

# HEIR

A Secure Healthcare environment for informatics resilience



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

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.

# Summary

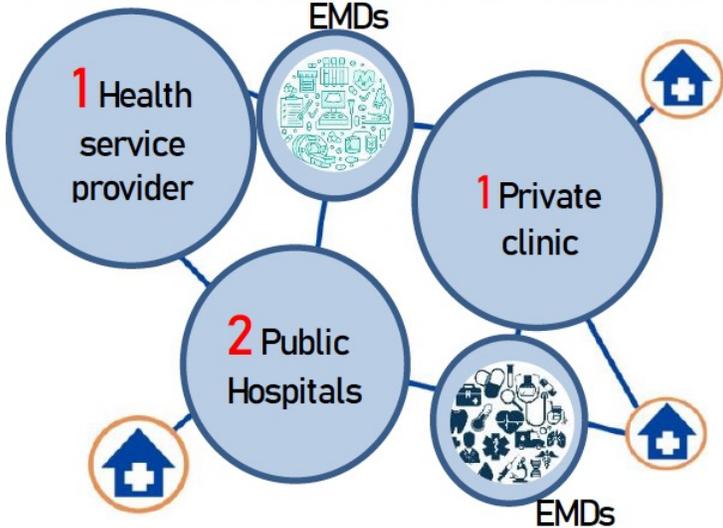
- HEIR is an RIA 2020 project started in September 2020 with duration of 36 months
  - Project number: 883275
- The topic of the project is SU-DS05-2018-2019 - Digital security, privacy, data protection and accountability in critical sectors
- The consortium includes partners from ten (10) countries: France, Germany, Greece, Cyprus, Switzerland, Romania, Norway, the Netherlands, United Kingdom, and Israel.
- The budget is € 4.999.975.

# General information



## The validation ecosystem

4 real-world pilots from health domain with physically entangled systems involving connected electronic medical devices and distributed medical facilities



# HEIR Vision: comprehensive framework

- Infrastructure protection through real time intelligent threat hunting services
  - Multi-tier unified architecture
- Sensitive data sharing
  - Policy-based access
  - Blockchain-based logging
- Benchmarking based on the calculation of the Risk Assessment of Medical Applications (RAMA) score
- Observatory
- Four validation use cases



# Privacy Aware Framework (PAF) Blockchain logging



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

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.

# The Problem

- How can we control access to data based on policy?
- How can we supply auditability for data accesses?
- Data access policy can depend on:
  - Intent
  - Categorization of the data (e.g. PII)
  - Geography
  - User role
  - etc.

# The Concept

- Policy decision and enforcement needs to be separate from application logic
- Take advantage of cutting edge technologies such as Kubernetes for security, orchestration etc.
- Create a “data mesh”

# The Starting Point

Data security framework

**Fyrik**

A cloud-native platform to control data usage

Get started

Go to GitHub

Policy



Open Policy Agent

Orchestration



kubernetes



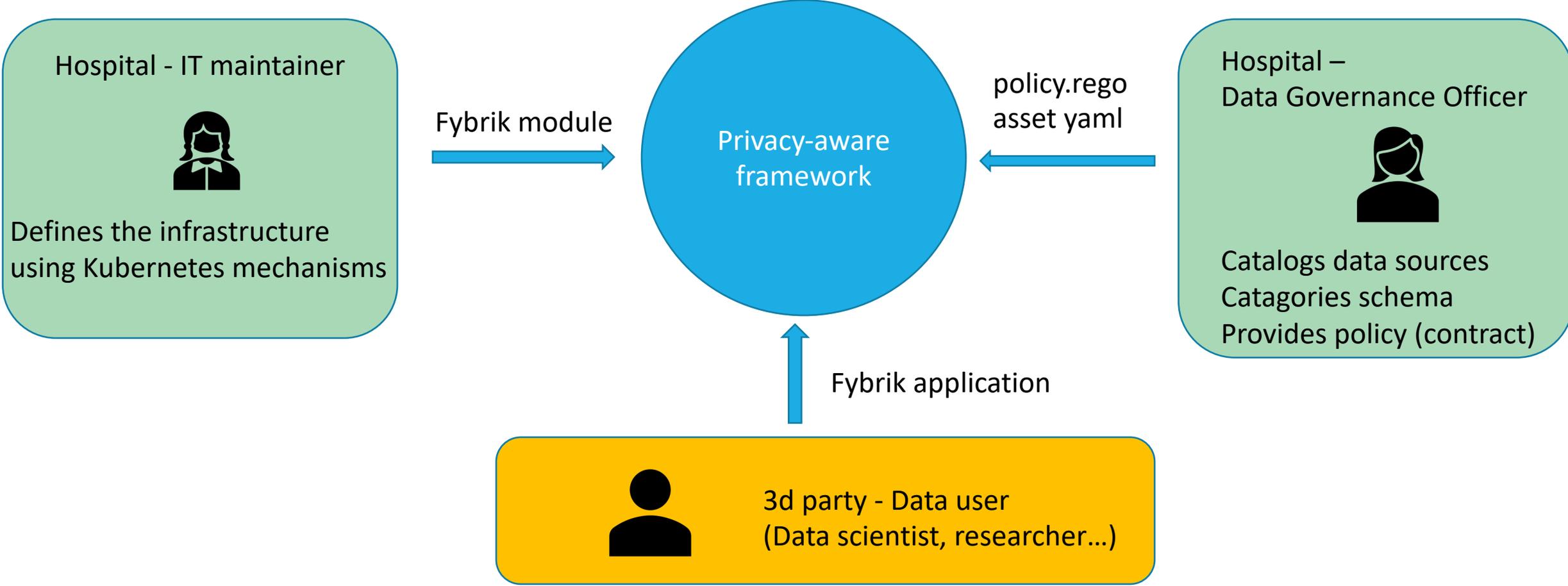
Istio

Containers

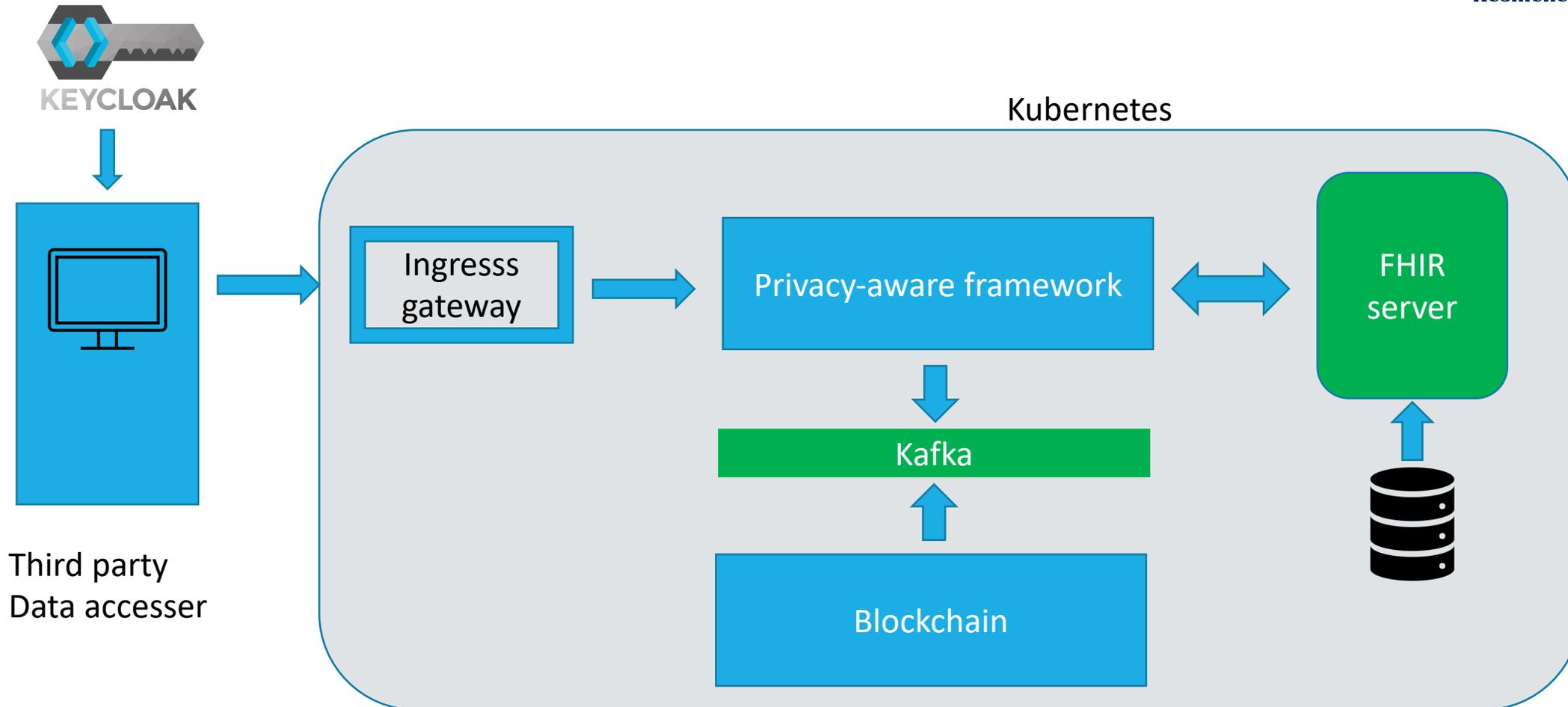


docker

# Configuring the PAF in a hospital



# Conceptual Architecture



# The problem

- IT services, devices, infrastructure, applications and their users create a constant flow of events
- Many systems rely on the auditing of logs to identify security incidents and threats
- Audit trails can serve as proofs when disputes arise regarding serious issues such as abuse of permissions, illegal access attempts, and the improper disclosure of patients' health data
- However
  - Confidentiality and integrity of the audit trails must be ensured for effective, trustworthy auditing
  - Confidentiality can be achieved by a proper access control mechanism to the audit logs
  - What about integrity?

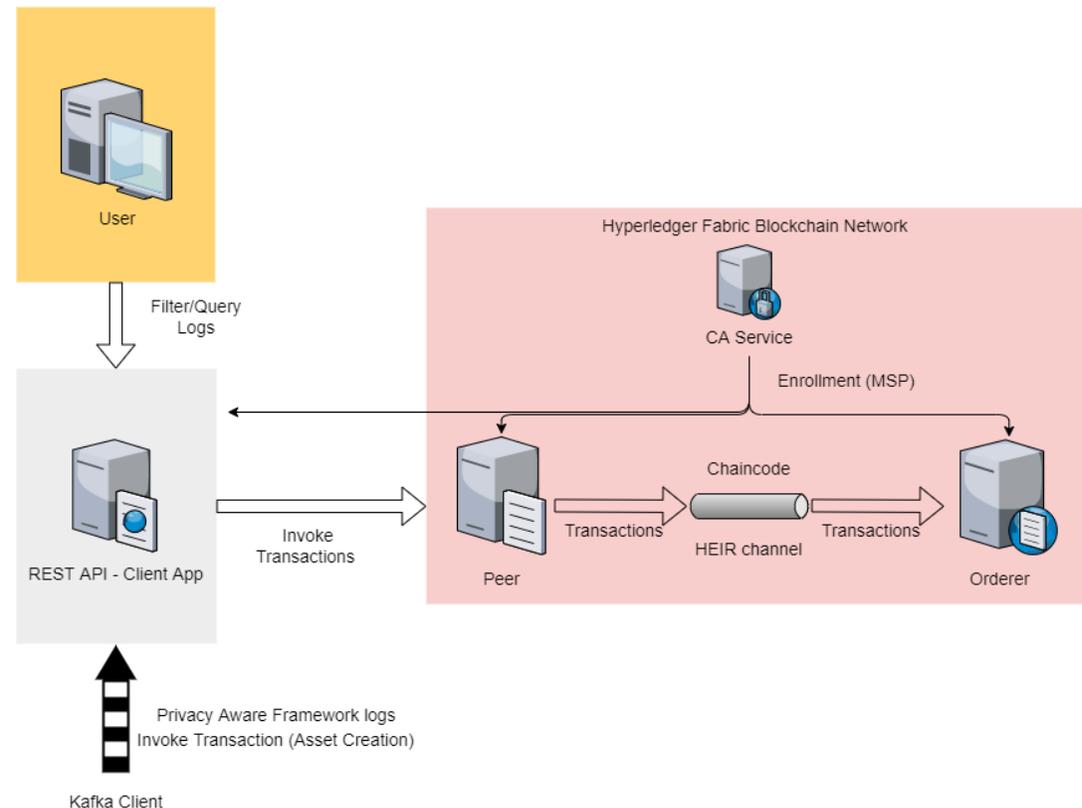
# HEiR's solution

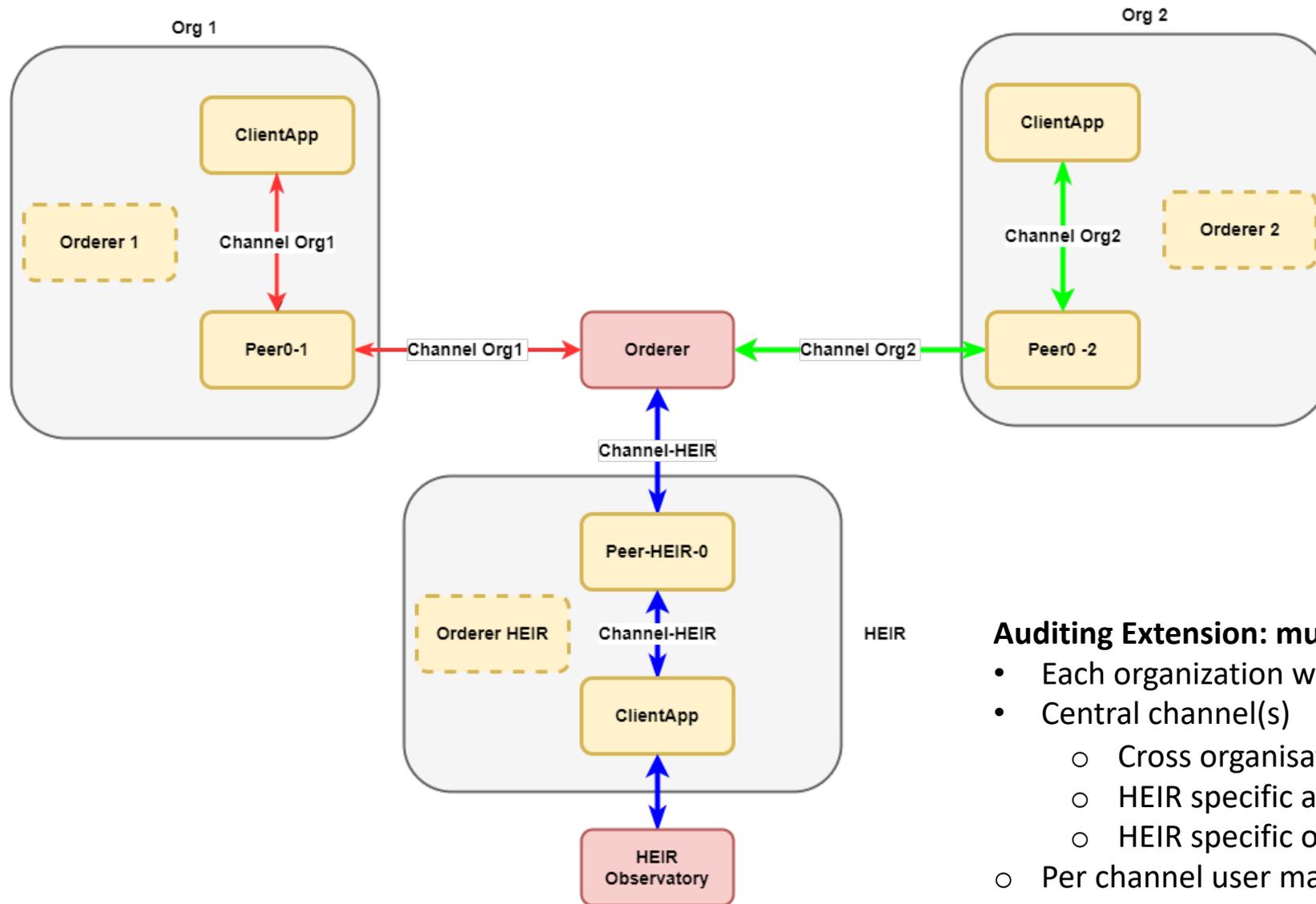
## A Blockchain-based Auditing mechanism

The auditing mechanism is designed to provide:

- Tracking of who accessed what data over time and for what purpose
- An immutable, tamper-proof record of all patient data access attempts
- Audit log isolation on a per medical institution auditing, while still enabling scenarios for cross-organization auditing
- A filtering mechanism for the identification of malicious unauthorized access attempts
- A timeline of events in the form of abnormal data access requests

Blockchain Network - Auditing Mechanism





### Auditing Extension: multi-organisation setup

- Each organization with discrete channels -> internal, isolated logs
- Central channel(s)
  - Cross organisation audit logs
  - HEIR specific audit logs
  - HEIR specific other needs
- Per channel user management and access control policies in place

# HEIR Threat Hunting

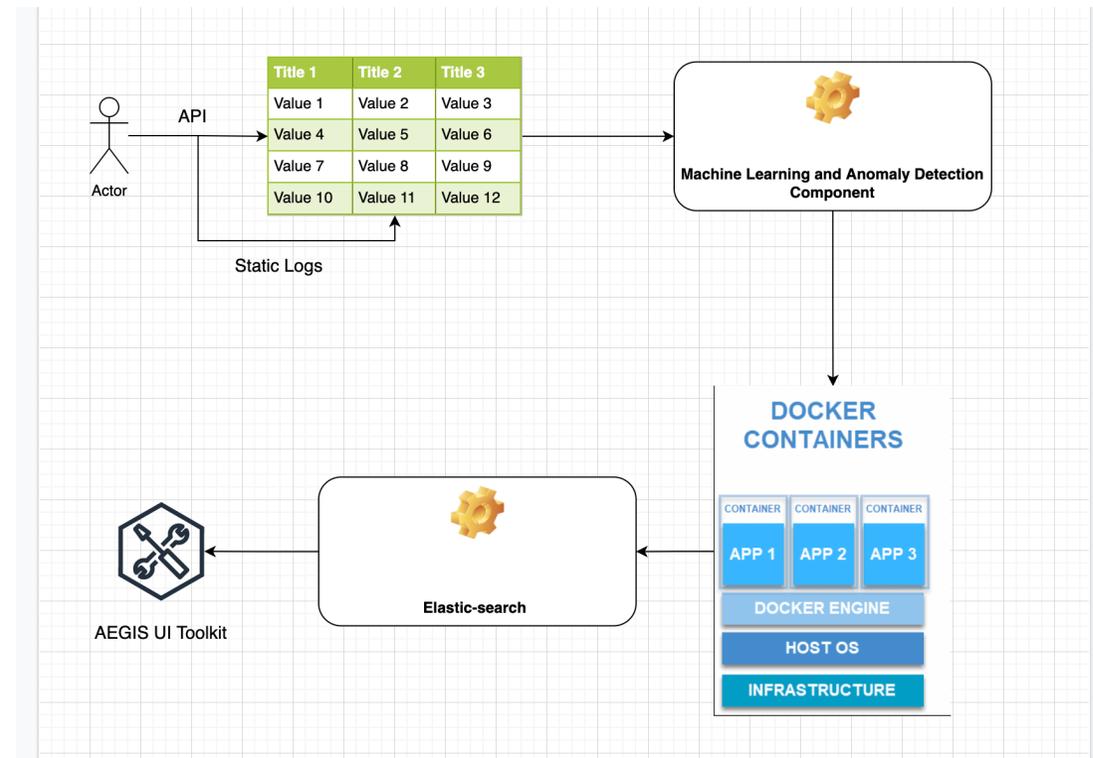


This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883275.

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.

# ML based Anomaly Detection

- Tested several supervised algorithms
- Based on the results we ended up into using the Random Forest Algorithm
- Trained the model using synthetic data (created based on actual data from one of the pilots)
- Execute the model using data from PAGNI

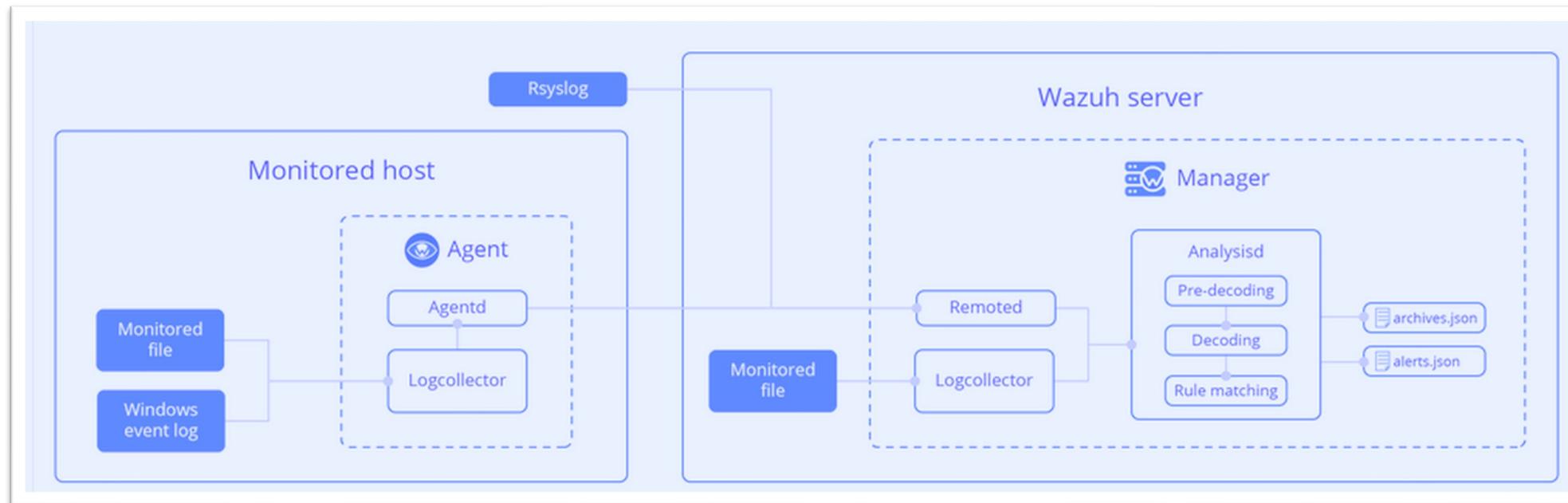


# SIEM



a secure Healthcare  
Environment for Informatics  
Resilience

- It is based on the widely established Wazuh open-source solution
- Supports multiple OS (Windows, Linux, Mac OS X, AIX, Solaris and HP-UX)
- Data is collected by lightweight agents which run on the monitored systems, collecting events and forwarding them to the Wazuh Manager, where data is aggregated, analyzed, indexed and stored.



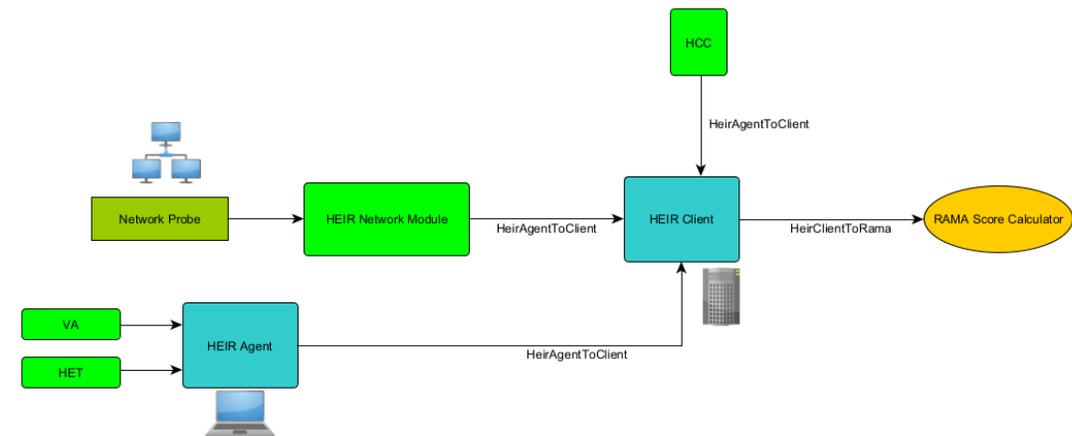
# SIEM - Key features

- The collected data support a wide range of sources
  - Inventory of running processes and installed applications
  - Log and events data collection
  - File and registry keys integrity monitoring
  - Monitoring of open ports and network configuration
  - Configuration assessment and policy monitoring
- All received events are processed through a toolset of decoders and rules, using threat intelligence to look for well-known IOCs (Indicators Of Compromise), resulting to appointment of a computed severity level to each enabling the administrators to focus on the crucial issues
- Wazuh is also able to collect and integrate logs deriving from network devices such as routers, firewalls etc. either by monitoring the log files themselves or via forwarding log messages in through Rsyslog.
- It supports a variety of plugins and provides easy integration with tools like Elastic Stack, Kibana visualization etc.



# HEIR Client

- Central aggregation component
- Collects data from
  - Facilitators
    - HEIR Agent (Application Vulnerabilities)
  - Integrated modules
    - HEIR Network Module
    - HEIR Exploit Tester (Operating System Vulnerabilities)
    - HEIR Cryptographic Checker
- Main data provider to the RAMA Score calculator



# Local and Global RAMA score

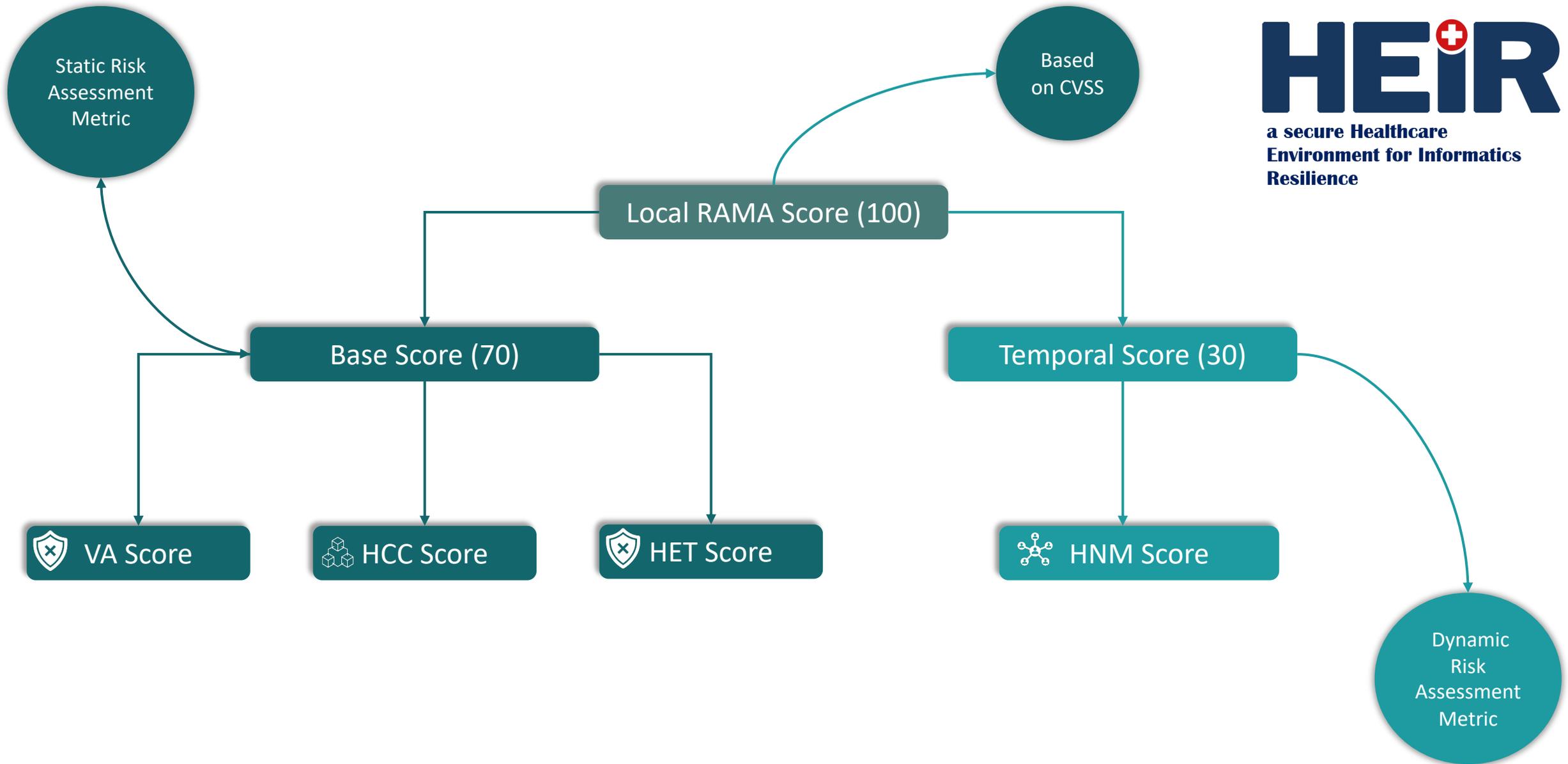


This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883275.

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.

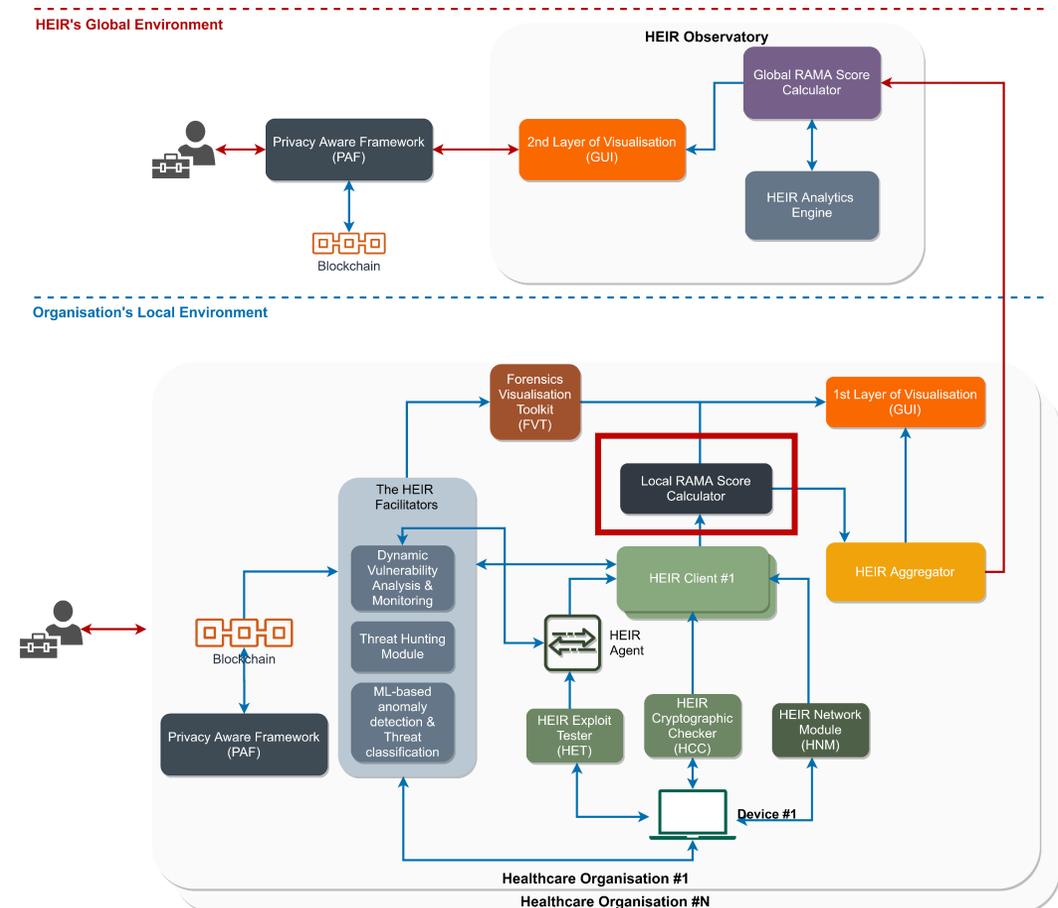
# Local RAMA score

- The Risk Assessment of Medical Applications (RAMA) score will **measure the security status** of every **medical device** and provide thorough **vulnerability assessment** of hospitals and **medical centers**
- The **calculation** of the score is based on the following components:
  - HEIR's Exploit Tester
  - HEIR's Network Module
  - HEIR's Vulnerability Assessment, and
  - HEIR's Cryptographic Checker
- The **local RAMA score** is then separated into the **base** and **temporal** score.



## Local RAMA Score Calculator

- The Local RAMA Score calculator is a component responsible to calculate the local RAMA Score, and the corresponding metadata
- It receives input from the HEIR Client and provides output to the HEIR Aggregator.

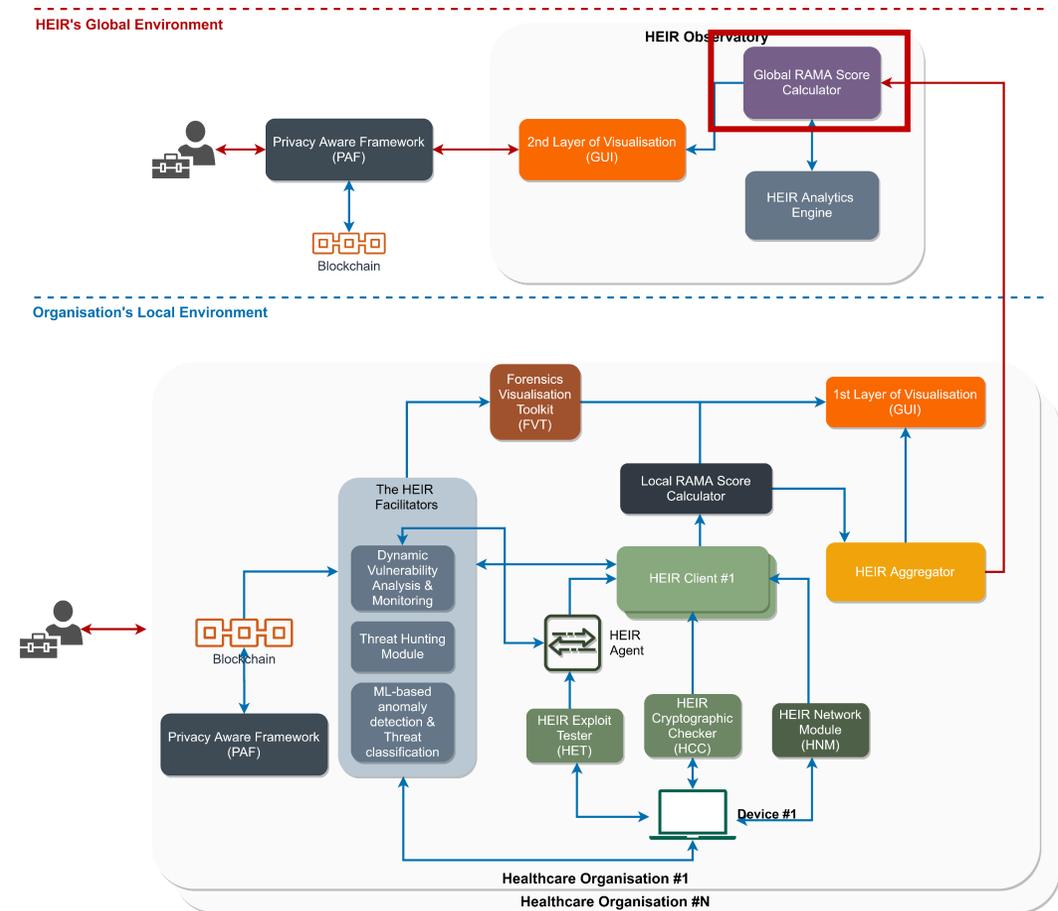


# Global RAMA score

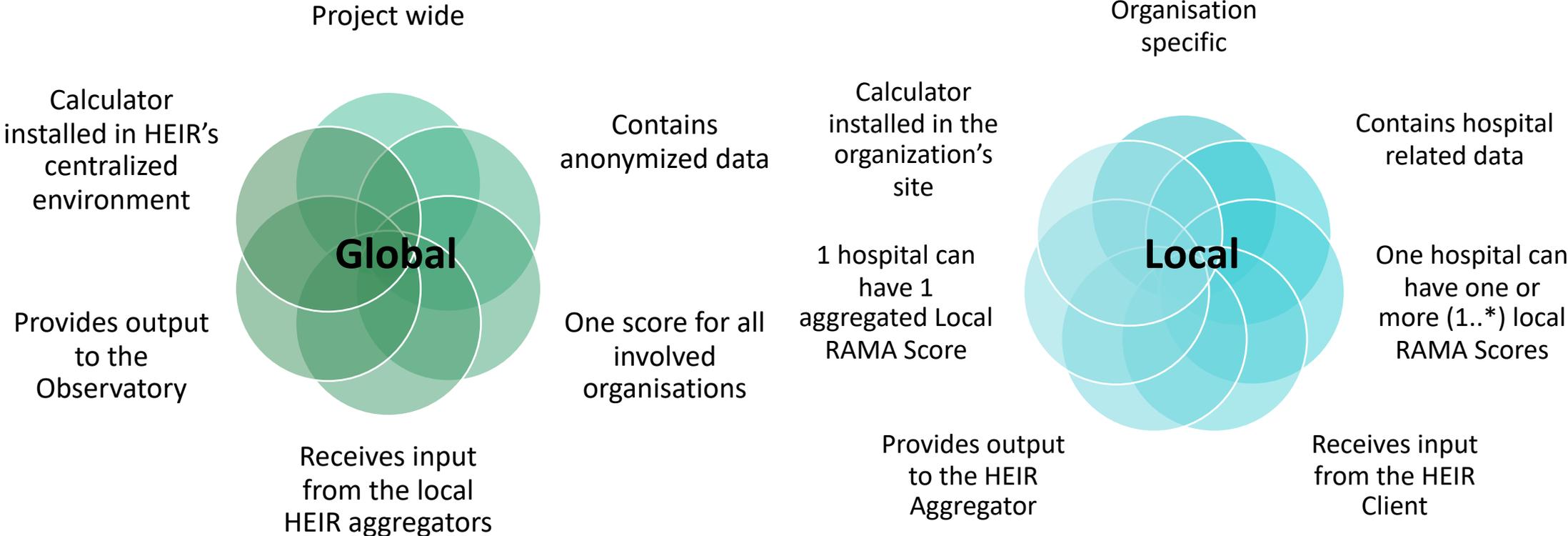
- The **global** Risk Assessment of Medical Applications (RAMA) score acts as a global benchmark against which the RAMA scores of the individual health facilities will be compared
- The **calculation** of the score is based on the **local** RAMA scores per healthcare unit
- The **global RAMA score** is also separated into the **base** and **temporal** score.

## Global RAMA Score Calculator

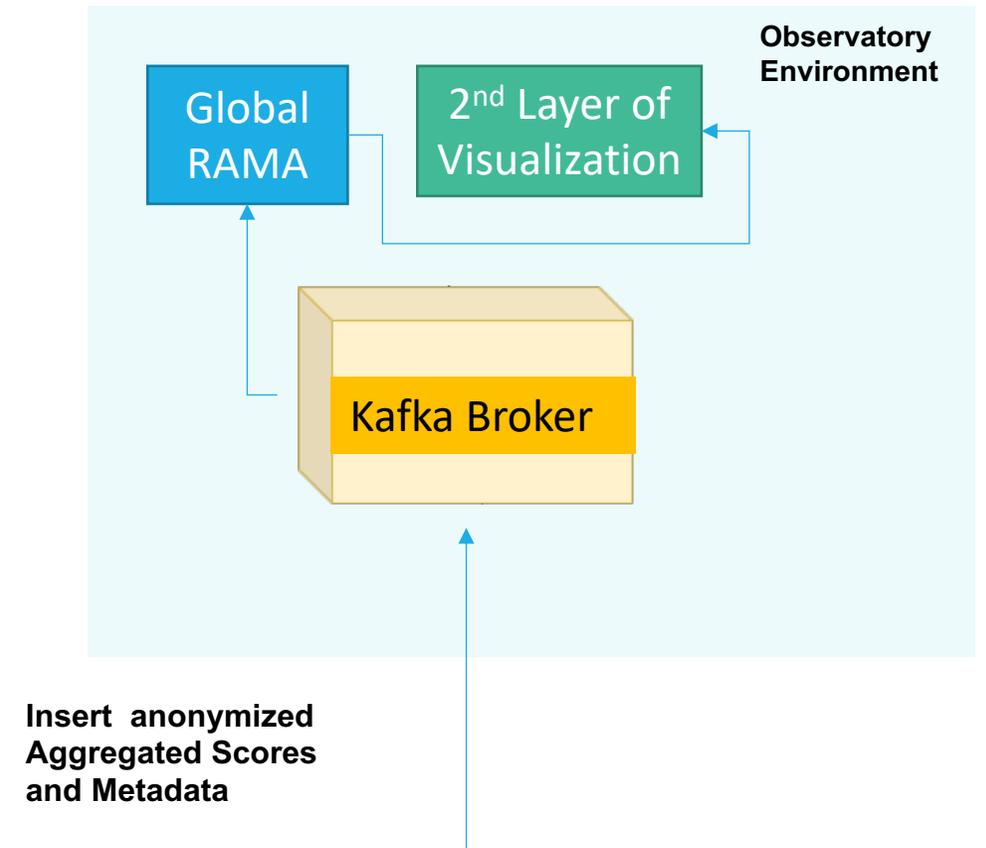
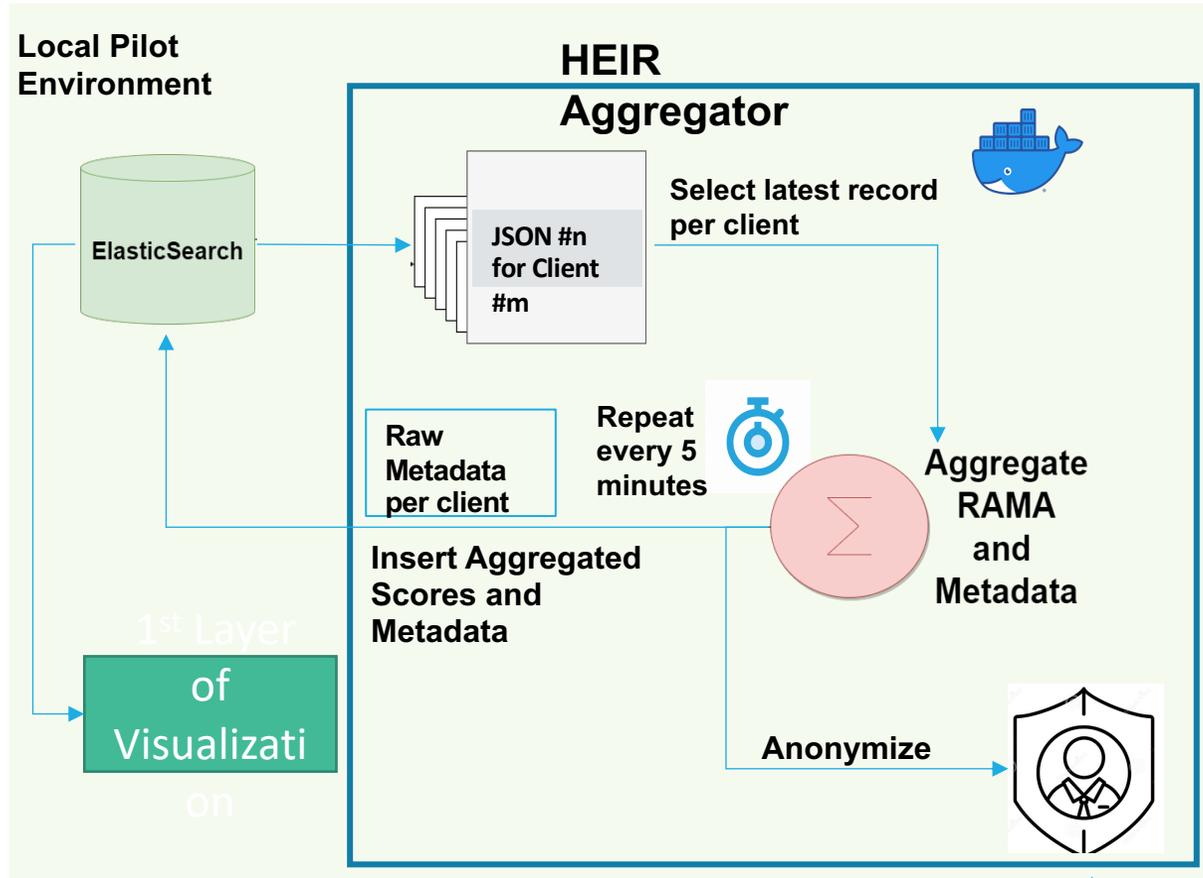
- The Global RAMA Score calculator is a component responsible to calculate the global RAMA Score, and the corresponding metadata
- It receives **anonymized input** from the HEIR Aggregator and provides output to the HEIR Observatory.



# Global vs Local RAMA Score



# HEIR Aggregator



# Visualisations



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

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.

# 1<sup>st</sup> Layer GUI and FVT



**HEiR - PAGNI** AEGIS FVT

Events Analysis - Department: **Nephrology Clinic**

Filter Devices: Events | Filter ML Events

Device: Select Device | Classification: Anomalies | Apply

Security: S: 6 x 4 Items | Show until date: 4/19/2022, 13:22:21 | Show until date: 4/19/2022, 01:27:54 | Search | Last 344

Temporal Representation | Stacked View

Inspect device: Select Device | Inspect

Timeline (Mon 18 April to Tue 19 April):

- 19:00: Update Department (Anomaly)
- 21:00: Host-based anomaly (Anomaly)
- 14:00: Windows System on (Anomaly)
- 14:00: Windows Application (Anomaly)
- 14:00: The Open Procedure (Anomaly)
- 16:00: System time changed (Anomaly)

ML Events Details

Filter	Rule	Action	Timestamp	Anomaly	Anomaly probability
	Doctor	Update Department Data	18/04/2022, 19:21:25	YES	2.2811577246855

Items per page: 5 | 1 - 1 of 1

Devices' Events Details

Filter	Device	Timestamp	Severity	Description	Message
	mtn-dc02	18/04/2022, 21:09:05	7	Host-based anomaly detection event (notcheck)	NTFS Alternate data stream found: 'C:\Program Files\AMC\Win32App,1'. Possible hidden content.
	mtn-dc02	18/04/2022, 21:09:05	7	Host-based anomaly detection event (notcheck)	NTFS Alternate data stream found: 'C:\Program Files\Hospital 2003\Win32App,1'. Possible hidden content.
	mtn-dc02	18/04/2022, 21:09:05	7	Host-based anomaly detection event (notcheck)	NTFS Alternate data stream found: 'C:\Program Files\Vermpol\Win32App,1'. Possible hidden content.
	mtn-dc02	18/04/2022, 21:09:05	7	Host-based anomaly detection event (notcheck)	NTFS Alternate data stream found: 'C:\Program Files\vuim\Win32App,1'. Possible hidden content.
	mtn-dc02	18/04/2022, 21:09:05	7	Host-based anomaly detection event (notcheck)	NTFS Alternate data stream found: 'C:\Program Files\UNP\Win32App,1'. Possible hidden content.

Items per page: 5 | 1 - 5 of 18

**HEiR**

Hospital Region: PAGNI | Critical Events: 1  
Address: Street no 1 | Security Risk Level: Low  
Connected Clients: 5 | Reported: Apr 18, 2022, 8:55:40 AM

Global RAMA - 84.23  
Avg Critical Events: 1  
Risk Frequency Risk Level: Low  
Connected Hospital: 1

RAMA Score: 84.23  
Temporal: 0  
Base: 8.18

RAMA Indicators & Scores

- HER Network Module [NEM]: 0
- Vulnerability Assessment [VA]: 7.26
- HER Exploit Tester [HET]: 2.14
- HER Cryptographic Checker [CC]: 0

RAMA Infographics

RAMA Scores evolution

Generic Statistics

Aggregated Clients Measures				
[NEM] Identified Heartbeats	[VA] Application Vulnerabilities	[NEM] Total Findings Attacks Exploits	[HET] OS Vulnerabilities	Misconfigurations
0	37	0	0	11

DIET: Total Events Analysis

- Malicious Findings: 16.9%
- Bumpy Findings: 83.1%

Connected Clients

**Nephrology Clinic**  
Security Risk Level: Low  
RAMA Score: 98.31

- Critical Events: 1
- Identified Heartbeats: 0
- App Vulnerabilities: 0
- Total Findings: 0

**General surgery Clinic**  
Security Risk Level: Low  
RAMA Score: 100

- Critical Events: 0
- Identified Heartbeats: 0
- App Vulnerabilities: 1
- Total Findings: 0

**Pulmonology Clinic**  
Security Risk Level: Low  
RAMA Score: 99.47

- Critical Events: 0
- Identified Heartbeats: 0
- App Vulnerabilities: 0
- Total Findings: 0

**Gastroenterology Clinic**  
Security Risk Level: Low  
RAMA Score: 99.61

- Critical Events: 0
- Identified Heartbeats: 0
- App Vulnerabilities: 0
- Total Findings: 0

**Otorhinolaryngology Clinic**  
Security Risk Level: Medium  
RAMA Score: 73.79

- Critical Events: 0
- Identified Heartbeats: 36
- App Vulnerabilities: 0
- Total Findings: 0





## Thank you!

