shared not approved

Once the PAF receives a request for medical observation records from an requesting data researcher, it will match the consent with the patients data and check whether the date of the data collection falls within the consent timeframe. If this is the case, the data requested will be returned to the entity requesting data.

The PAF policy can easily be configured to anonymize personally identifiable information (PII) before it is returned to the researcher as depicted on the Figure 21, where subject reference and observation values are transformed into 'XXXX's.

4.3.4.3 Distributed data registries using PAF and blockchain technology

Components: PAF, HEIR's Observatory

The final use case depicts the use of blockchain technology for the logging of data access actions and demonstrates how the PAF can provide role-based accessing of information.

There are two types of data requesters in this scenario, patients who should be given a collection of all their medical records from the linked registries and researchers, who need access to a large collection of medical records from the registries, but based on policy restrictions, can only access information with PII removed.

The demonstrations starts with a patient submitting a request for all of her medical records from the linked registries. The patient's identity is authenticated by a login process, and a cryptographic certificate is generated and attached to every subsequent request. The certificate contains information about the type of the request and embeds the requester's patient id.

When the PAF receives this request, it uses securely stored passwords to go out to all the linked registries and retrieve all the records associated with this patient. All data is returned to the patient without filtering or redaction of values.

Next, a Researcher will issue a request for all records across the registries for a medical study. Once again, the request will be accompanied by a cryptographic certificate identifying the researcher. The PAF will gather the medical records, and based on the data categorization we previously discussed, will replace PII fields with X's - in this example it is visible that the "subject id" has been removed.

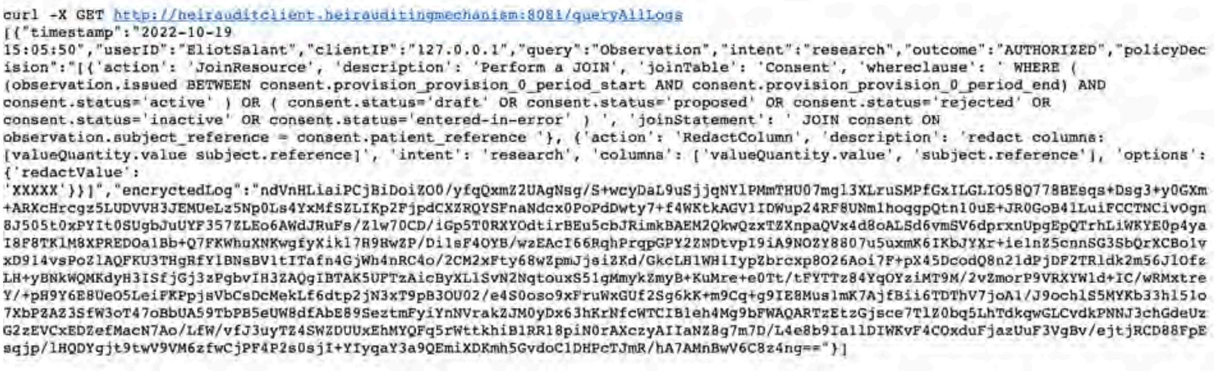
4.3.4.4 Auditing with the PAF using blockchain technology

Components: PAF, Blockchain ledger

For accountability purposes, the PAF logs information about received data requests – who requested the information, when it was requested, the actions performed on the returned data (for example, anonymization) and other parameters to a blockchain ledger. This functionality was previously demonstrated at the midterm review.

While the blockchain gives a cryptographic guarantee that stored data has not been tampered with, this logged information itself can be considered as sensitive and different roles of users should be given access to different parts of this database. Such as for example, the IT Administrator who is investigating suspicious activity might be given access to all blockchain data, whereas another role may only be allowed to get a summary of data access requests, without any details about the requester or decision taken on the request.

A sample output from the Blockchain is used to demonstrate how the log is structured and what kind of information is stored within the log. The sample log contains Information who requested the information, the IP of the requester, the intent of the request, whether the request was authorized or not and the encrypted version of the log to prevent any changes on the data.



```
curl -X GET http://heirauditclient.heirauditingmechanism:8081/queryAllLogs
[{"timestamp":"2022-10-19
15:05:50","userID":"EliotSalant","clientIP":"127.0.0.1","query":"Observation","intent":"research","outcome":"AUTHORIZED","policyDec
ision":"[{'action': 'JoinResource', 'description': 'Perform a JOIN', 'joinTable': 'Consent', 'whereclause': ' WHERE (
(observation.issued BETWEEN consent.provision_provision_0_period_start AND consent.provision_provision_0_period_end) AND
consent.status='active' ) OR ( consent.status='draft' OR consent.status='proposed' OR consent.status='rejected' OR
consent.status='inactive' OR consent.status='entered-in-error' ) ', 'joinStatement': ' JOIN consent ON
observation.subject_reference = consent.patient_reference '}, {'action': 'RedactColumn', 'description': 'redact columns:
[valueQuantity.value subject.reference]', 'intent': 'research', 'columns': ['valueQuantity.value', 'subject.reference'], 'options':
{'redactValue':
'XXXXX'}}]","encryctedLog":"ndVnHLiaiPCjBiDoiZO0/yfqQxmZ2UAgNsg/S+wcyDaL9uSjjqNYlPMmTHU07mgl3XLruSMPfGxILGLIO58Q778BEsqs+Dsg3+y0GXm
+ARXcHrcgz5LUDVVH3JEMUeLz5Np0Ls4YxMfSZLIKp2FjpdCXZRQYSFnaNdcx0PoPdDwty7+f4WKtkAGV1IDWup24RF8UNmlhoqgpQtnl0uE+JR0GoB4lLuiFCCTNCivOgn
8J505t0xPYIt0SUgbJuUYF357ZLEo6AWdJRuFs/Zlw70CD/iGp5T0RXYOdtirBEu5cbJRimkBAEM2QkwQzxTZXnpaQVx4d8oALSd6vmSV6dprxnUpgEpQTrhLiWKYE0p4ya
I8F8TKlM8XPREDOa1Bb+Q7FKWhuXNKwgfyXikl7H9HwZP/DilsF4OYB/wzEAcI66RqhPrqpGPY2ZNDtvpI9iA9NOZY8807u5uxmK6IKbJYXr+ielnZ5cnnSG3SbQrXCBolv
xD914vsPoZlAQFKU3THgRfYlBNsBV1tITafn4GjWh4nRC4o/2CM2xFty68wZpmJjsiZKd/GkcLH1WHlIypZbrcxp8O26Aoi7F+pX45DcodQ8n21dPjDF2TRldk2m56J1Ofz
LH+yBNkWQMKdyH3ISfjGj3zPgbvIH3ZAQgIBTAK5UPTzAicByXLlSvN2NqtouxS51gMmykZmyB+KuMre+e0Tt/tFYTTz84YqOYziMT9M/2vZmorP9VRXYWld+IC/wRMxtre
Y/+pH9Y6E8UeO5LeiFKPpjsVbCsDcMekLf6dtp2jN3xT9pB3OU02/e4S0oso9xFruWxGUf2Sg6kK+m9Cq+g9IE8MuslmK7AjfBii6TDThV7joAl/J9ochlS5MYKb33hl5lo
7XbPZAZ3SfW3oT47oBbUA59TbPB5eUW8dfAbE89SeztmFyiYnNVrakZJM0yDx63hKrNfcWTCIBleh4Mg9bFWAQARTzEtzGjsce7TlZ0bq5LhTdkqwGLCvdkPNNJ3chGdeUz
G2zEVCxEDZefMacN7Ao/LfW/vfJ3uyTZ4SWZDUUxEhMYQFq5rWttkhiBlRRl8piN0rAXczyAIIaNZ8g7m7D/L4e8b9Ia1lDIWKvF4COxduFjazUuF3VgBv/ejtjRCD88FpE
sqjp/lHQDYgjt9twV9VM6zfwCjPF4P2s0sjI+YIyqaY3a9QEmiXDKmh5GvdoClDHPcTJmR/hA7AMnBwV6C8z4ng=="}]
```

Figure 22: Blockchain

4.4 CUH

Croydon University Hospital aims to demonstrate the function of the HEIR components which monitors data flows from medical devices into the infrastructure of a medical facility, focusing on the detection of aberrant data flows indicative of a malfunctioning medical device that is intended to represent a medical device compromised by malware.

We aim to test the HEIR agent's ability to detect abnormal signals that may arise from an intrusion from such malware impregnated devices, in this case the aberrant signals arising from the team 3 device. This device is used to monitor maternal and fetal heart rate, maternal oxygenation saturation, as well as uterine activity (CTG). By reading such signals generated, then one is able to monitor the well-being of mother and baby during the pregnancy and labour, leading to timely intervention if needed to ensure safe delivery of the baby or preservation of maternal health.

The premise for this playbook is that the team 3 device has been compromised, thereby generating aberrant signals which would then compromise patient safety. It is therefore anticipated that the HEIR components would be able to capture these aberrant signals, reflective of a compromised medical device, and help reassure end users that compromised medical devices may be detected when the HEIR system is in use.

4.4.1 Infrastructure and Architecture

The following is the architecture that would be used for testing the HEIR system on site.

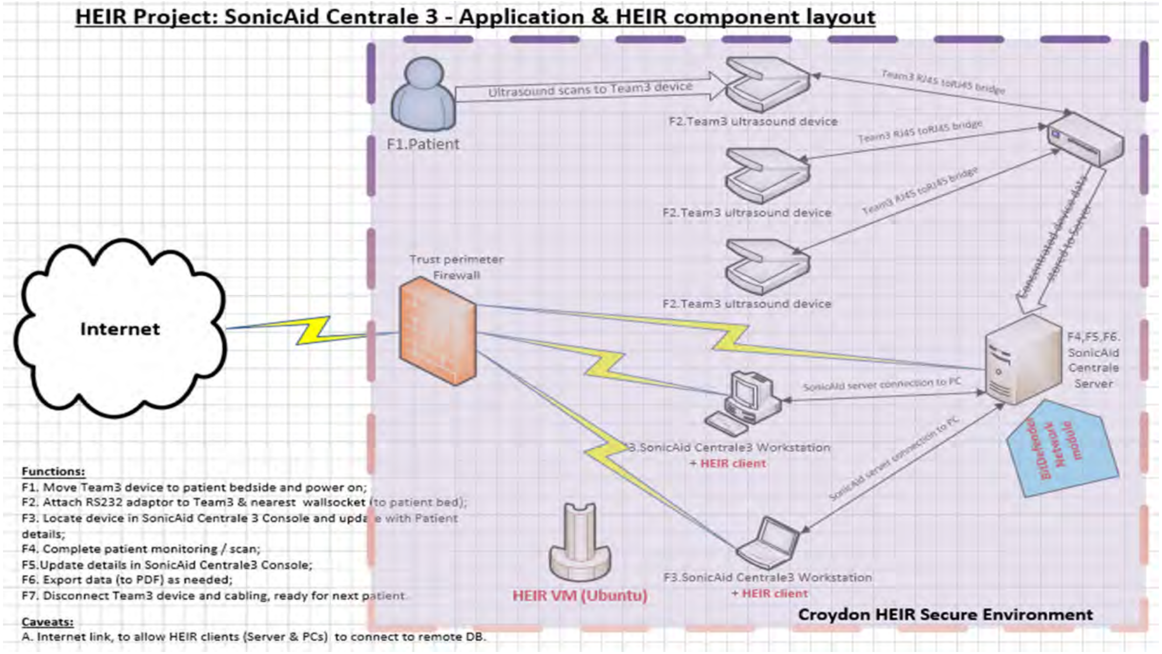

HEIR Project: SonicAid Centrale 3 - Application & HEIR component layout
F1.Patient
Ultrasound scans to Team3 device
F2.Team3 ultrasound device
F2.Team3 ultrasound device
F2.Team3 ultrasound device
Team3 RJ45 toRJ45 bridge
Team3 RJ45 toRJ45 bridge
Team3 RJ45 toRJ45 bridge
Concentrated device data stored to Server
Internet
Trust perimeter Firewall
F4,F5,F6. SonicAid Centrale Server
SonicAid server connection to PC
SonicAid server connection to PC
F3.SonicAid Centrale3 Workstation + HEIR client
F3.SonicAid Centrale3 Workstation + HEIR client
BitDefender Network module
HEIR VM (Ubuntu)
Croydon HEIR Secure Environment
Functions:
F1. Move Team3 device to patient bedside and power on;
F2. Attach RS232 adaptor to Team3 & nearest wallsocket (to patient bed);
F3. Locate device in SonicAid Centrale 3 Console and update with Patient details;
F4. Complete patient monitoring / scan;
F5.Update details in SonicAid Centrale3 Console;
F6. Export data (to PDF) as needed;
F7. Disconnect Team3 device and cabling, ready for next patient
Caveats:
A. Internet link, to allow HEIR clients (Server & PCs) to connect to remote DB.

Figure 23: CUH Infrastructure architecture

4.4.2 Playbook Scenario

The following section explains the scenario foreseen in the playbook, namely the Team 3 device infection and Threat detection through HEIR´s Machine Learning.

4.4.2.1 Team 3 device infection and Threat detection through HEIR´s Machine Learning

Involved components: Team 3 device, HEIR´s Machine Learning

For the actual demonstration, we intend to demonstrate a team 3 device in normal operation, and the HEIR user interface highlighting normal signals being detected. We would then simulate an abnormal device output and would then demonstrate the change seen within the user interface to then reflect abnormal signals, an anomaly, is now detected, and action is therefore needed from the clinical team to check on the device being monitored.

Finally, we would revert back to normal team 3 output, and would then demonstrate the return to base line on the user interface, highlighting normal signals are again detected

The demonstration starts with the utilization of machine learning. A fully anonymized data extract from historic team 3 device database utilized in the Croydon University labour ward for over 6 months was obtained after data control approval.

This data extract of the defined biophysiological components (heart rate, uterine contractions, pulse oximetry) was used to train the system, along with synthetically generated data of abnormal profiles, so that detection of anomalies could be established that could be distinguished from normal profiles.

These trained components was then installed into the virtual network pre-setup at Croydon upon which the HEIR system, as well as an isolated Team 3 device and mock infrastructure reflective of current working IT systems, was established.

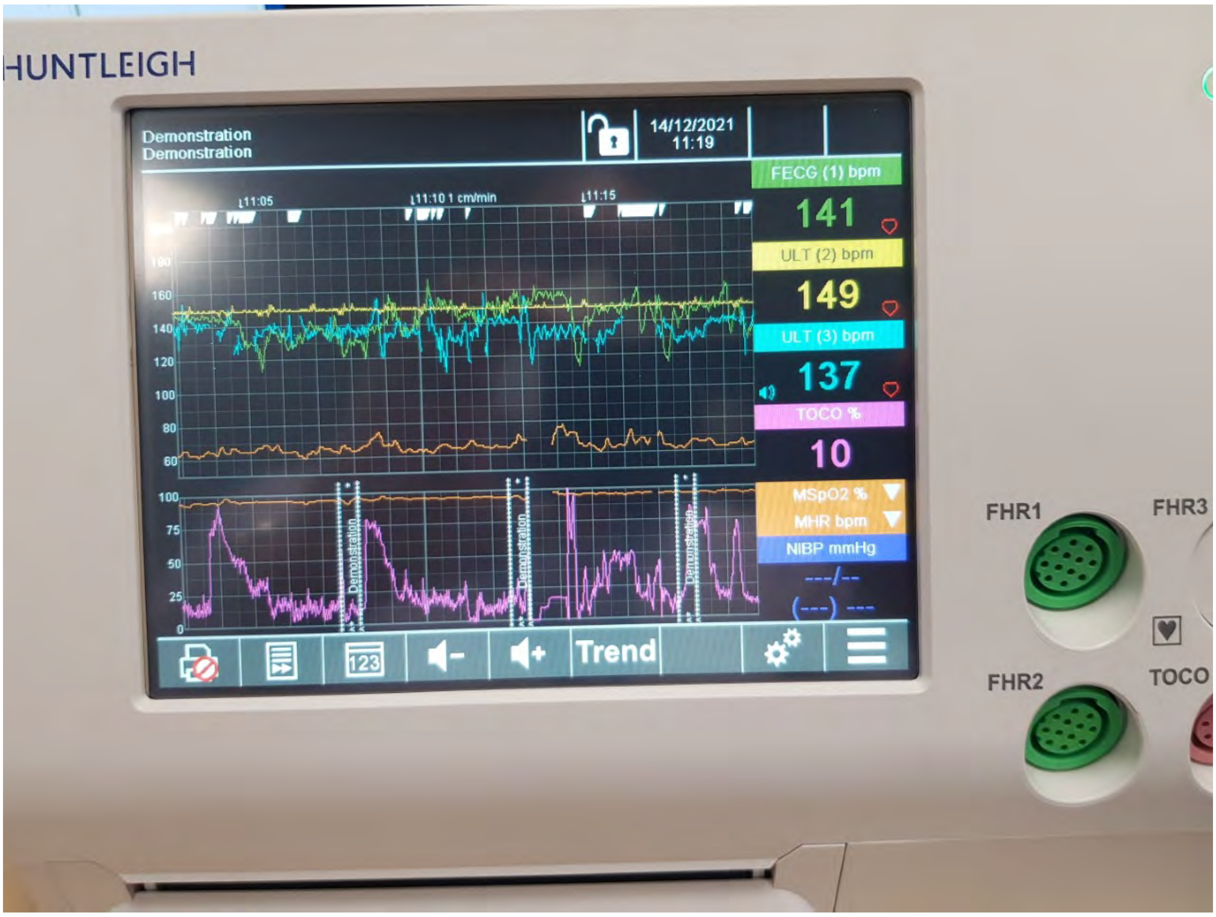


Figure 24: Team3 device in operation

4.4.2.2 External threat and possible system error

Involved components: Threat hunting module.

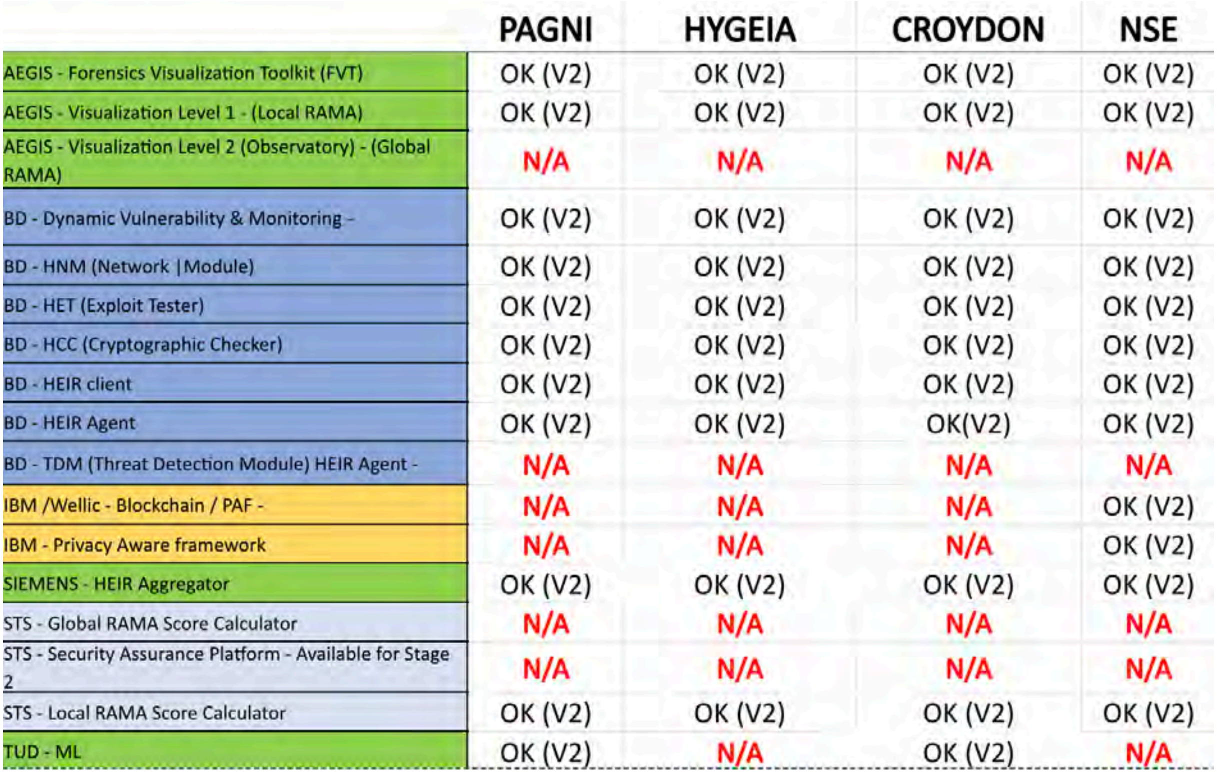
These components have been demonstrated at other sites and have been seen in previous review. It is therefore not intended to be replicated.

5. Technical status of the pilot sites

The aim of this section is to provide a brief but comprehensive overview over the technical components behind the four use cases as well as their status as of this deliverable.

Table 1 provides a clear overview of the individual components installed for each pilot. It should be noted that not every component is installed on every pilot; for example, the PAF is only part of the environment at NSE/NOKLUS. More information on the individual components can be found in the respective deliverables.

- “OK” indicates that the component is installed.
- “NA” indicates that the component is not installed as it is not applicable to the use case.
- “v1” and/or “v2” indicate the current version of the installed component.



	PAGNI	HYGEIA	CROYDON	NSE
AEGIS - Forensics Visualization Toolkit (FVT)	OK (V2)	OK (V2)	OK (V2)	OK (V2)
AEGIS - Visualization Level 1 - (Local RAMA)	OK (V2)	OK (V2)	OK (V2)	OK (V2)
AEGIS - Visualization Level 2 (Observatory) - (Global RAMA)	N/A	N/A	N/A	N/A
BD - Dynamic Vulnerability & Monitoring -	OK (V2)	OK (V2)	OK (V2)	OK (V2)
BD - HNM (Network |Module)	OK (V2)	OK (V2)	OK (V2)	OK (V2)
BD - HET (Exploit Tester)	OK (V2)	OK (V2)	OK (V2)	OK (V2)
BD - HCC (Cryptographic Checker)	OK (V2)	OK (V2)	OK (V2)	OK (V2)
BD - HEIR client	OK (V2)	OK (V2)	OK (V2)	OK (V2)
BD - HEIR Agent	OK (V2)	OK (V2)	OK(V2)	OK (V2)
BD - TDM (Threat Detection Module) HEIR Agent -	N/A	N/A	N/A	N/A
IBM /Wellic - Blockchain / PAF -	N/A	N/A	N/A	OK (V2)
IBM - Privacy Aware framework	N/A	N/A	N/A	OK (V2)
SIEMENS - HEIR Aggregator	OK (V2)	OK (V2)	OK (V2)	OK (V2)
STS - Global RAMA Score Calculator	N/A	N/A	N/A	N/A
STS - Security Assurance Platform - Available for Stage 2	N/A	N/A	N/A	N/A
STS - Local RAMA Score Calculator	OK (V2)	OK (V2)	OK (V2)	OK (V2)
TUD - ML	OK (V2)	N/A	OK (V2)	N/A

Table 1 - Technical Status of the components

The evaluation of the usability and user experience with the different components as well as the technology and operational acceptance will be conducted in D6.3

6. Conclusion

Deliverable D6.2 was intended to provide a comprehensive overview over the development and execution of the HEIR framework at the four pilot sites. In line with the four use-cases several conclusions can be made:

1. The rapid proliferation of wearable medical devices and associated digital app technology that help people manage their diabetes has given rise to a range of privacy and cybersecurity issues. Against this background, the primary aim of the NSE/Noklus use case is to make the exchange of medical data between patients' wearable diabetes devices and researchers/clinicians more secure as well as giving patients the opportunity to freely decide which data they want to share with whom.
2. The increasing use of IT infrastructures to help patient management has led to a level of risk not initially considered given the degree of increased cyber activity to be malignant. The drive to have more community care and use telemedicine to help support citizens within the community has opened a door via which cyber-attacks can be harnessed to further compromise the safe care of patients.
   The HEIR project enables CUH to explore methods that can help mitigate some of these potential healthcare risks, be it attacks on IT infrastructure or on medical devices themselves.
3. PAGNI aims to use the outcomes of HEIR in order to improve the security and privacy of its services against advanced security threats. Finally, through HEIR, PAGNI intends to utilize the results of the project's findings to strengthen its current products and overall infrastructure and to adopt the ideal and most effective technology framework for cyber security protection.
4. Early on, HYGEIA decided to explore the use of the HEIR Framework for the proactive managing of system vulnerabilities that can compromise the security and data privacy of its IT infrastructure, especially of the components supporting the relatively new "my-Ygeia" mobile application, that the patients use to access, manage, track, and share data, contained in their Personal Health Records (PHRs).
   The demonstration focused on the HEIR Cryptographic Checker (HCC) module, which provides enhanced capabilities compared to existing functionality. However, HYGEIA will consider implementing the HEIR Framework in the production environment of the "my-Ygeia" application, if certain prerequisites are met, as described in D6.3.

The HEIR framework will be maintained in a fully functional state throughout the project's duration to provide a stable and efficient system for end-users, and appropriate measures are taken to ensure that this state is maintained beyond the project's completion. This is to ensure that further projects can follow up on the results of the HEIR project (see Deliverable 5.5).