ER1

SAFECARE

Integrated cyber-physical security for health services

SAFEguard of Critical heAlth infrastructure

SAFECARE Project

Philippe Tourron
AP-HM, Project Coordinator

Isabel Praça
ISEP, Scientific Coordinator

SAFECARE has received funding as part of the "Secure societies – Protecting freedom and security of Europe and its citizens" challenge of the Horizon 2020 Research and Innovation programme of the European Union under grant agreement 787002

HORIZON 2020

Slide 1

ER1 Please add your logo here

Elodie Reuge; 03/02/2020

Challenge for health systems managers

- 3 perimeters that overlap and collaborate :
  - Medical devices
  - Building management
  - Medical data and software
- Polymorphic, agile, and combined threats : today and tomorrow, a strong attraction for cybercriminals and terrorists
- A strong dependence between assets and complex impact chains... that can affect the lives of patients and staff
- Paradoxically: A lot of information in specialized supervision systems without communication or integration

Need for a global vision in anticipation, protection, and crisis management

Addressing the challenge…

SAFECARE aims to:

- Provide high-quality, innovative, and cost-effective solutions that will improve physical and cyber security; and
- Enhance threat prevention, threat detection, incident response, and mitigation of impact in healthcare infrastructures, through the creation of a global protection system.

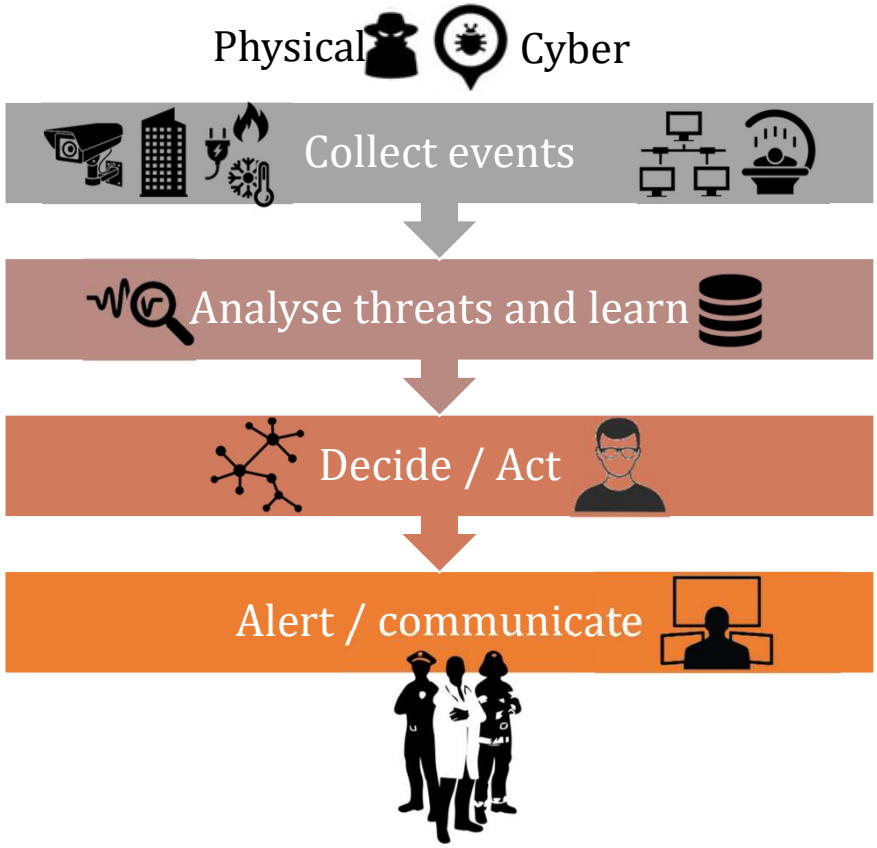
Over the course of 36 months, SAFECARE will design, test, validate and demonstrate 13 innovative elements optimizing the protection of critical infrastructure under operational conditions

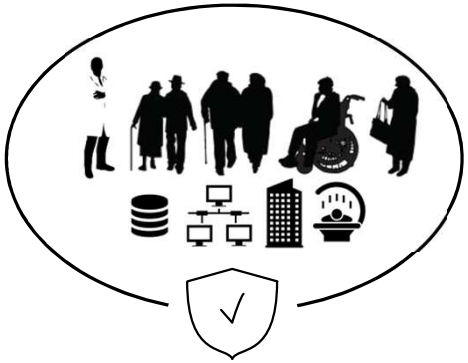
Project Identity

GA Number	787002
Starting date	01/09/2018
Duration in months	36
Topic	CIP-01-2016-2017
Consortium	21 partners - 10 EU countries Technical providers, hospitals, national public health agencies and security bodies
Project Coordinator:	Philippe Tourron, Marseille Public University Hospital (AP-HM)
Technical coordinator:	David Lancelin, Airbus CyberSecurity (CCS)
Scientific coordinator:	Isabel Praça, Instituto Superior de Engenharia do Porto (ISEP)

SAFECARE
Integrated cyber-physical security for health services

Four steps to manage the security



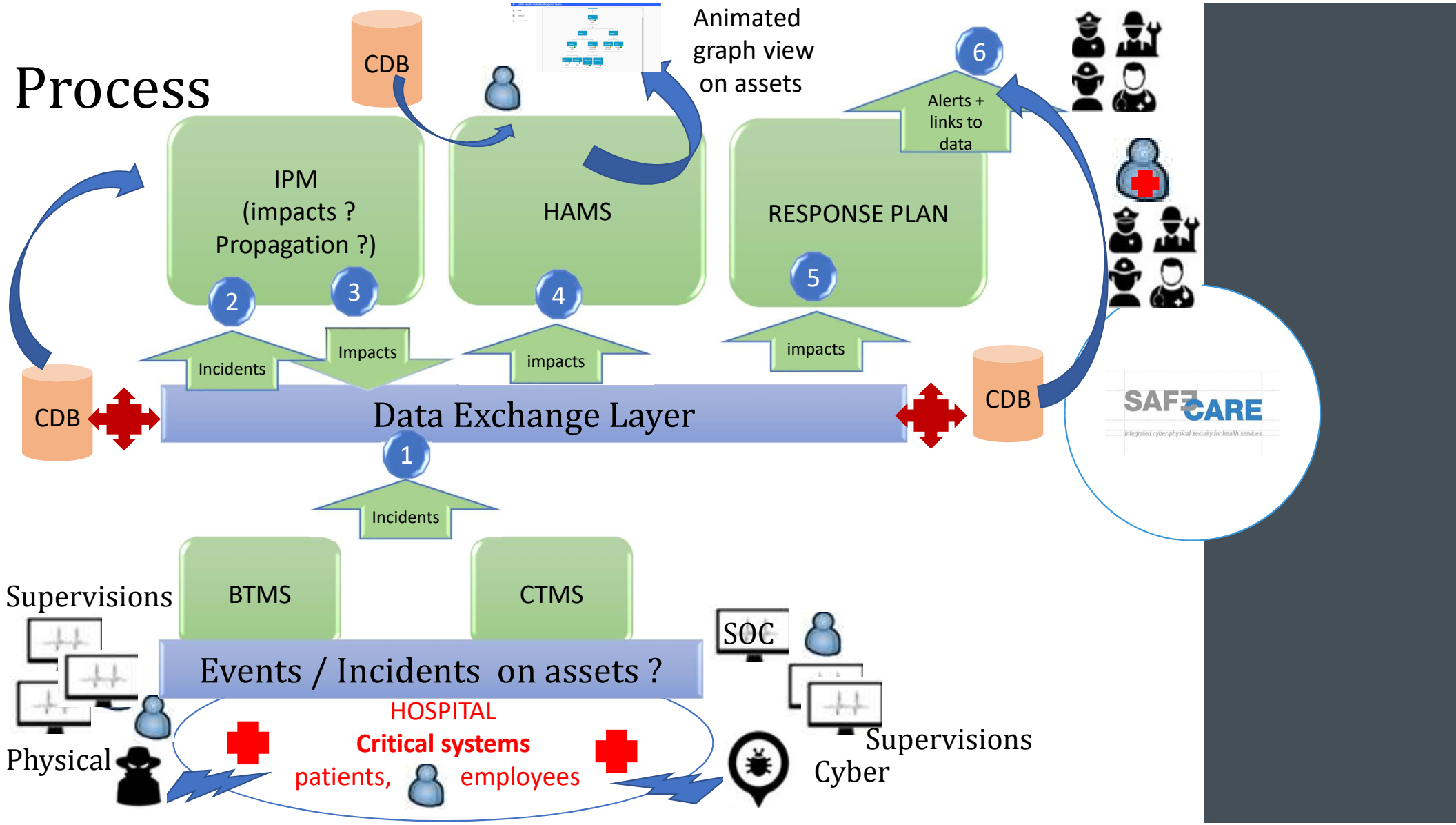


Patients, employees, assets, and services to protect

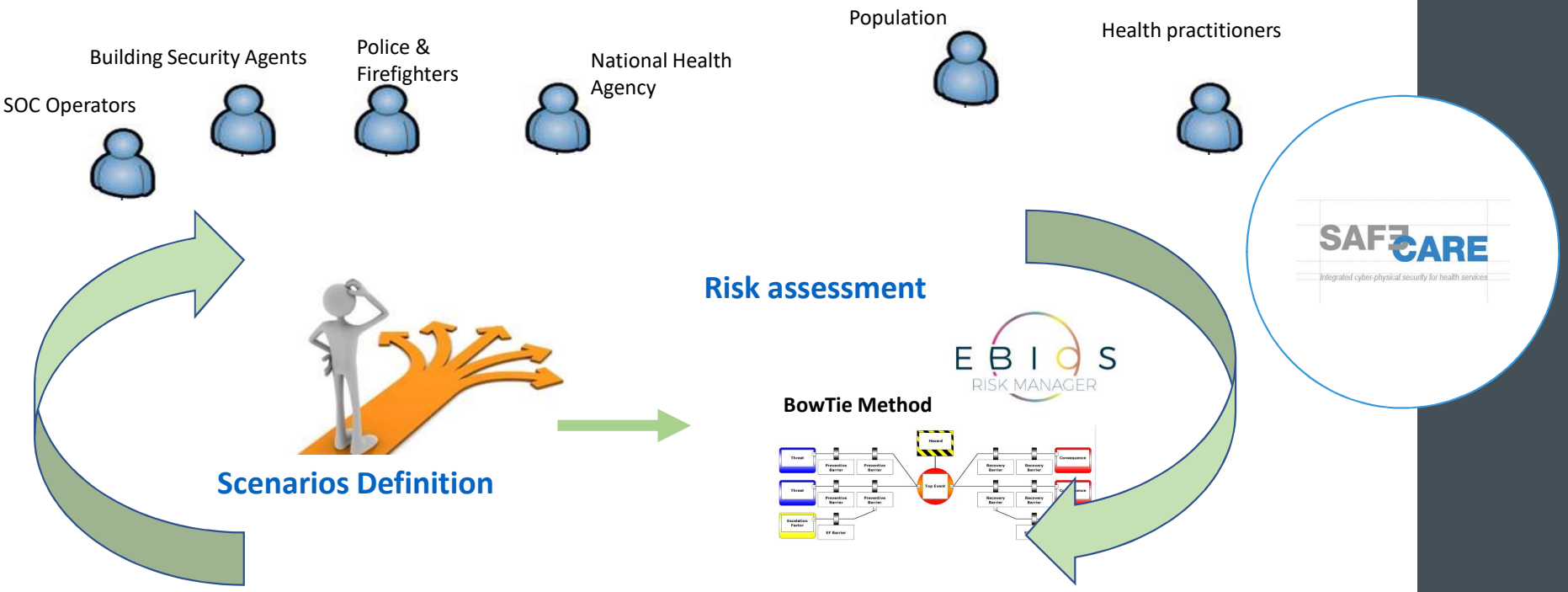
SAFE CARE

Integrated cyber-physical security for health services

Process


CDB
Animated graph view on assets
IPM (impacts ? Propagation ?)
HAMS
RESPONSE PLAN
6
Alerts + links to data
2
3
4
5
Incidents
Impacts
impacts
impacts
CDB
Data Exchange Layer
CDB
1
Incidents
SAFECARE
Supervisions
BTMS
CTMS
SOC
Events / Incidents on assets ?
HOSPITAL
Critical systems
patients,
employees
Physical
Supervisions
Cyber

High Level Architecture



Scenarios and risk assessment

Scenarios

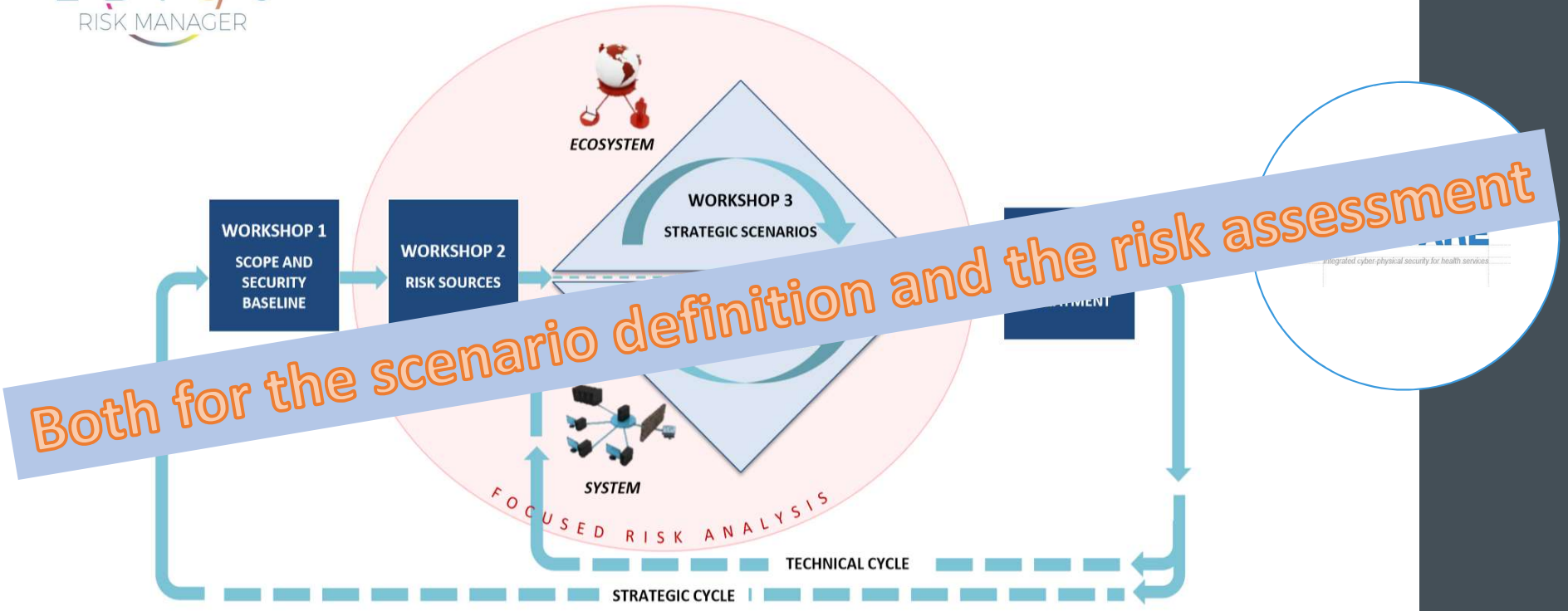
- Sc1: Cyber-physical attack targeting **power supply** of the hospital
- Sc2: Cyber-physical attack to steal **patient data** in the hospital
- Sc3: Cyber-physical attack targeting **IT systems**
- Sc4: Cyber-physical attack to cause a **hardware fault**
- Sc5: Cyber-physical attack targeting the **air-cooling system** of the hospital
- Sc6: Cyber-physical attack on **medical devices**
- Sc7: Cyber-physical attack to **steal credentials** to access IT systems
- Sc8: Cyber-Physical attack in access control provider to **steal medical devices**
- Sc9: Physical attack against hospital staff using a **gun**
- Sc10: Physical attack **to steal drugs**
- Sc11: Cyber-physical attack due to a **personal laptop**
- Sc12: Cyber-physical attack to **block national crisis management**

SAFECARE
Integrated cyber-physical security for health services

Risk Assessment

EBIOS RISK MANAGER

Expression of Needs and Identification of Security Objectives

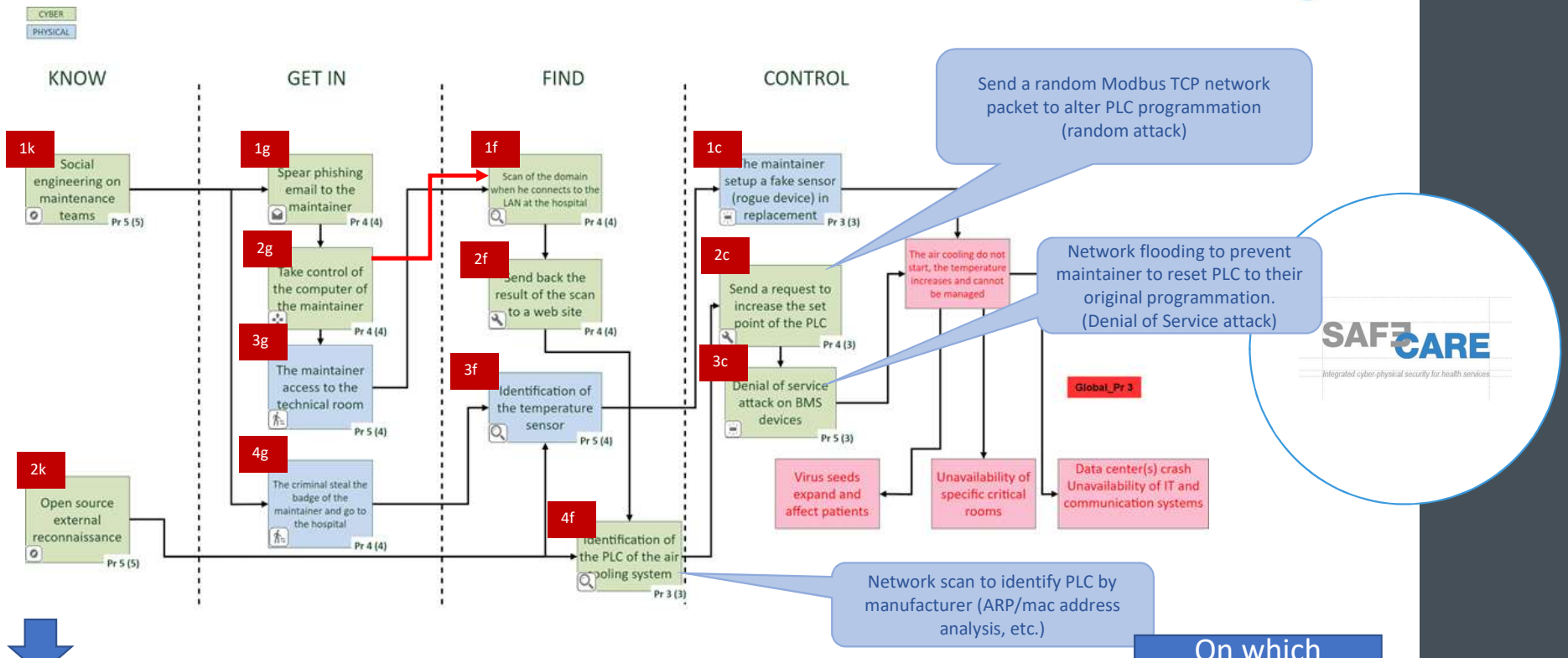


Both for the scenario definition and the risk assessment

Scenarios Definition

RISK SOURCE	OPPONENT OBJECTIVES	STAKEHOLDERS/ INTERM. EVENTS	IMPACT/ SEVERETY
Criminal	Financial	Maintenance teams	Physical harm to patients
Internal Employee	Revenge or extorsion		Unavailability of surgery rooms or other critical areas
External Service Providers	Cause damage		Unavailability of IT systems
Terrorist			

Risk Assessment



which assets

which vulnérabilites

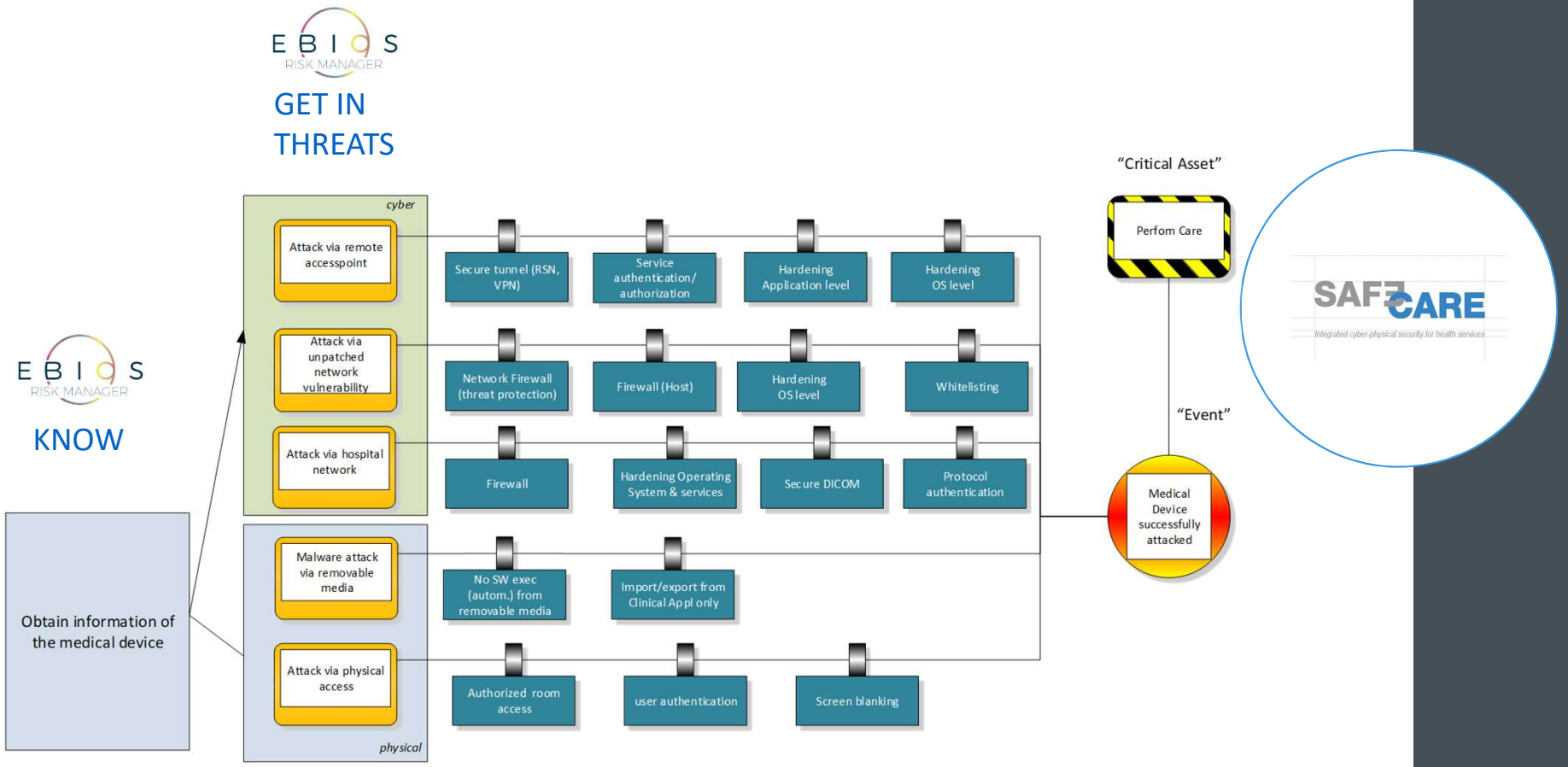
which incident

On which supporting assets

On which primary assets (critical/business value)

Risk Assessment

Combined with BowTie

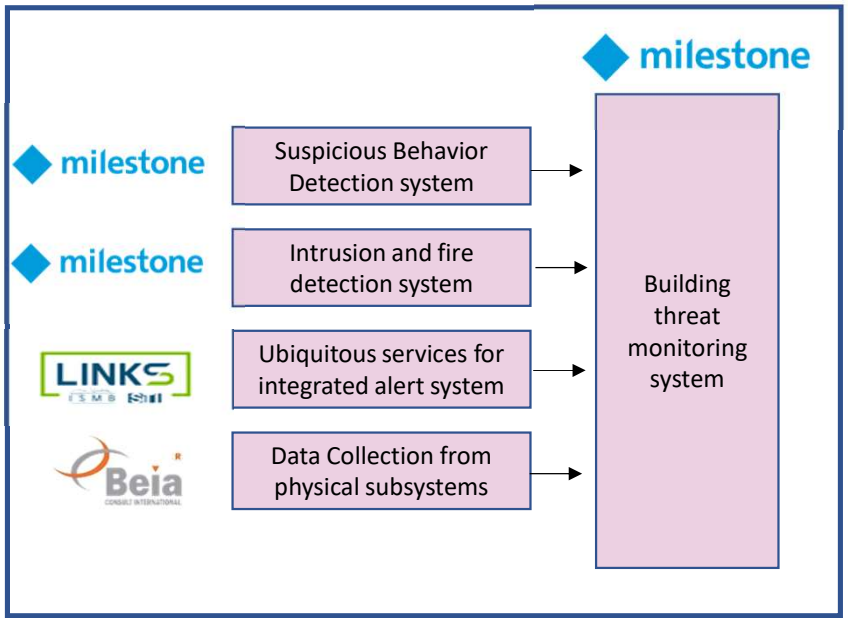


Business values (critical or primary assets)

Hospital Missions	Caring for patients						
Business values (Critical Assets)	Patient care data management	Patient health data	Administrative management of patient data	Guarantee the safety of the building and people	Receive patients 24/7/365	Perform care	Crisis management
Nature of critical assets (process or information)	Process	Information	Process	Process	Process	Process	Process
Description	Processing of patient data	Patient health data and administrative data	All the management necessary for the localisation, billing, patient identity and communication	Safe reception of patients, staff and visitors	Physical or telephone reception of patients. Emergency Medical Services. All services with a patient reception and offices dedicated to patient registration	Support for the patient, at all step of their care process (Nursing care, care unit, surgical procedures, psychological support, medical imaging, biological analyses)	Organisational and technical procedure during a health / humanitarian crisis (France : Orsan Plan)
Responsible entity or person	Health care facility	Health care facility	Health care facility	Health care facility	Health care facility	Health care facility	Health care facility

What appens during or at the end of the kill chain ?

Physical Security Solutions



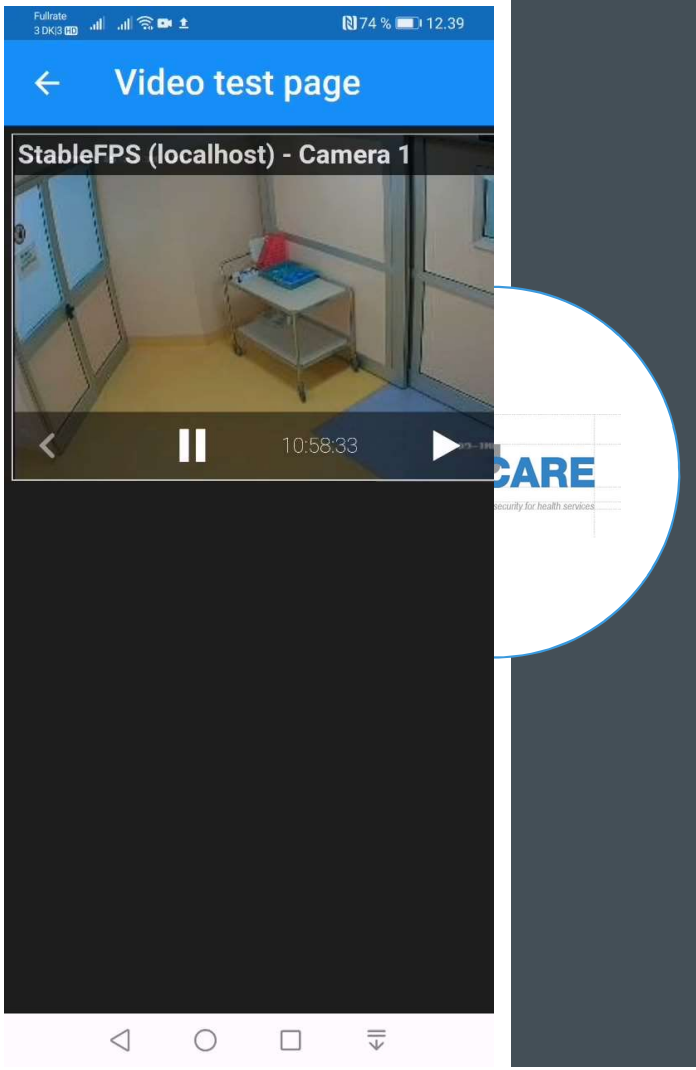
SAFECARE
Integrated cyber-physical security for health services

Physical Security Solutions

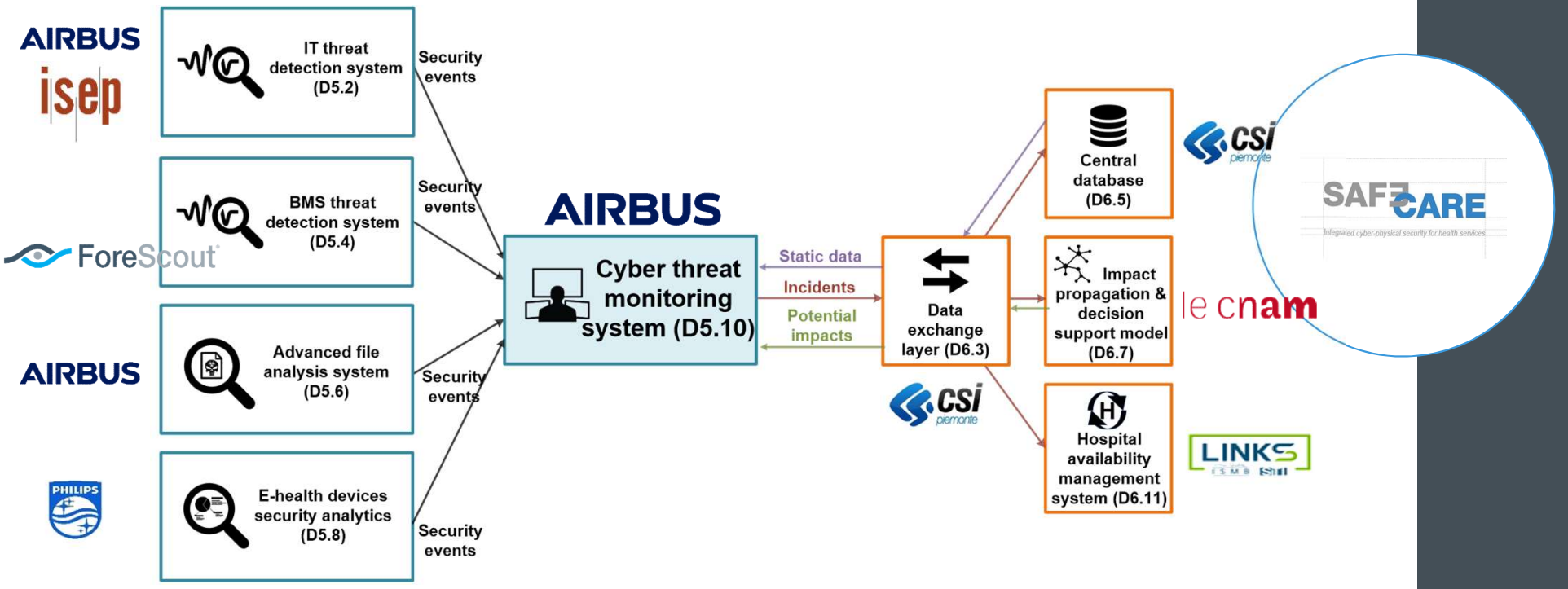
Physical Security Solutions

Integrated mobile alerting system

android iOS



Cyber Security Solutions



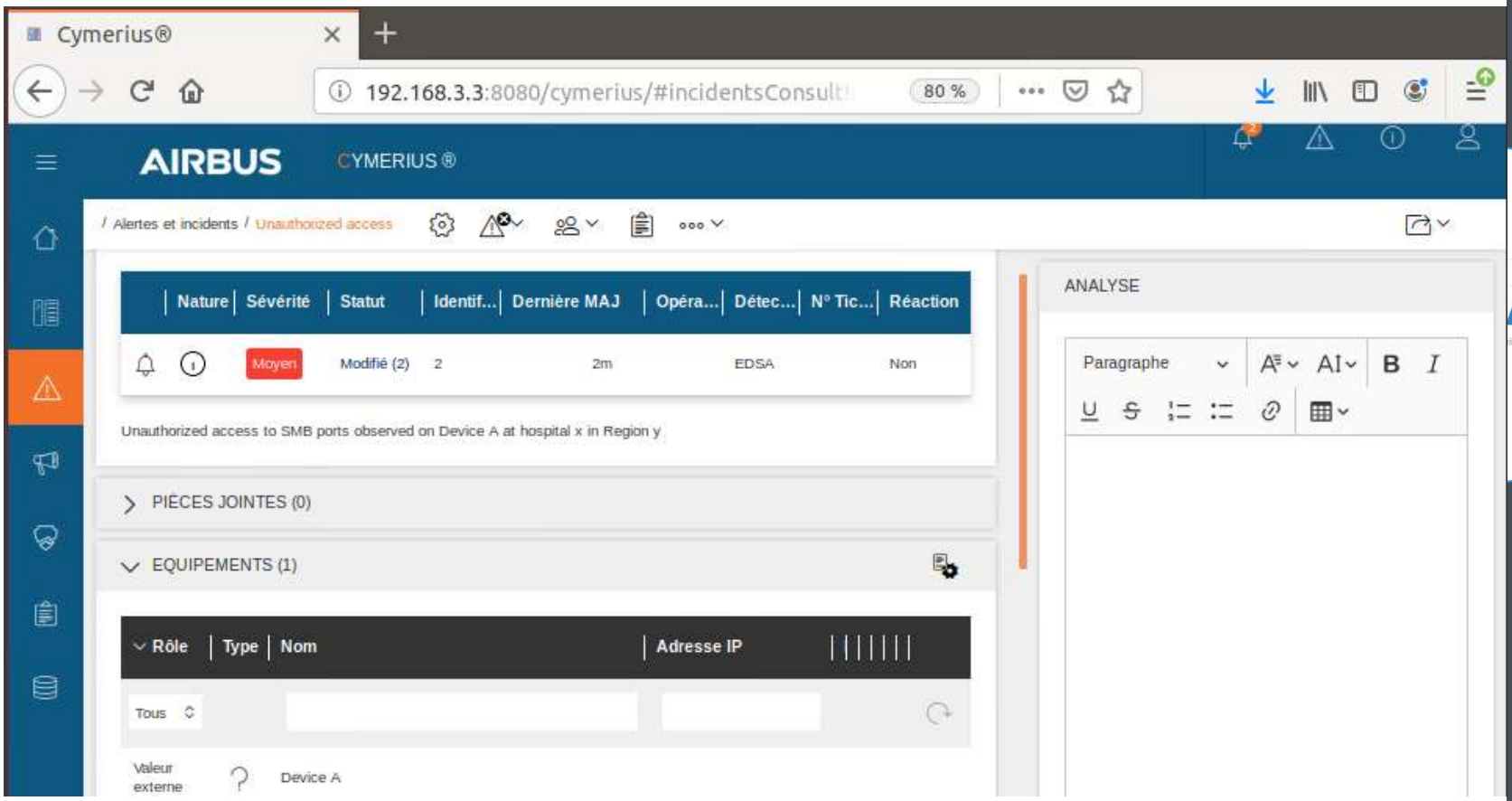
Cyber Security Solutions

E-health device security analytics

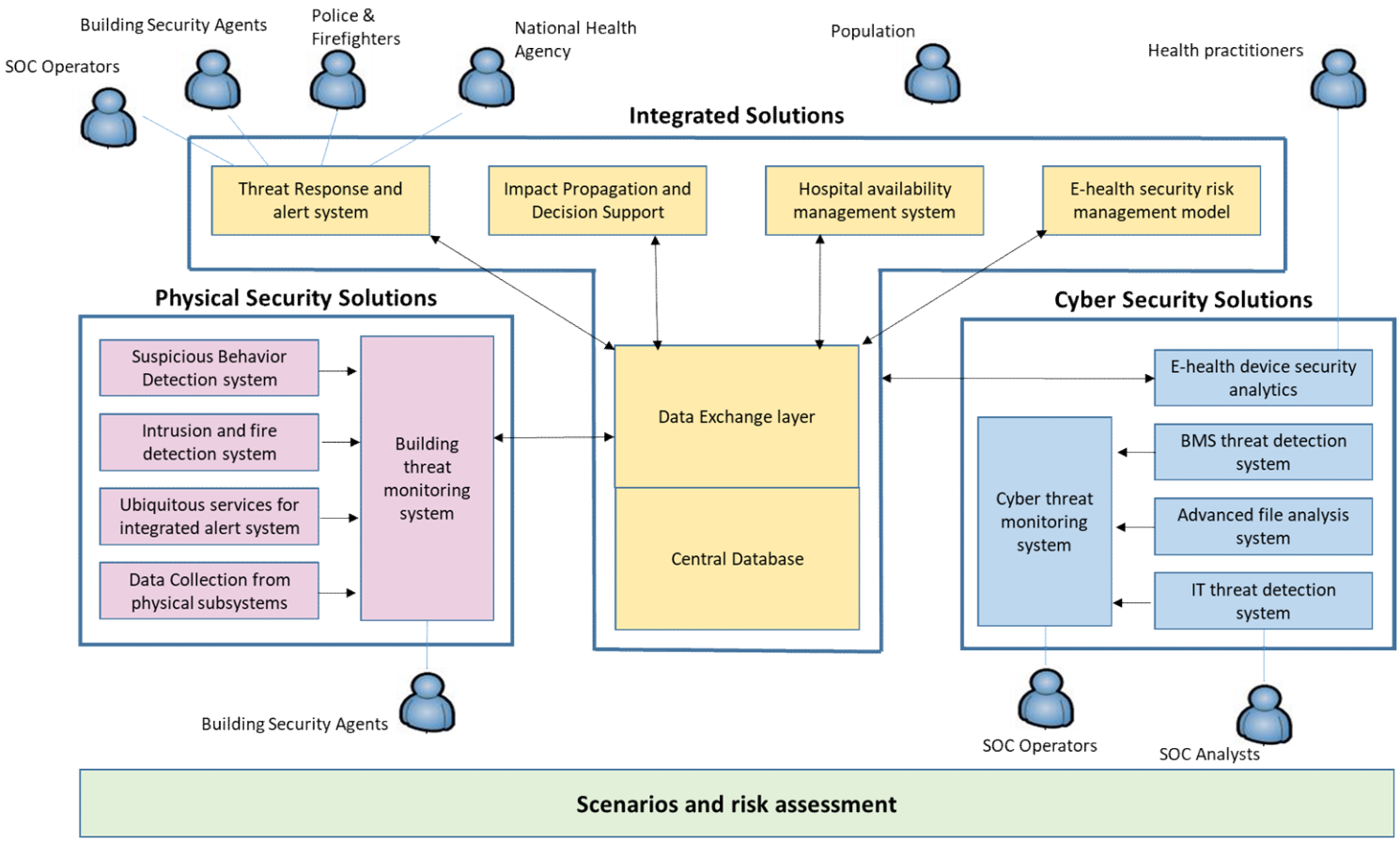
- Source event: E-health devices security analytics
- Event to incident path:
  1. **Sender:** E-health devices security analytics
  2. **Receiver/forwarder:** syslog-ng server
  3. **Collector & correlator (event → alert):** Graylog
  4. **SOAR (alert → incident):** Cymerius

Cyber Security Solutions

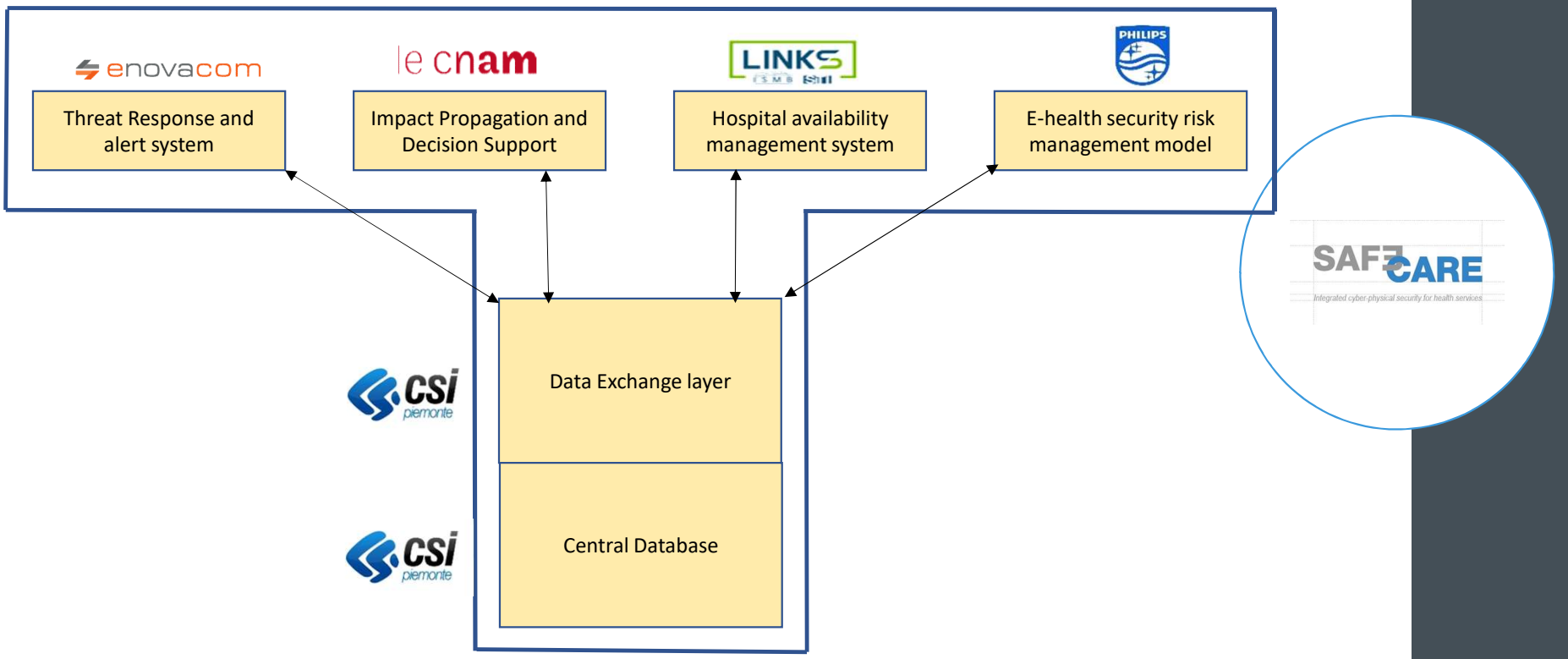
Cyber Threat Monitoring System



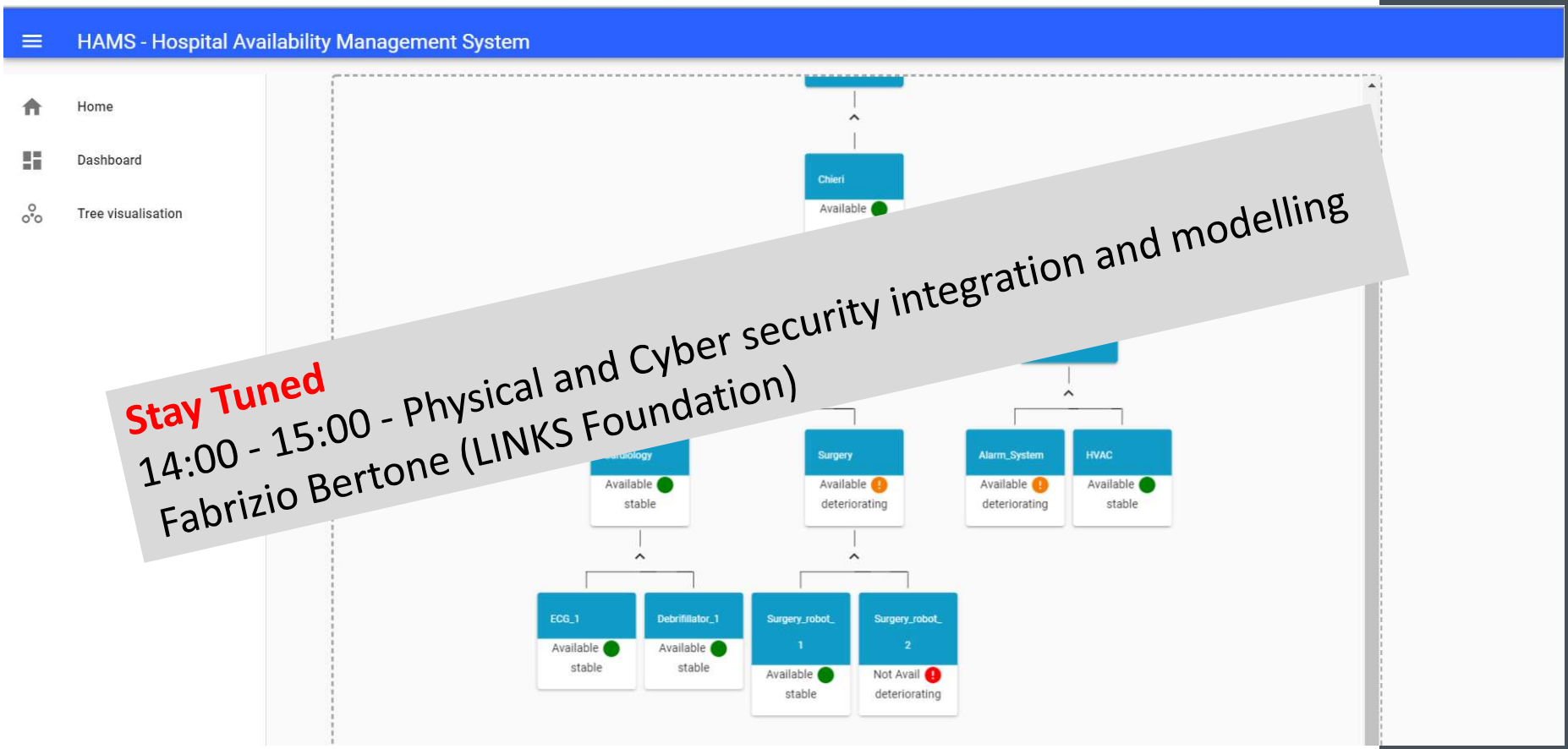
High Level Architecture



Integrated Solutions



Integrated Solutions



Stay Tuned

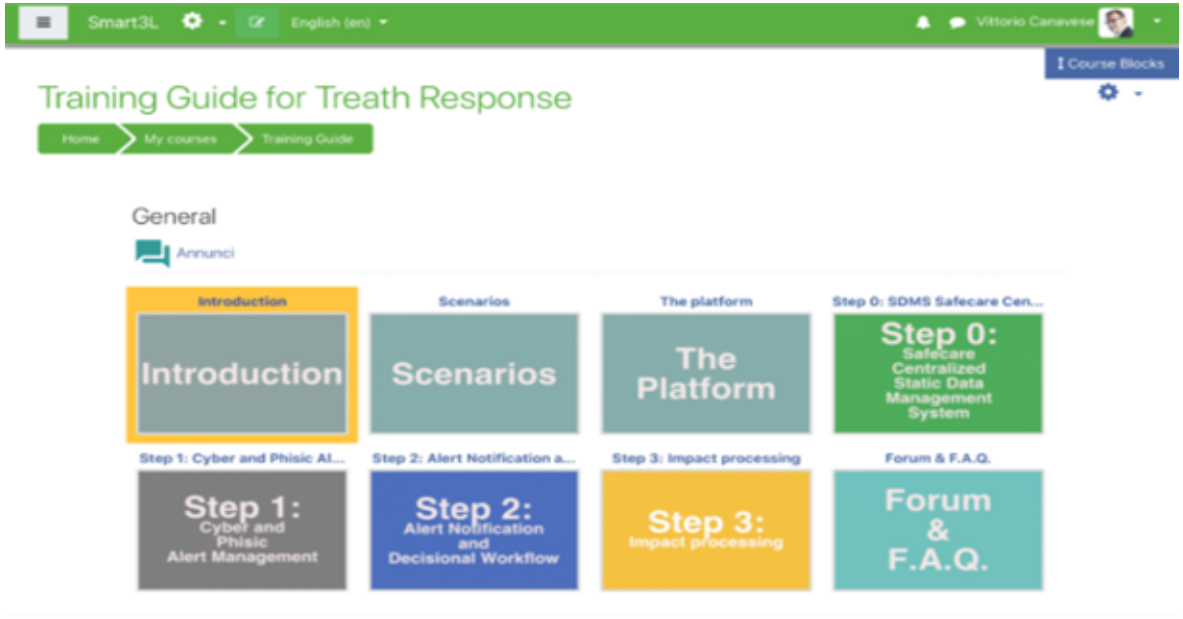
14:00 - 15:00 - Physical and Cyber security integration and modelling

Fabrizio Bertone (LINKS Foundation)

End-Users Training

- Training process (plan; prepare; facilitate and; evaluate)
- E-learning platform, based on LMCS Moodle, called Smart Life Long Learning (Smart3L)

* Planning training process (user-groups; training goal and objectives; training framework; training modules and content; training methods and delivery tools; evaluation methodology)



Simulation and Tests Platform

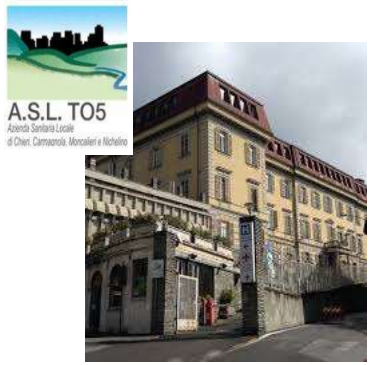
Cyber Range

Tests and Demonstration

Test Platform

Pilots

Marseille



Turin

Amsterdam

Thank you!

Questions?

Philippe Tourron
AP-HM, Project Coordinator

Isabel Praça
ISEP, Scientific Coordinator