



# SECANT

## **SECurity And privacy protectionN in Internet of Things devices**

Christiana Kyperounta, SECANT's Dissemination Manager



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101019645

Project Presentation

# SECurity And privacy protection in internet of Things devices



**SECANT**, an EU-H2020 project aimed to strengthen the understanding of risks, at both human and technical level through the delivery of a holistic framework for cyber security risk assessment for enhancing the digital security, privacy, and personal data protection in complex ICT infrastructures, such in the healthcare ecosystem.

A Project coordinated by **NTT DATA**



# SECANT Key facts



H2020- SU-DS02-2020 call  
 Sub-topic (b): Cyber-threat information sharing and analytics



19 partners from 9 countries

- 3 Large ICT industries



- 9 SMEs



- 5 research institutes and universities



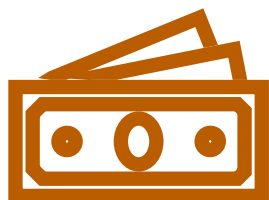
- 1 Healthcare organization



- 1 European CERT



Duration: 36 months  
 Starting date: 1 September 2021  
 Ending date: 31 August 2024

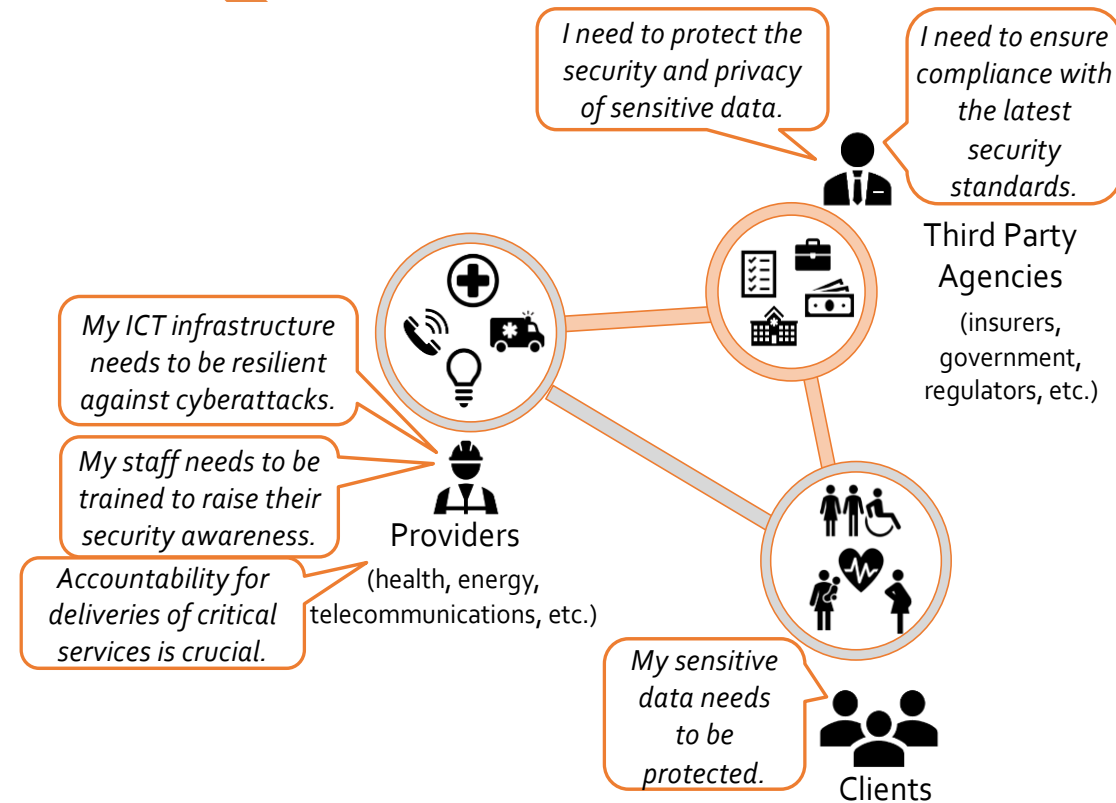


Budget 6.567.958,75 €  
 EU funding 5.202.226,38 €



# Context and Main Aim

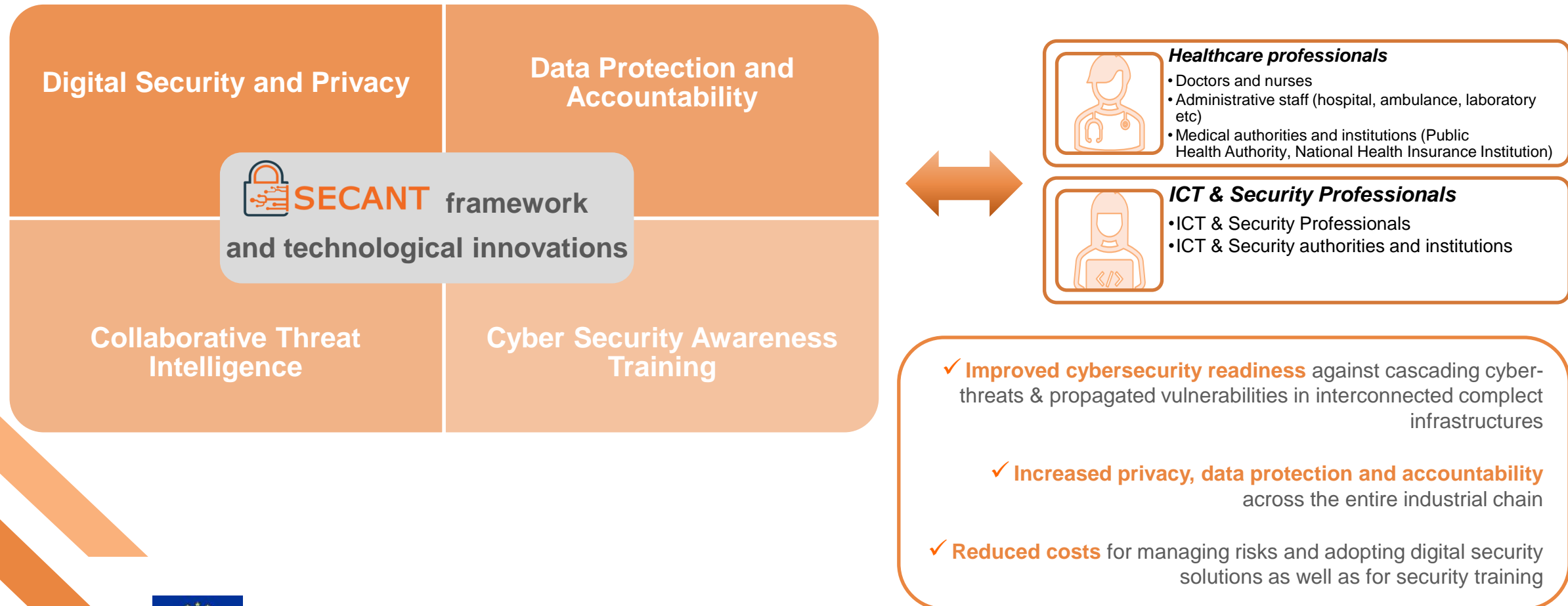
- The industrial sector is experiencing an unprecedented number of changes in recent years:
  - New models of remote delivery, especially in **complex ICT infrastructures**, increase the potential impact of cyber security breaches
  - The level of security awareness is still disproportionately low compared to the criticality and potential of a security breach in critical sectors
  - **Healthcare** is a constantly increasing data-driven ecosystem with a high criticality since the sensitive data
- Need to **complement traditional** platform-specific and attack-specific **countermeasures**



**AIM:** To strengthen the **understanding of risks**, at both **human and technical level** through the delivery of a holistic framework for cyber security risk assessment for enhancing the digital security, privacy, and personal data protection in complex ICT infrastructures, such in the healthcare ecosystem.

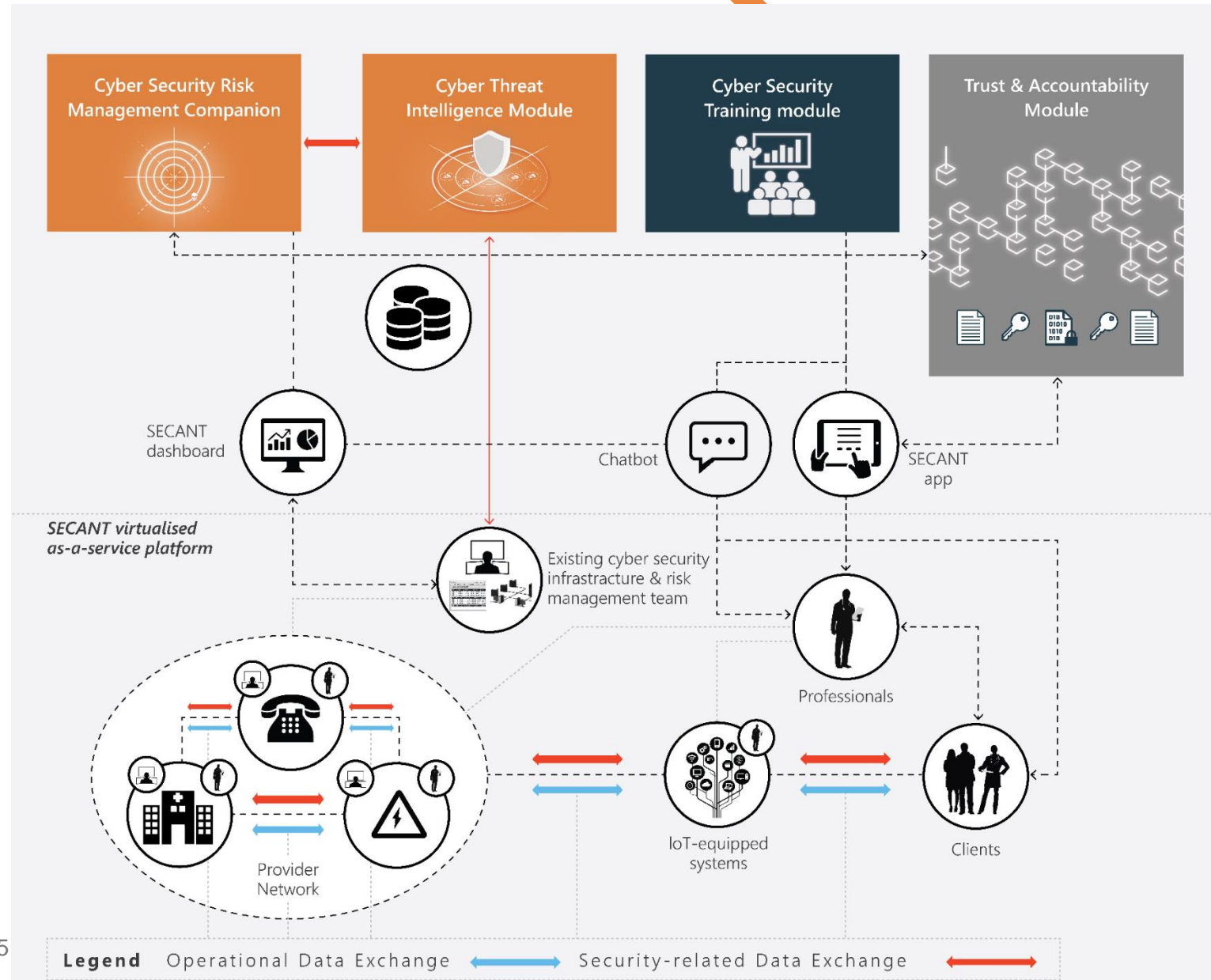
# Objective

To develop a **threat detection platform** that is capable of identifying threats and attacks and **promote the situational security awareness** as a priority.

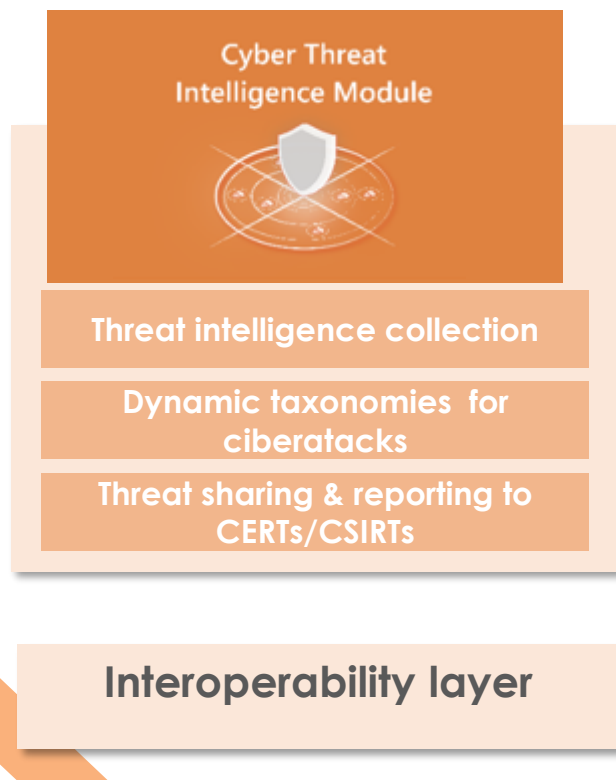




# SECANT approach



Collaborative toolkit to allow the organization stakeholders and European CERTs/CSIRTs create and exchange dynamic vulnerability databases & taxonomies for cyber-attacks targeting ICT systems, technologies, applications and services



**Threat Intelligence Module (TIM):** Supports the creation of dynamic vulnerability databases and taxonomies for cyber-attacks against ICT-based systems, applications and services.

- Collect and share threat intelligence from SECANT's supply chain stakeholders
- Report such intelligence to CERTs/CSIRTs
- Build dynamic taxonomies for cyber-attacks

**Interoperative level (IPL):** middleware between the medical equipment and the SECANT platform including a central repository

Dynamic, evidence-based **security and privacy risk assessment framework** to deal with the cascading effects of cyber-attacks and with propagated vulnerabilities in interconnected complex ICT systems, services, and applications

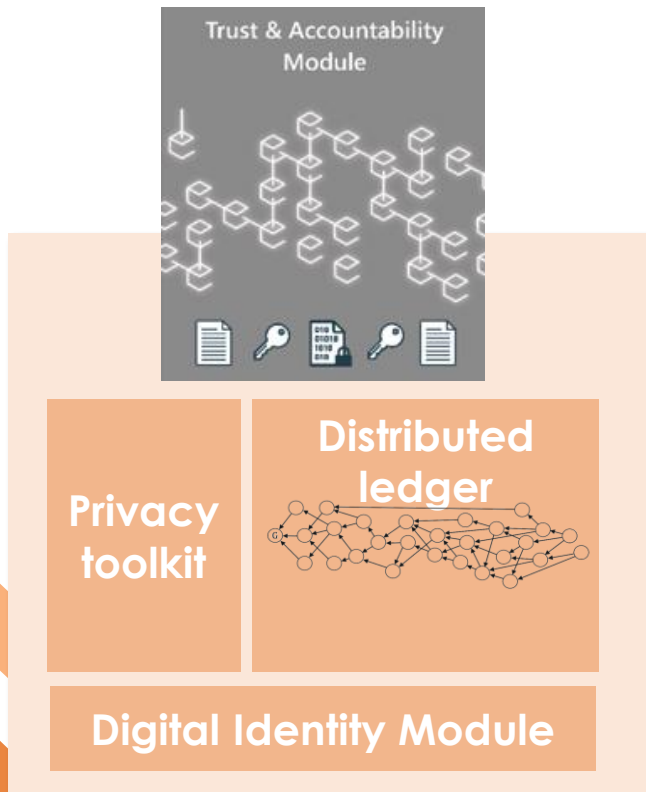


**Cyber Security Risk Assessment Companion (CSRAC):** Facilitate decision making and effective and timely response to detected cyber security risks and minimize their risks

- **Connected Organizations Cyber Risk Assessment Engine (CO-CRAE):** analyze cascading cyber-attacks in industrial ecosystems
- **Human Vulnerability Assessment (HVA):** tackle and assess Social Engineering attacks
- **Technical Vulnerability and Impact Assessment (TVIA):** identify and dynamically isolate propagated vulnerabilities in the ecosystem.
- **Behaviour analytics engine (BAE):** identify suspicious patterns in the behaviour of an entity in the network.



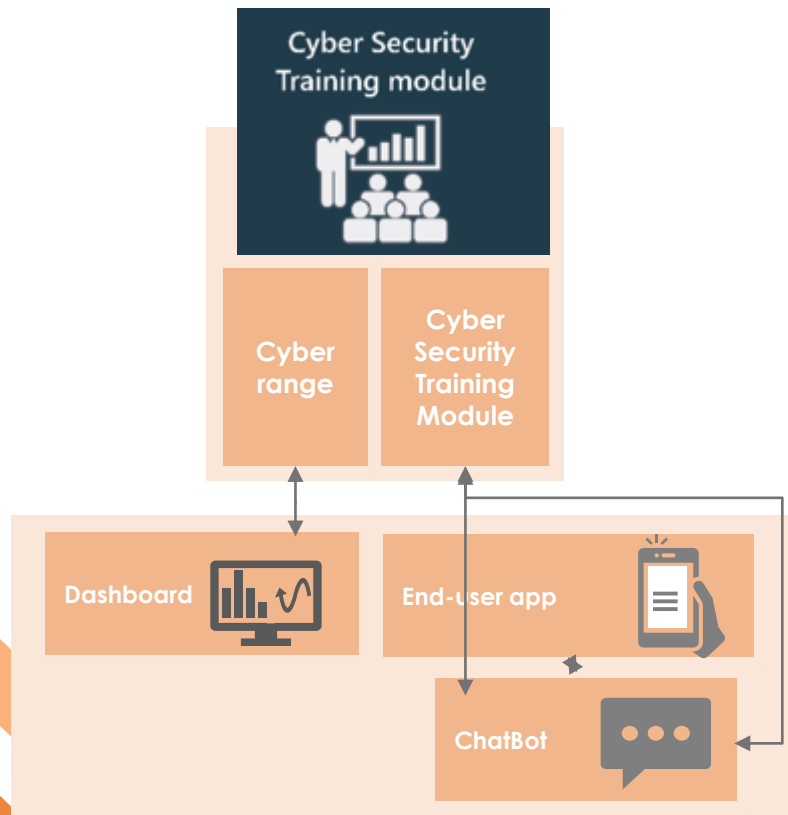
Data protection and multi-level accountability framework, relying on a distributed ledger system, to establish trust, integrity and protect sensitive data



**Trust and accountability module (TAM):** Ensures transparency and integrity of the collected data and the management of identities both for devices and persons

- **DLT:** Verifies devices and data integrity, on behalf of the data owner and provided access only to actors in the medical ecosystem that are authorized to access them through verifiable credentials
- **Digital Identity Management module (DIM):** Unequivocal identification of professionals, clients and instruments of an organization based on SSI concept.
- **Privacy Toolkit:** merge advanced encryption technologies to mediate all access to information flowing through the TAM.

## User interfacing applications and security training platforms with cyber range capabilities



**Security Awareness Training** : make smarter security decisions with training and simulated social engineering.

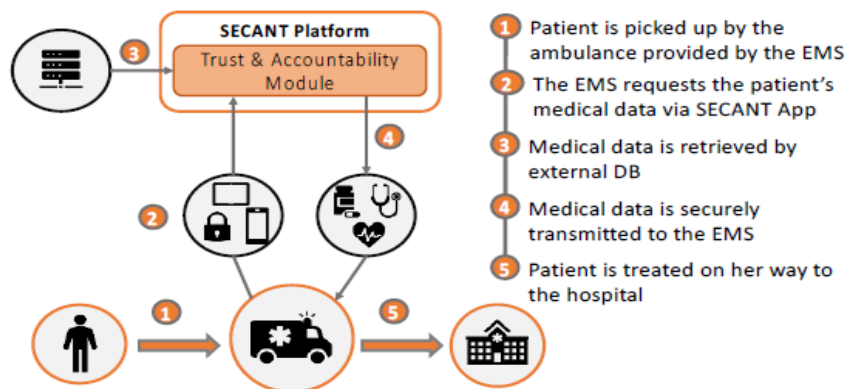
- **Cyber Range (CR)**: for security professionals to train using a simulated representation of the supply chain, modelling and emulating the complex ICT infrastructures.
- **Cyber Security Training Module (CSTM)**: Security awareness training for other professionals and clients to familiarize themselves with best cyber security practices. Enhanced with **Chatbot** for interactive training.

**SECANT Dashboard and End User Application**: interfaces to the platform

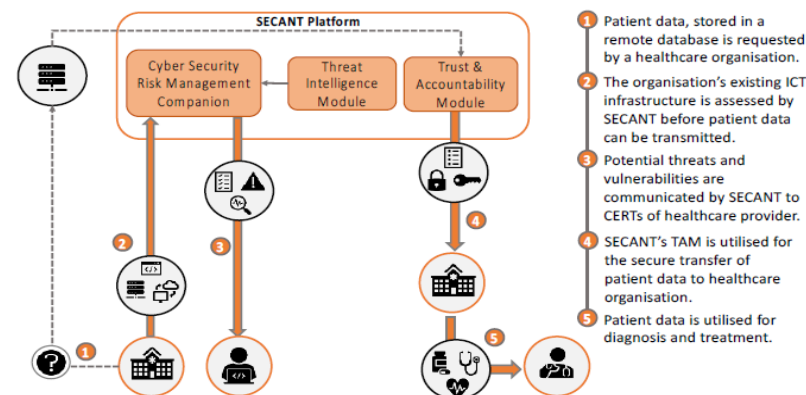
- **Dashboard**: for cyber security professionals, access to TIM and CSRAC
- **End User Application**: for patients and other professionals to access to CSTM and **Chatbot app**

# SECANT Pilot Use Cases

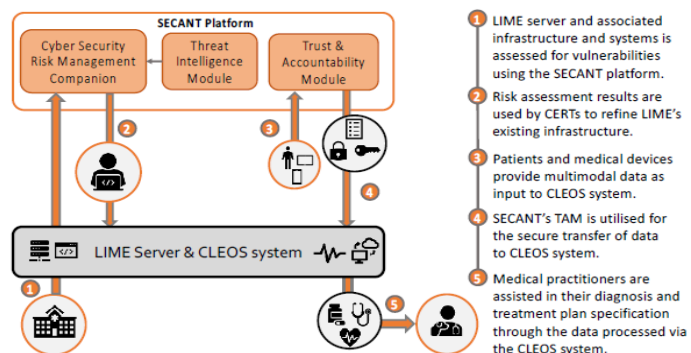
## PUC1: Protecting the connected ambulance of the future



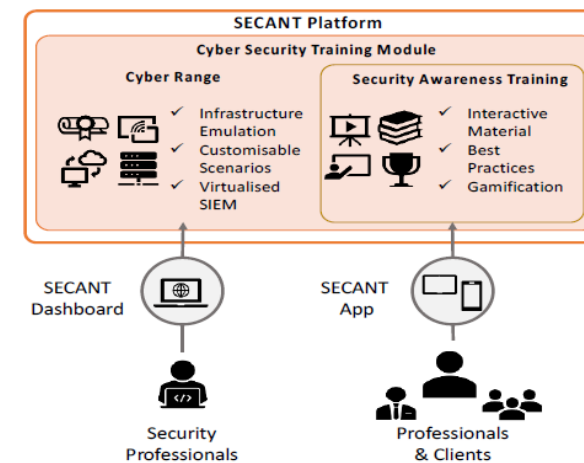
## PUC3: Health data protection in healthcare supply chain



## PUC2: Cybersecurity for connected medical devices & mobile app



## PUC4: Cyber Security Training





## Innovative risk analysis methodologies

- *Support organizations and stakeholders to identify risks which may impact data security and privacy*

## Real-time information sharing capabilities

- *Facilitates to cybersecurity professionals the handling and forecasting of security incidents, complex attacks and propagated vulnerabilities*

## Highly scalable ledger infrastructure

- *Innovations in the field of **trust and accountability** and enables end-to-end integrity and protection of sensitive operational data*

## SECANT as a whole

- *Allows for both technologically protecting connected organizations and empowering their users towards their better protection*



# Contact and more information

Project Coordination: NTT Data Spain  
[Secant\\_pc@nttdata.com](mailto:Secant_pc@nttdata.com)

Scientific and Technical Management: CERTH-ITI  
[secant-stm@iti.gr](mailto:secant-stm@iti.gr)

Dissemination Management: 8 BELLS  
[secant-dcm@8bellsresearch.com](mailto:secant-dcm@8bellsresearch.com)

<https://secant-project.eu/>



<https://twitter.com/SecantProject>



<https://www.linkedin.com/in/secant-project/>

