CONCORDIA

Cyber security cOmpeteNCe fOr Research anD InnovAtion

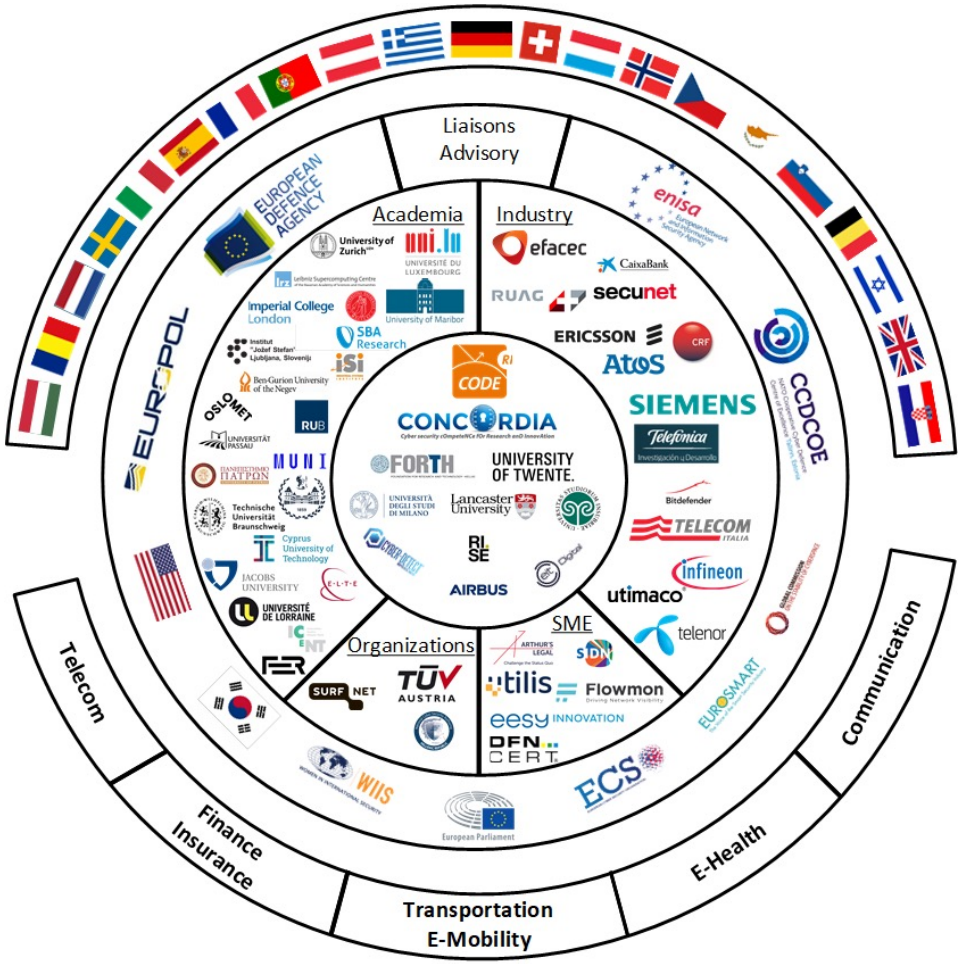
The leaders for boosting Europe's cybersecurity future

Christos Papachristos
cpapachr@ics.forth.gr
FORTH

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 830927.

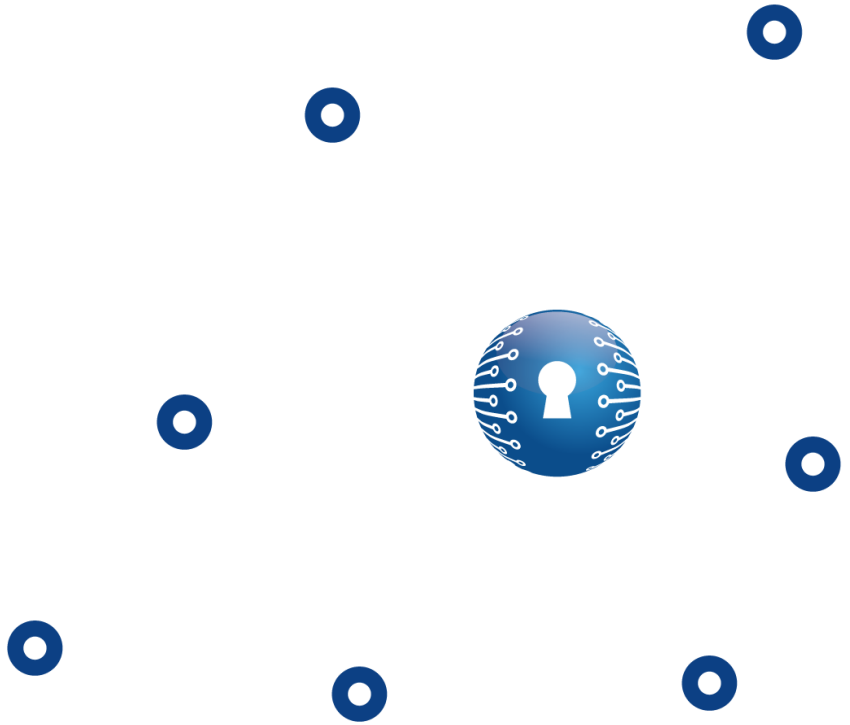
Consortium

- Current consortium with 56 official partners:
  - 30 research organisations or academia
  - 24 industry partners (including 7 SMEs)
  - 2 public body and other types of organisations
- Representing **17 EU member states** and **3 Horizon 2020 associated** countries and UK



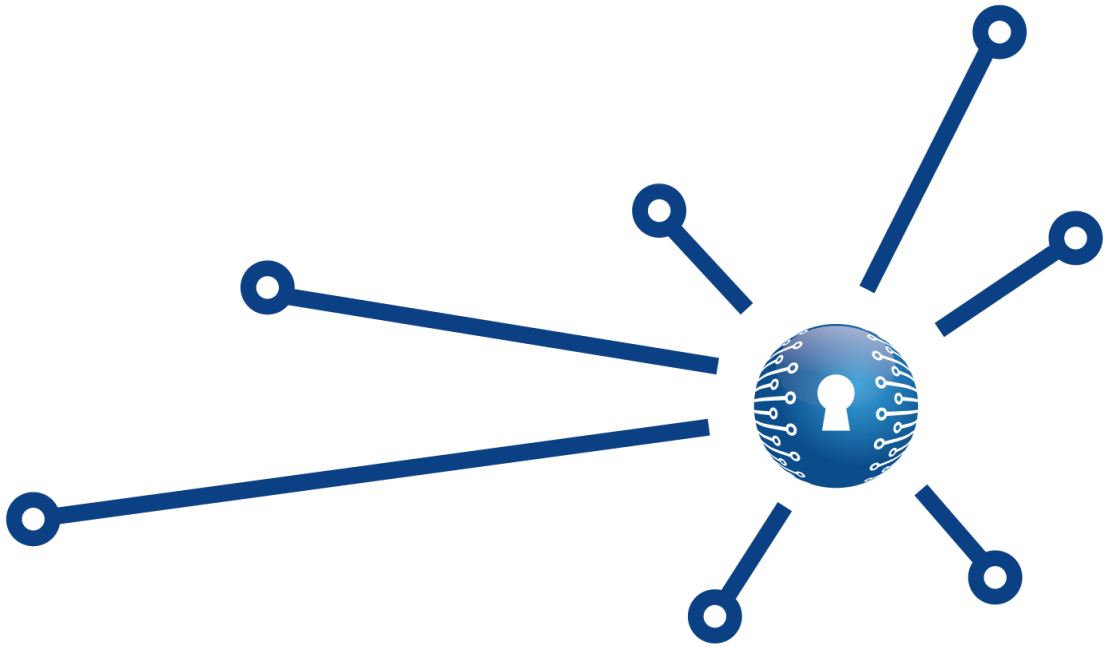
Vision

Integration of available but still fragmented European cybersecurity competences



Vision

Into a strong
European Cybersecurity Competence Network



CONCORDIA's Objectives

- Build and position CONCORDIA as European Secure, Resilient and Trusted Cybersecurity Ecosystem
- Bringing (technical, legal, economical) expertise to European policy makers and industry
- Providing CONCORDIA's cybersecurity roadmap for Europe

CONCORDIA's Objectives

- Developing new, innovative market ready cybersecurity solutions

- Support the development and validation of cybersecurity products by providing the necessary infrastructure (virtual labs and services)

- Establishing an European Education Ecosystem for Cybersecurity (modern training courses, competitions, cyber ranges)

The CONCORDIA pilots

T2.1	T2.2	T2.3	T2.4	T2.5
Telco	**Finance**	**eMobility**	**eHealth**	**Mobile Communication**
Use cases: • TI Automated processing • Preventing IoT Flooding • Protection of privacy data	Use cases: • Financial Threat Intelligence Platform. • Federated Machine Learning for Financial Sector Threat Intelligence. • Collaborative improvement of KYC	Use cases: • Securing the network of IoT devices in Logistics and Manufacturing • Efficient and secure Monitoring and certification of inbound logistics for EV battery pack • Automated aerial delivery of components in compound	Use cases: • Remote health service from home • Emergency health service	Use cases: • Secure authentication • Trusted interaction • Ad-hoc networking

The CONCORDIA pilots

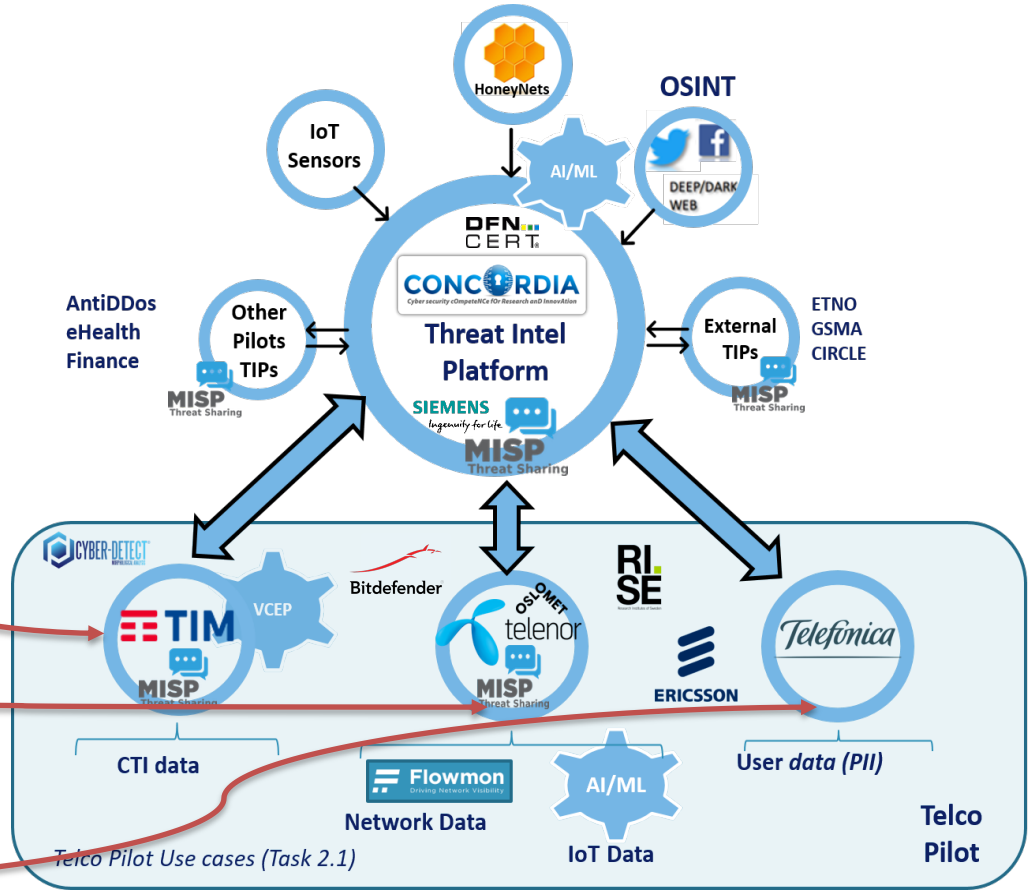
T2.1	T2.2	T2.3	T2.4	T2.5
Telco	**Finance**	**eMobility**	**eHealth**	**Mobile Communication**
Use cases: • TI Automated processing • Preventing IoT Flooding • Protection of privacy data	Use cases: • Financial Threat Intelligence Platform. • Federated Machine Learning for Financial Sector Threat Intelligence. • Collaborative improvement of KYC	Use cases: • Securing the network of IoT devices in Logistics and Manufacturing • Efficient and secure Monitoring and certification of inbound logistics for EV battery pack • Automated aerial delivery of components in compound	Use cases: • Remote health service from home • Emergency health service	Use cases: • Secure authentication • Trusted interaction • Ad-hoc networking

Telco Pilot

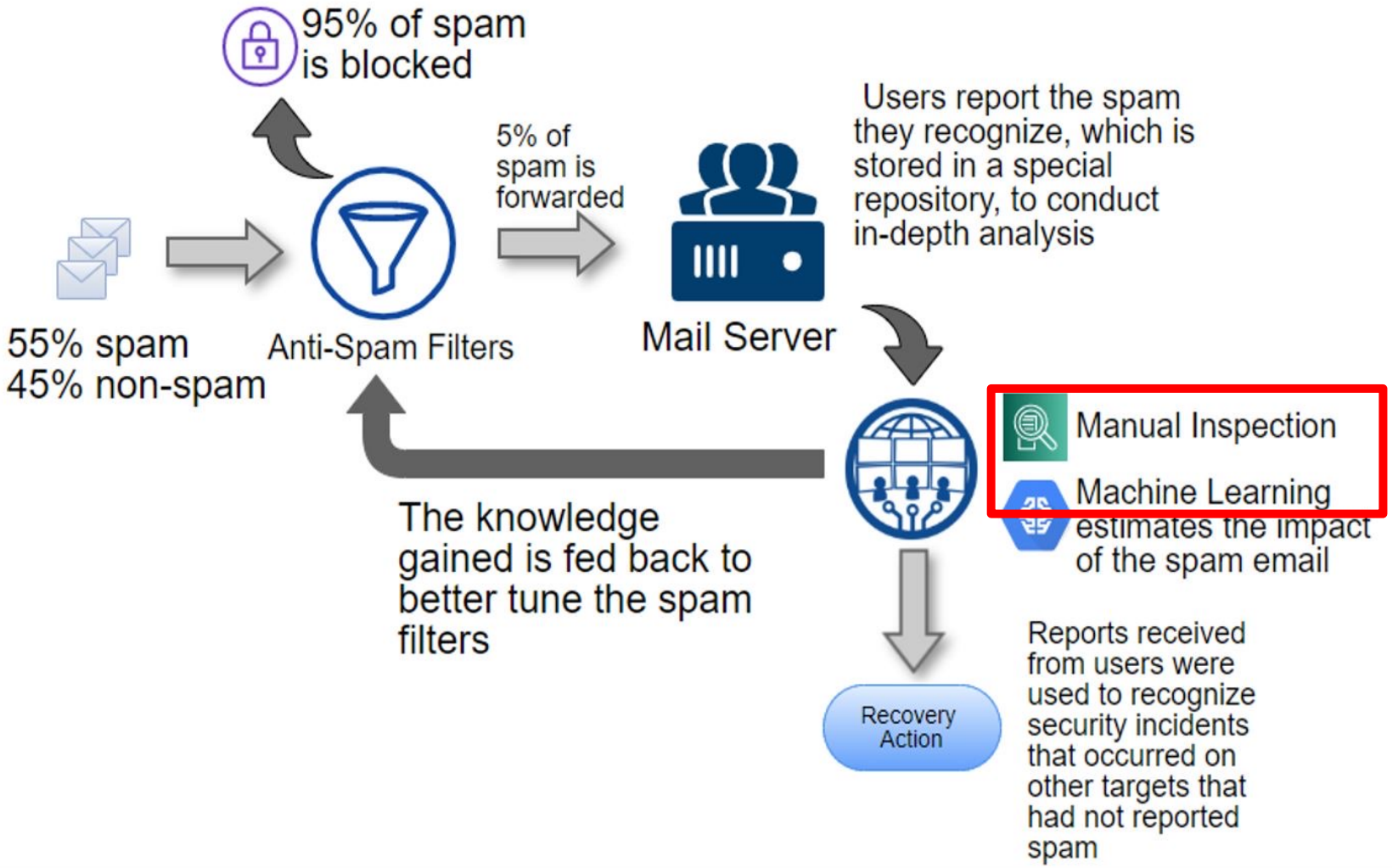
CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

Main Objective

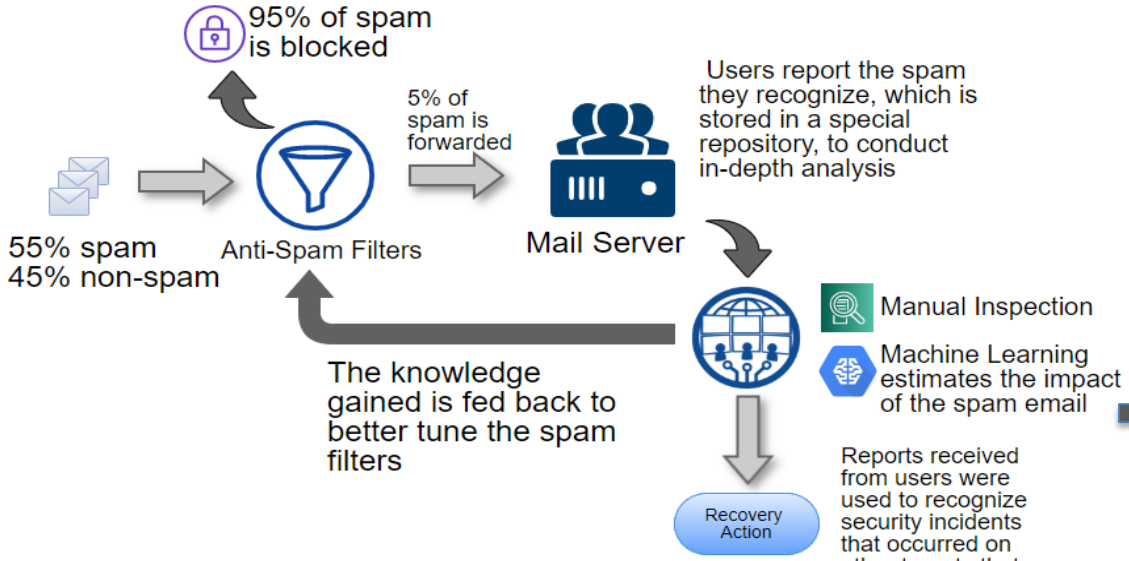
- Extend and enhance the CONCORDIA Threat Intelligence Platform with 3 use cases;
- TI Automated processing
- Preventing IoT Flooding
- Protection of privacy data



Automated Processing of TI Information: Scenario

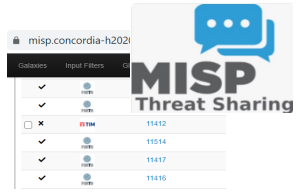


Automated Processing of TI Information



Prototype implementation of ML-based IoC prioritization for consumption

Threat Intel Platform



misp.concordia-h2020.eu

E-Health Pilot

Paradigm Shift

	In the past	In the future
Aging society	In **hospitals**, IT-systems and medical devices must be protected	In **smart home: secure** data acquisition and **secure** data transmission to hospitals, clinics and family doctor´s;
Ambulance services	Vehicle for **transportation**	Vehicle for • 1st **patient analyzing** and • 1st **aid treatments** („mobile hospital on 4 wheels“)

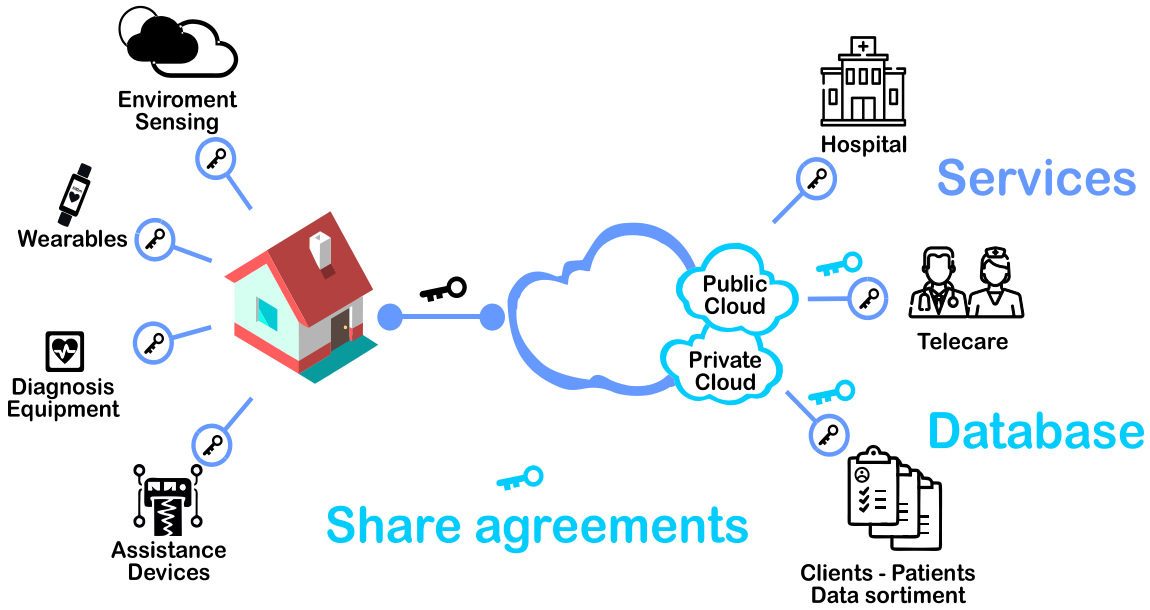
Key inputs for CONCORDIA:

- Impact for smart home: creeping transition from **health-tech** (healthcare) to **wearables** (wellness)
- Impact for emergency: shifting from **stationary** medical products to **smart and mobile** medical products

Remote health service from home

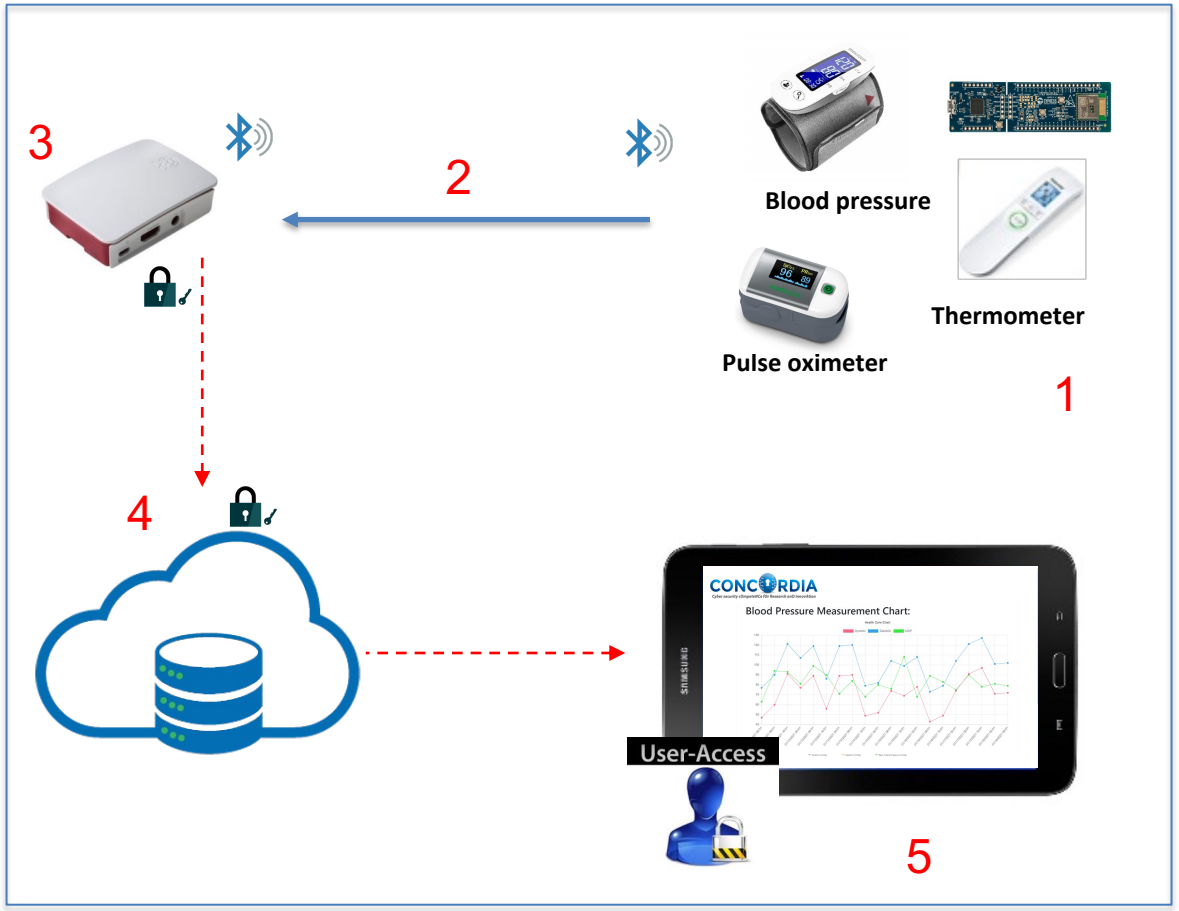
Security aspects:

- on **device** level
  - medical devices, wearables, mobile phones …
- on **person/patient data**
  - e.g. client authentication
- on **IT/network**
  - LAN
- on **Web, Cloud** connection/services
  - e.g. remote data sharing

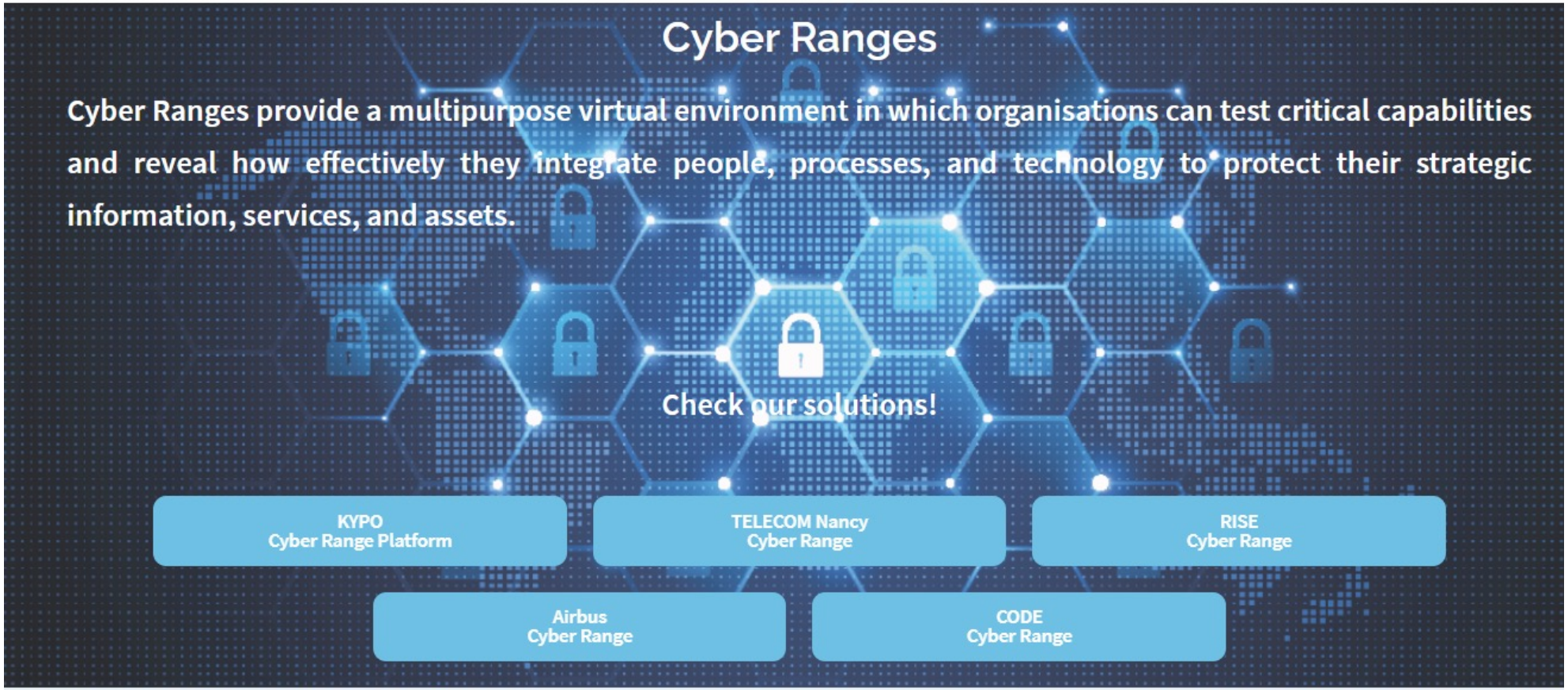


Demonstrator - overview

1. Step: Patient measures blood pressure, temperature, blood oxygen saturation, pulse.
2. Step: Device sends measurements to Smart Home Gateway via Bluetooth communication.
3. Step: Measurement data are secured in Gateway.
4. Step: Secured patient measurements are sent to Servers and saved in database.
5. Step: User/Doctor sees measurements displayed in graphic by securely accessing server.



CONCORDIA Virtual Labs



https://www.concordia-h2020.eu/#cyberrange

concordia-h2020.eu

twitter.com/**concordiah2020**

linkedin.com/in/**concordia-h2020**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 830927.