HEIR

a secure Healthcare Environment for Informatics Resilience

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.

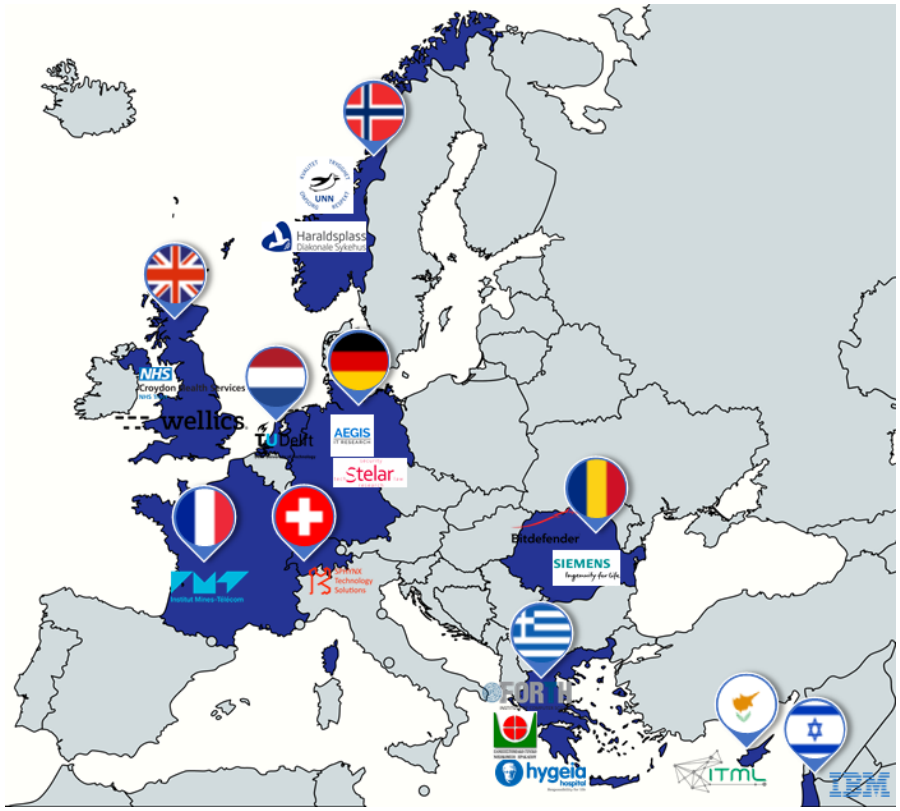
Summary

HEIR
a secure Healthcare Environment for Informatics Resilience

- 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.

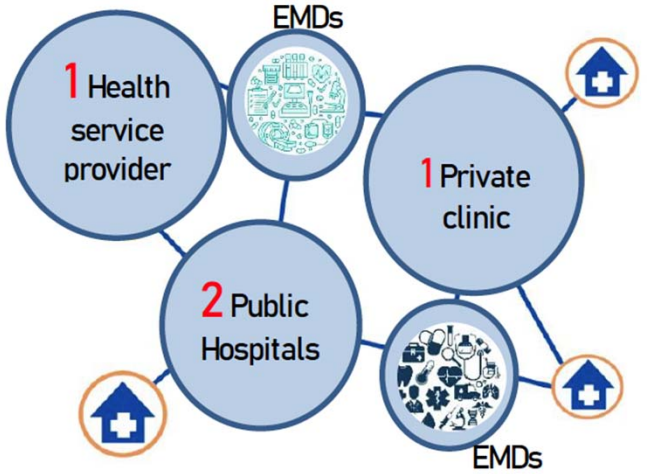
General information

HEIR
a secure Healthcare Environment for Informatics Resilience



The validation ecosystem

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



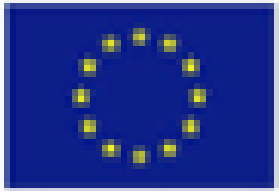
HEIR Vision: comprehensive framework

HEIR
a secure Healthcare Environment for Informatics Resilience

- 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

HEiR
a secure Healthcare
Environment for Informatics
Resilience

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

HEIR
a secure Healthcare Environment for Informatics Resilience

- 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.

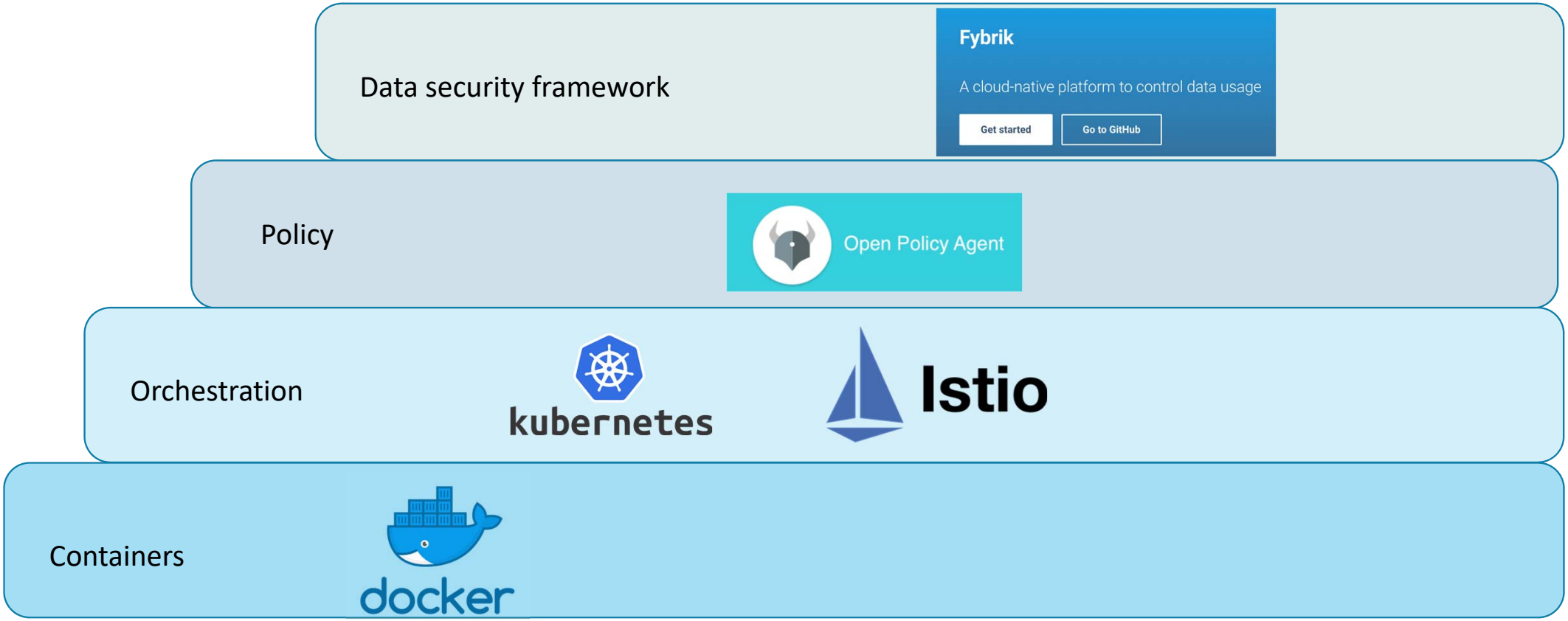
The Concept

HEIR
a secure Healthcare Environment for Informatics Resilience

- 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”

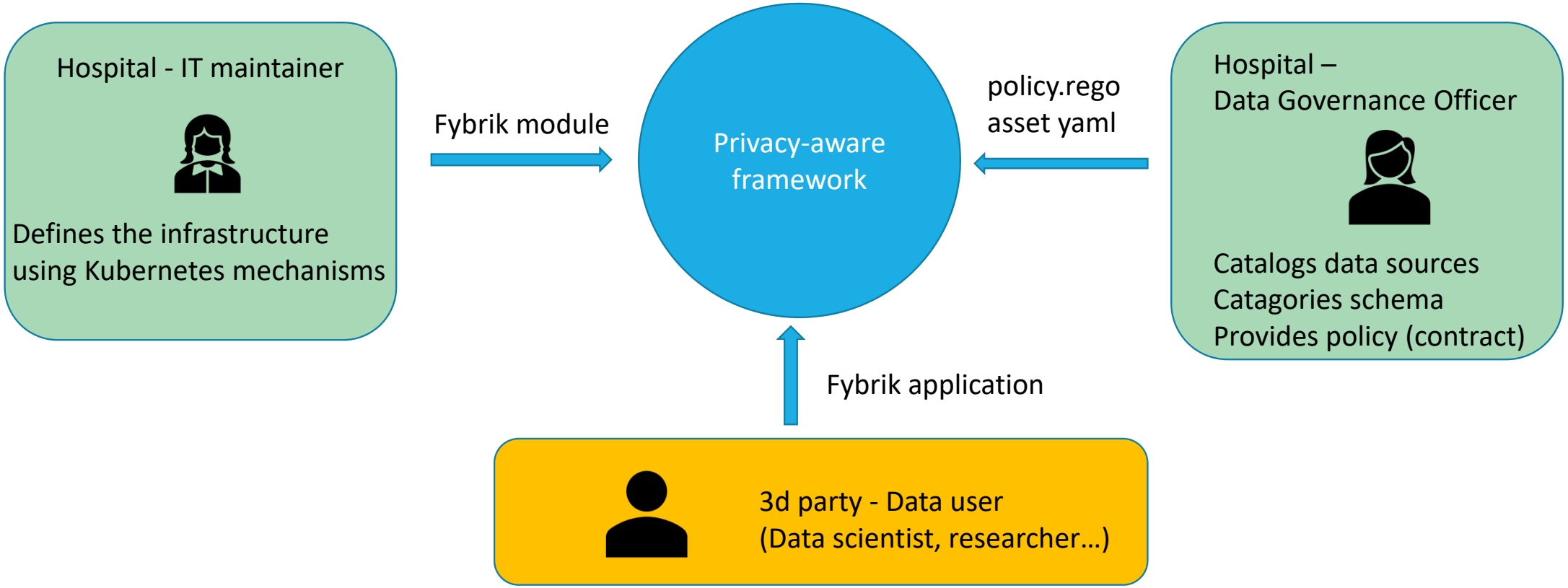
The Starting Point

HEIR
a secure Healthcare Environment for Informatics Resilience



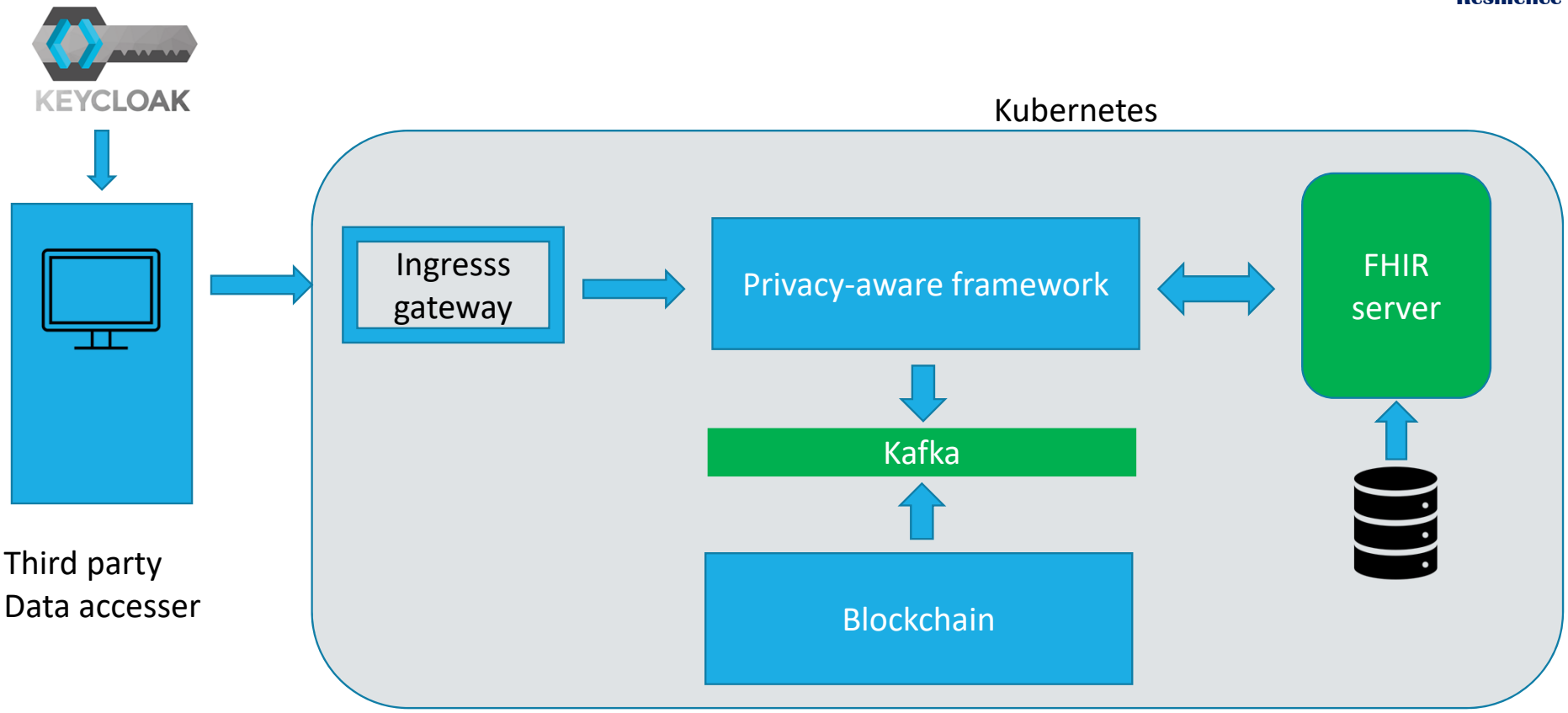
Configuring the PAF in a hospital

HEIR
a secure Healthcare Environment for Informatics Resilience



Conceptual Architecture

HEIR
a secure Healthcare Environment for Informatics Resilience



The problem

HEIR
a secure Healthcare Environment for Informatics Resilience

- 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?

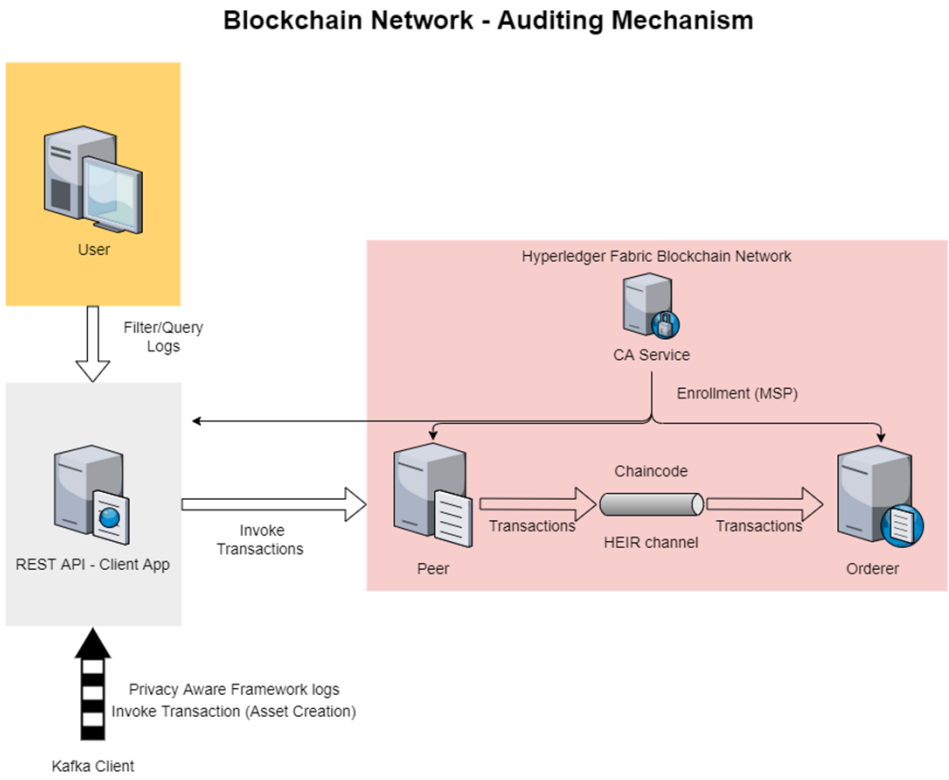
HEIR's solution

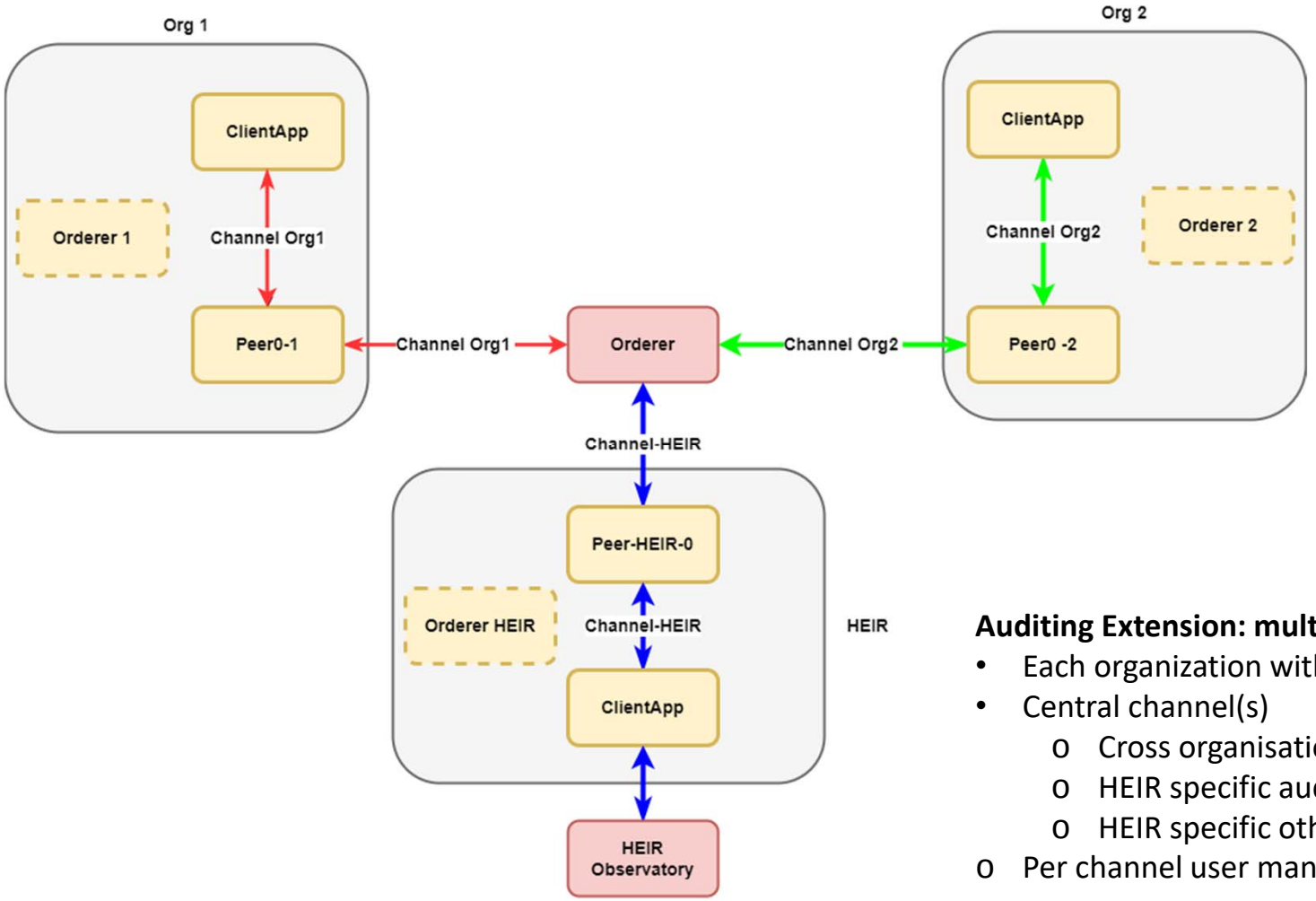
a secure Healthcare Environment for Informatics Resilience

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





a secure Healthcare Environment for Informatics Resilience

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

a secure Healthcare
Environment for Informatics
Resilience

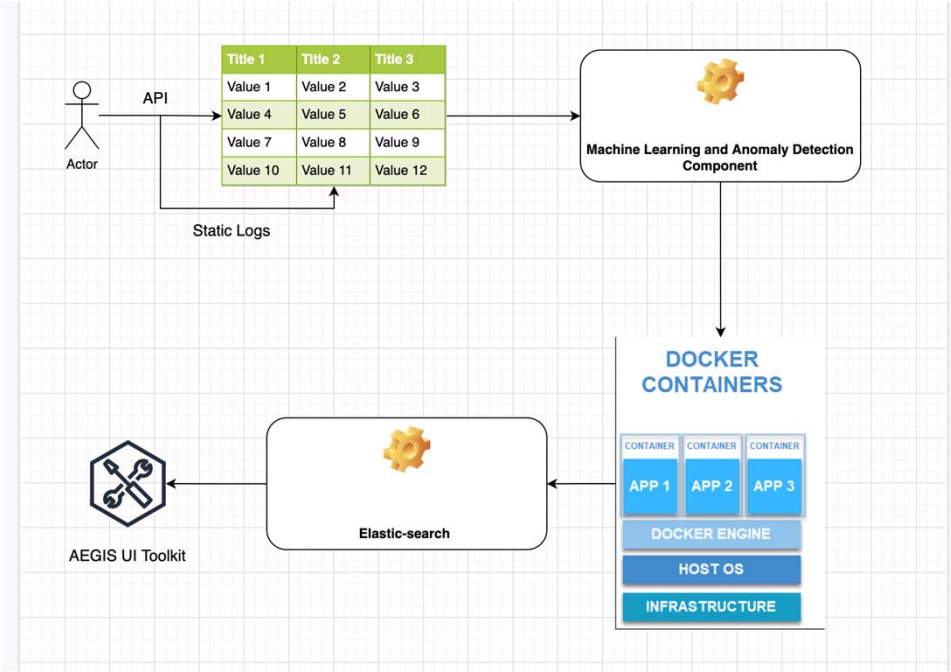
HEIR Threat Hunting

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

HEIR
a secure Healthcare Environment for Informatics Resilience

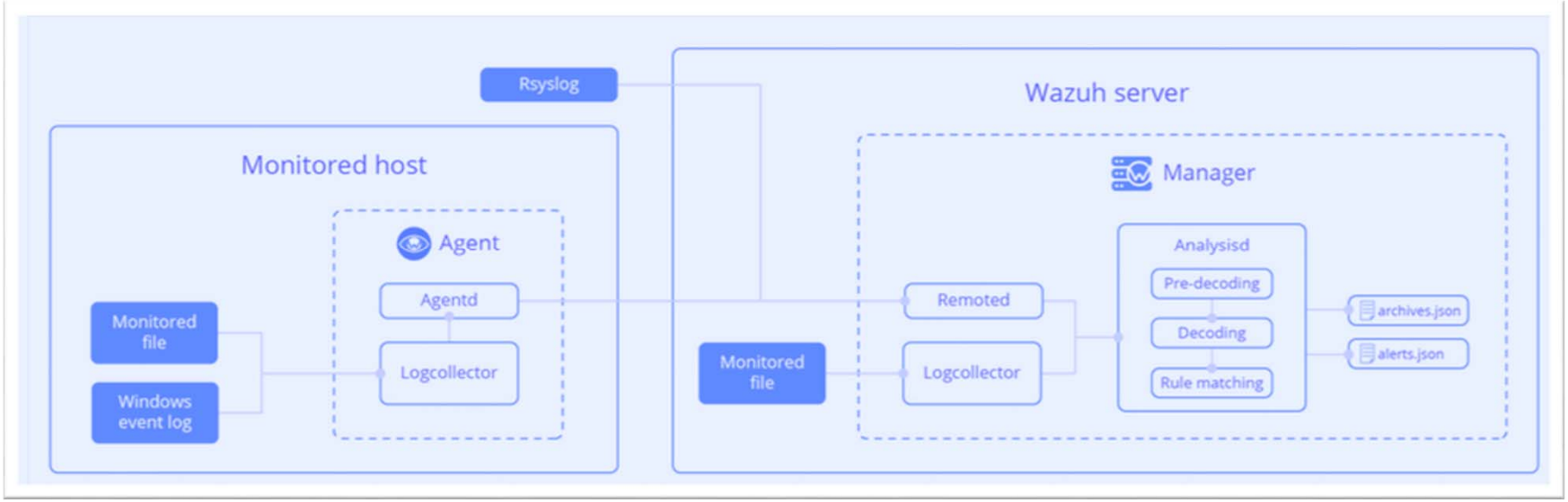
- Tested several supervised algorithms
- Based on the results we ended up into using the Random Forest Algorithm
- Trained the model using synthetic data (created based on actual data from one of the pilots)
- Execute the model using data from PAGNI



SIEM

HEIR
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

HEIR
a secure Healthcare Environment for Informatics Resilience

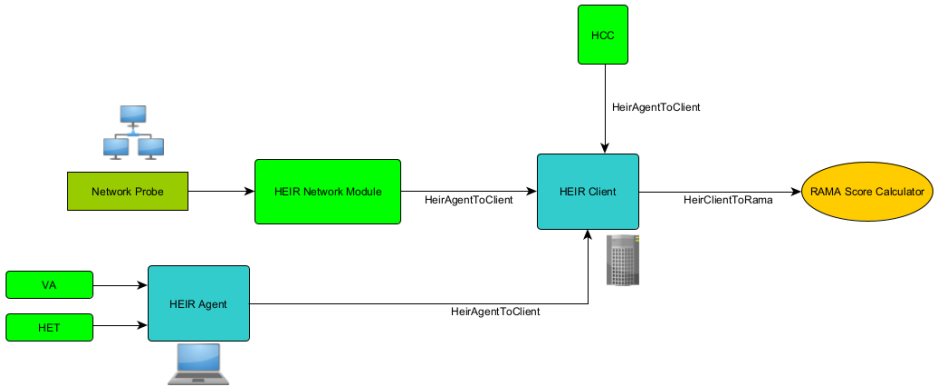
- The collected data support a wide rage of sources
  - Inventory of running processes and installed applications
  - Log and events data collection
  - File and registry keys integrity monitoring
  - Monitoring of open ports and network configuration
  - Configuration assessment and policy monitoring

- 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

a secure Healthcare Environment for Informatics Resilience

- 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



HEiR
a secure Healthcare
Environment for Informatics
Resilience

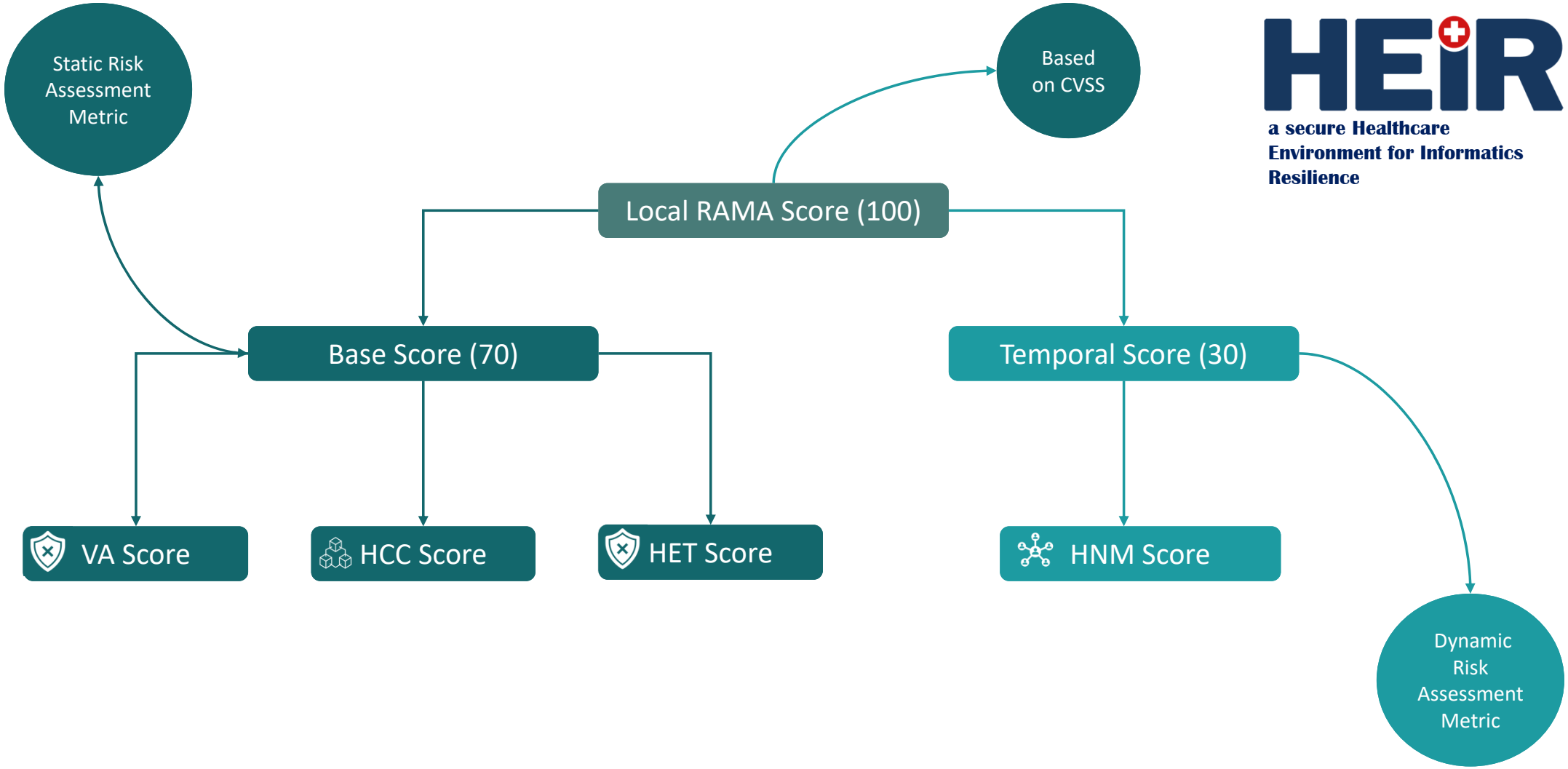
Local and Global RAMA score

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

HEIR
a secure Healthcare Environment for Informatics Resilience

- 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.

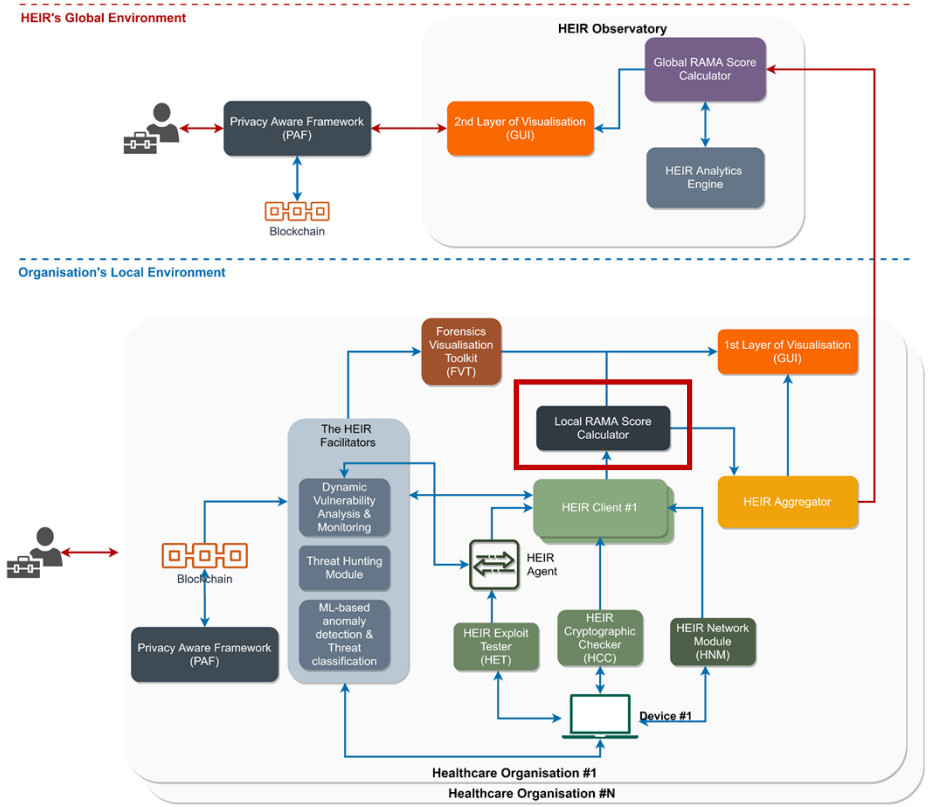


HEIR
a secure Healthcare Environment for Informatics Resilience

Local RAMA Score Calculator

HEIR
a secure Healthcare Environment for Informatics Resilience

- 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

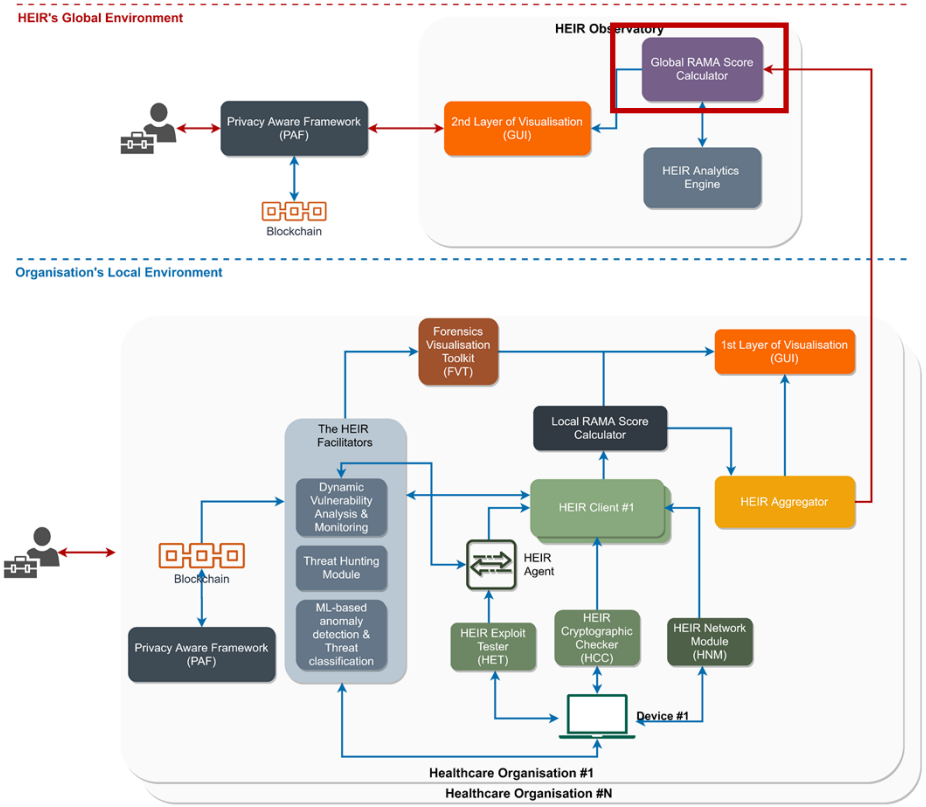
HEIR
a secure Healthcare Environment for Informatics Resilience

- 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

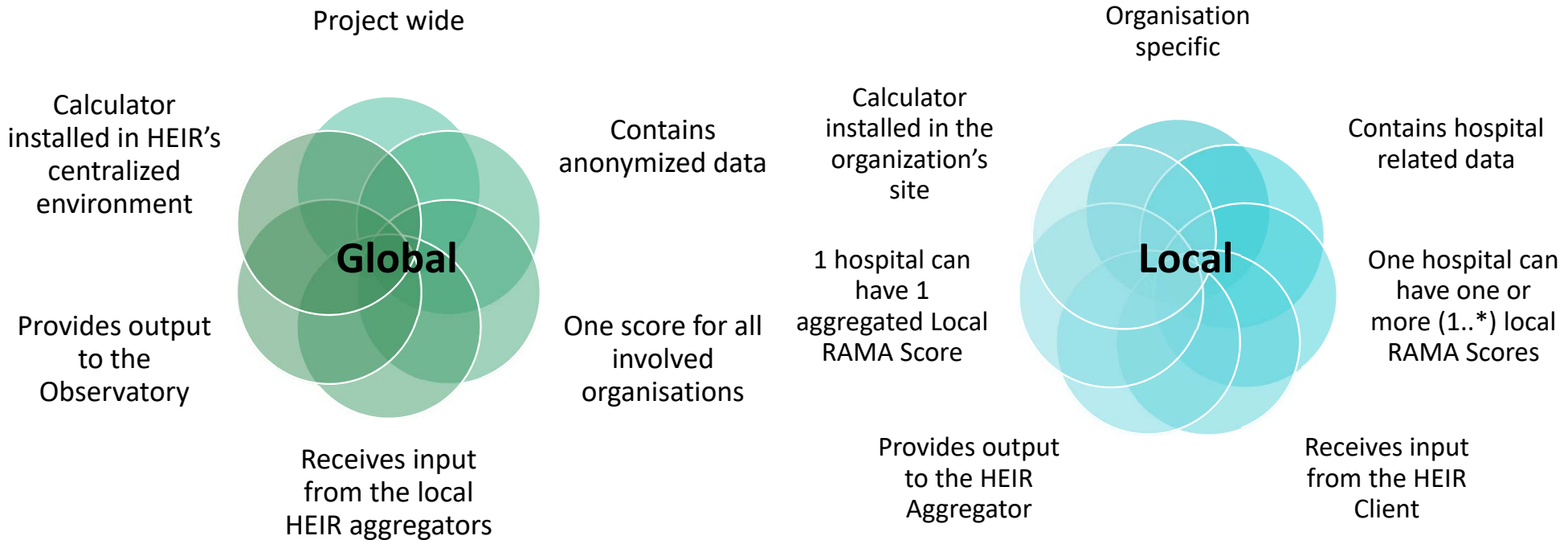
HEIR
a secure Healthcare Environment for Informatics Resilience

- 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.

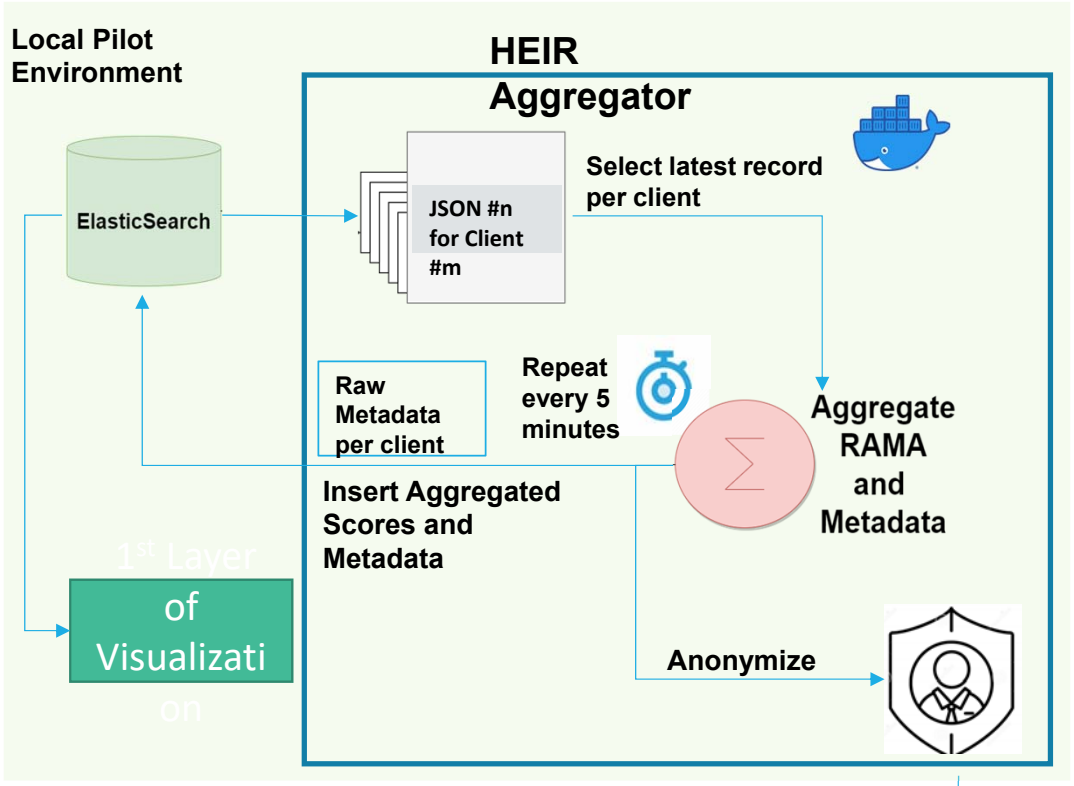


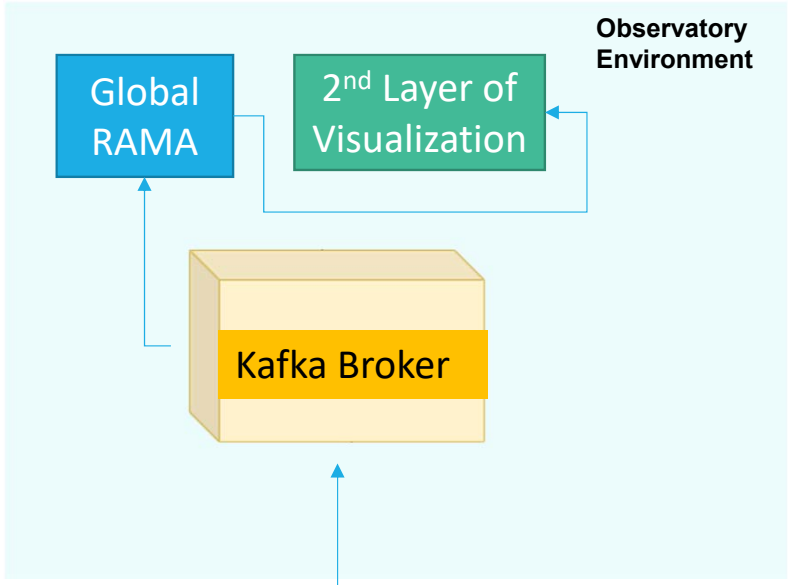
Global vs Local RAMA Score

a secure Healthcare Environment for Informatics Resilience



HEIR Aggregator





Insert anonymized Aggregated Scores and Metadata

HEiR

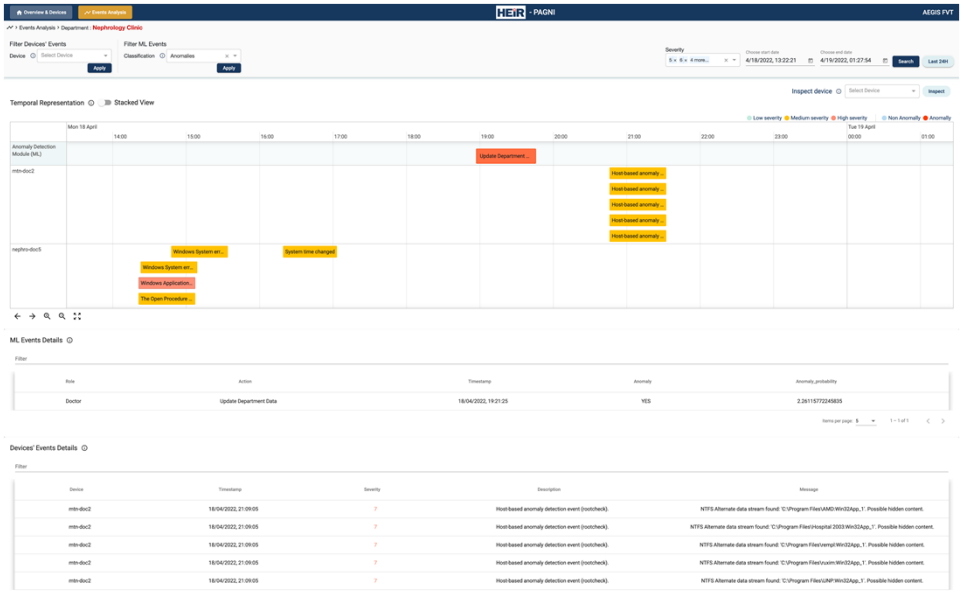
a secure Healthcare Environment for Informatics Resilience

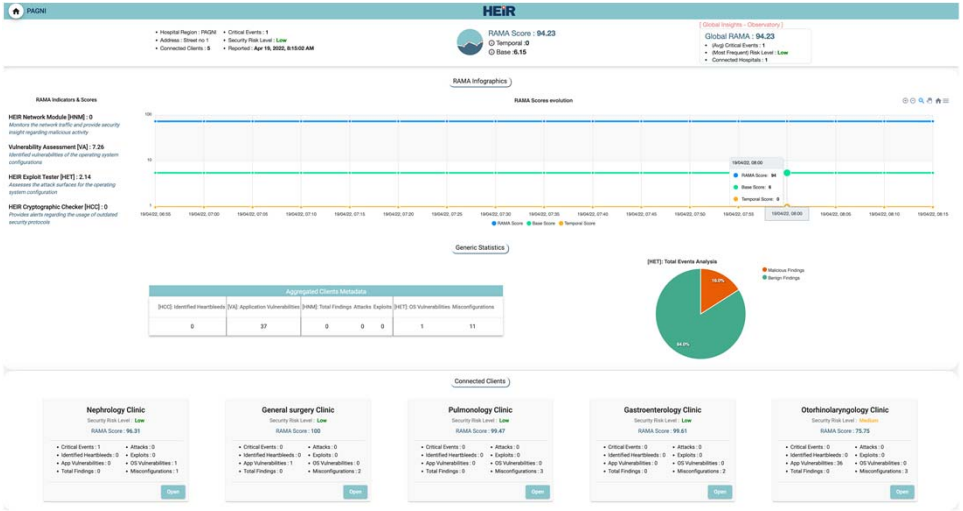
Visualisations

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.

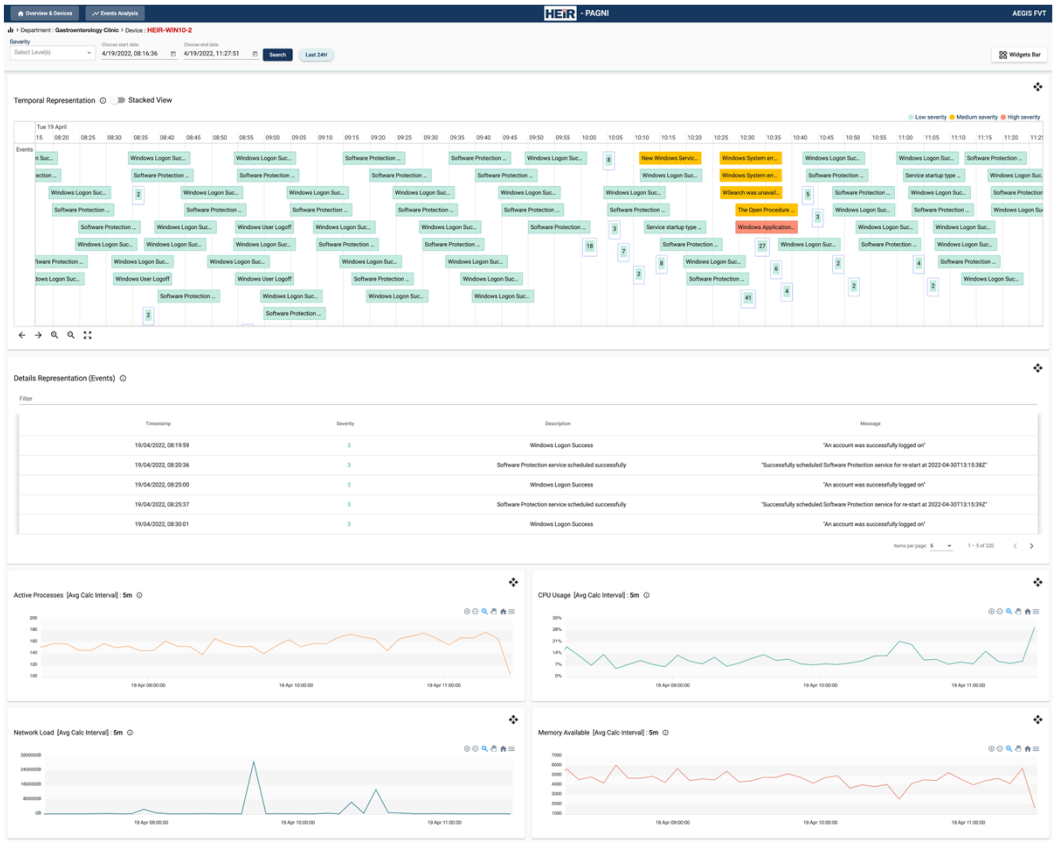
1st Layer GUI and FVT

a secure Healthcare Environment for Informatics Resilience





FVT : Device Inspection



a secure Healthcare Environment for Informatics Resilience

HEIR

a secure Healthcare Environment for Informatics Resilience

Thank you!