SAFECARE

Integrated cyber-physical security for health services

KEMEA

ΚΕΝΤΡΟ ΜΕΛΕΤΩΝ ΑΣΦΑΛΕΙΑΣ

CENTER FOR SECURITY STUDIES

SAFECARE Project

CYBERSEC4HEALTH – 10/07/2019

Eleni Darra

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

European Commission | HORIZON 2020

About SAFECARE

Project title	**SAFEguard of Critical heAlth infrastructure**
Project Number	**787002**
Starting date	**01/09/2018**
Duration in months	**36**
Topic	**CIP-01-2016-2017: Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe**

The consortium (composed by 21 partners from 10 EU countries) engages with active leading roles: hospitals, national public health agencies and security forces across Europe.

About SAFECARE

Because living in a safe and secure society is a fundamental human need

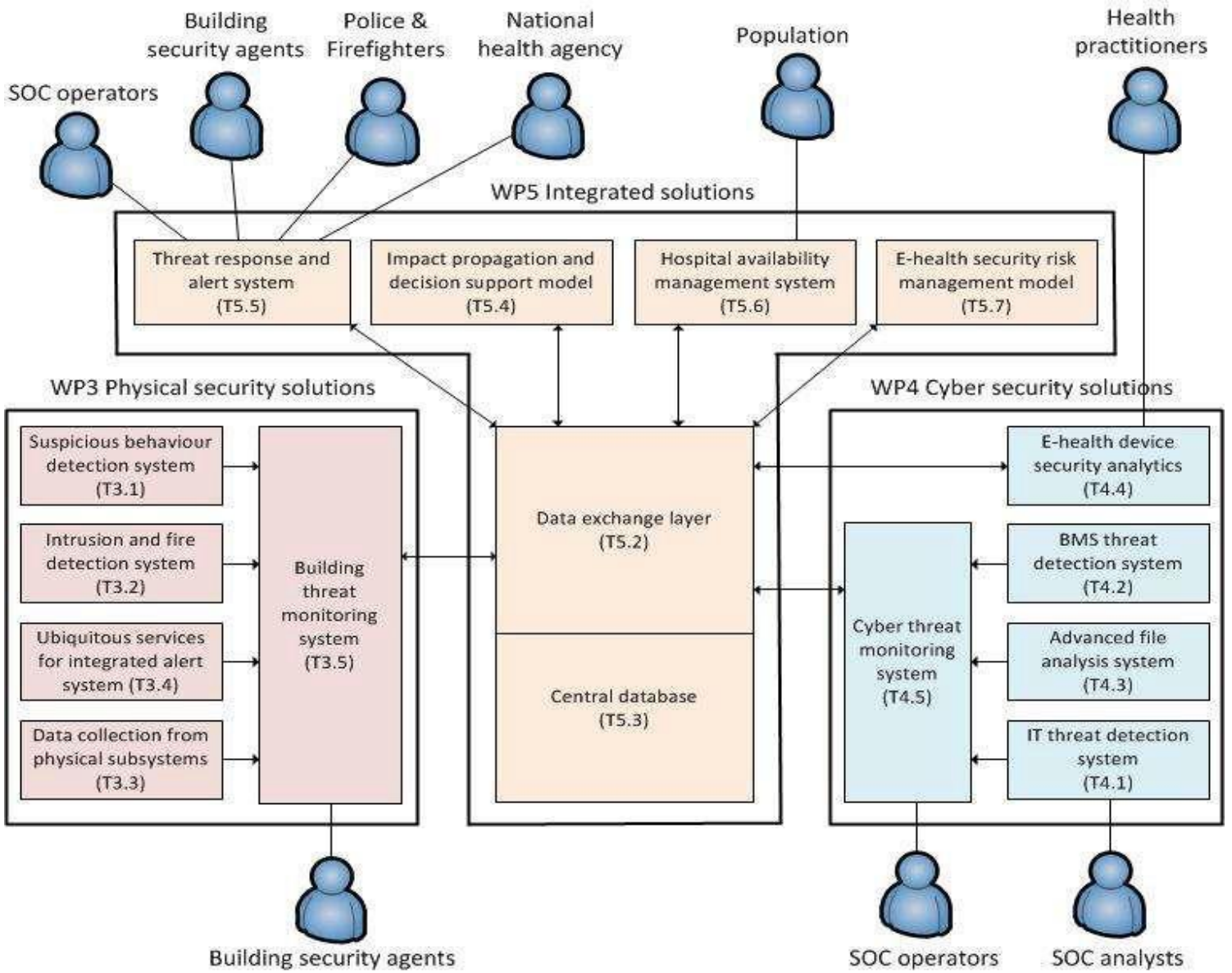
Aim of the project :

- to provide solutions that will improve **physical and cyber security** in a seamless and cost-effective way,
- to enhance threat **prevention**, threat **detection**, incident **response** and **mitigation** of impacts….

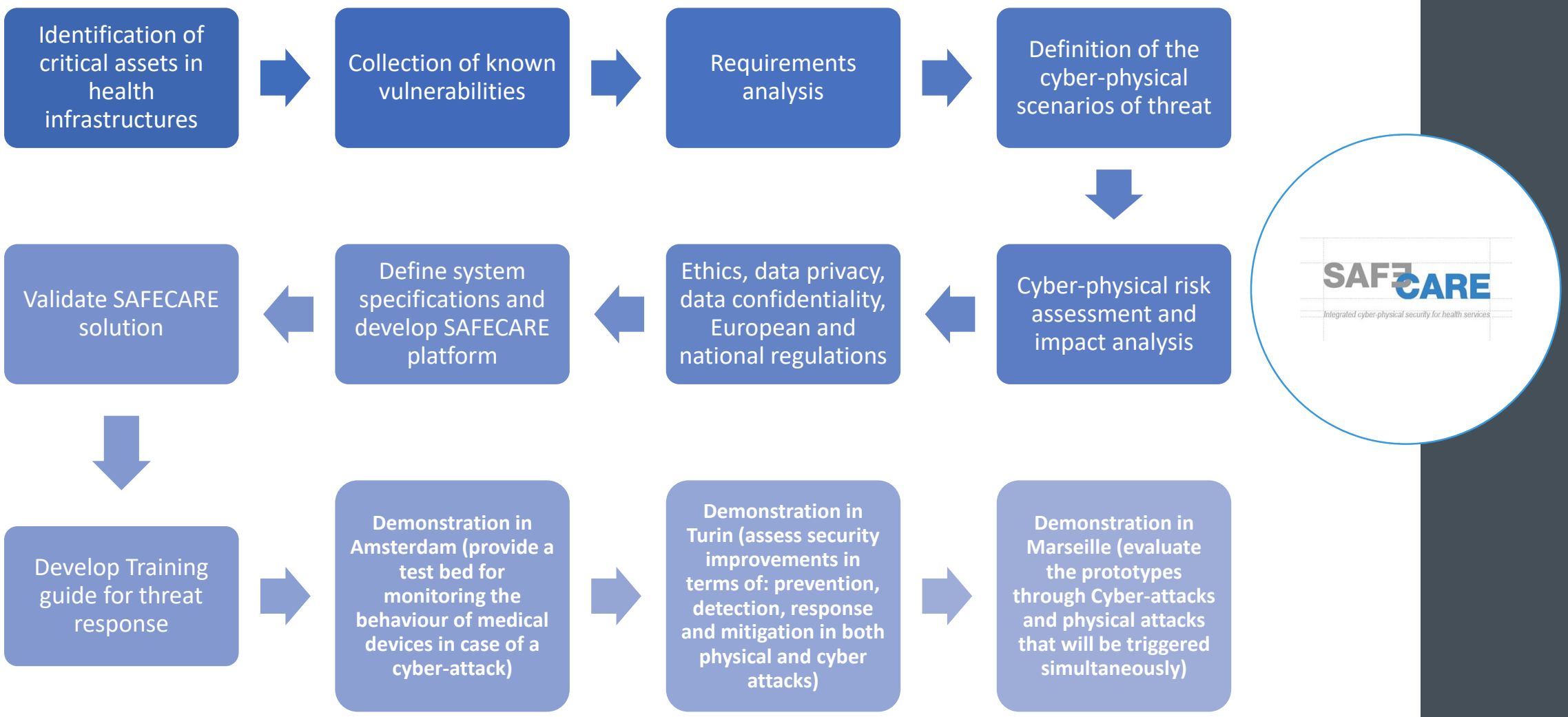
…in Healthcare infrastructures

*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***

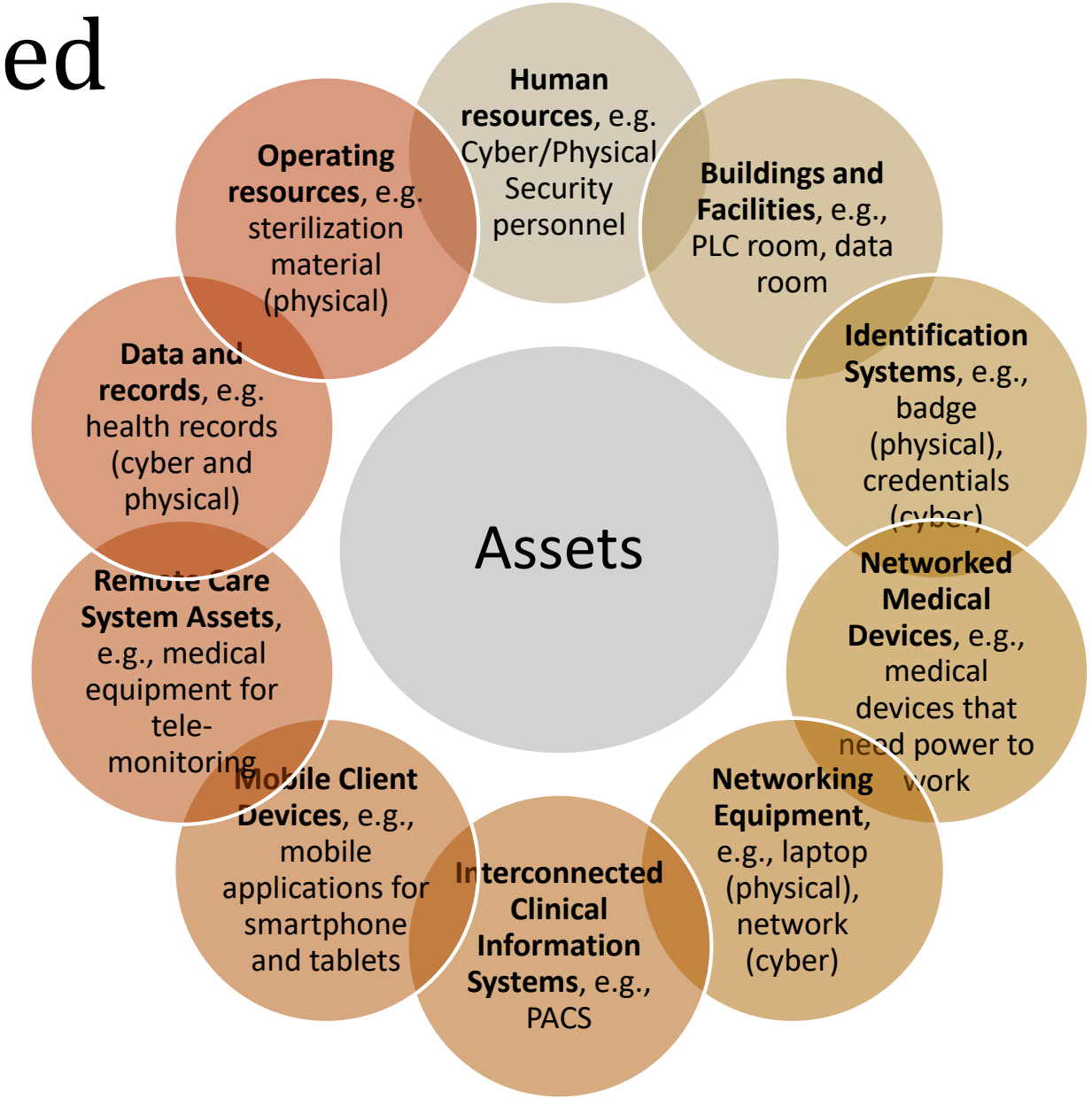
SAFECARE - High level architecture



End-users involvement…

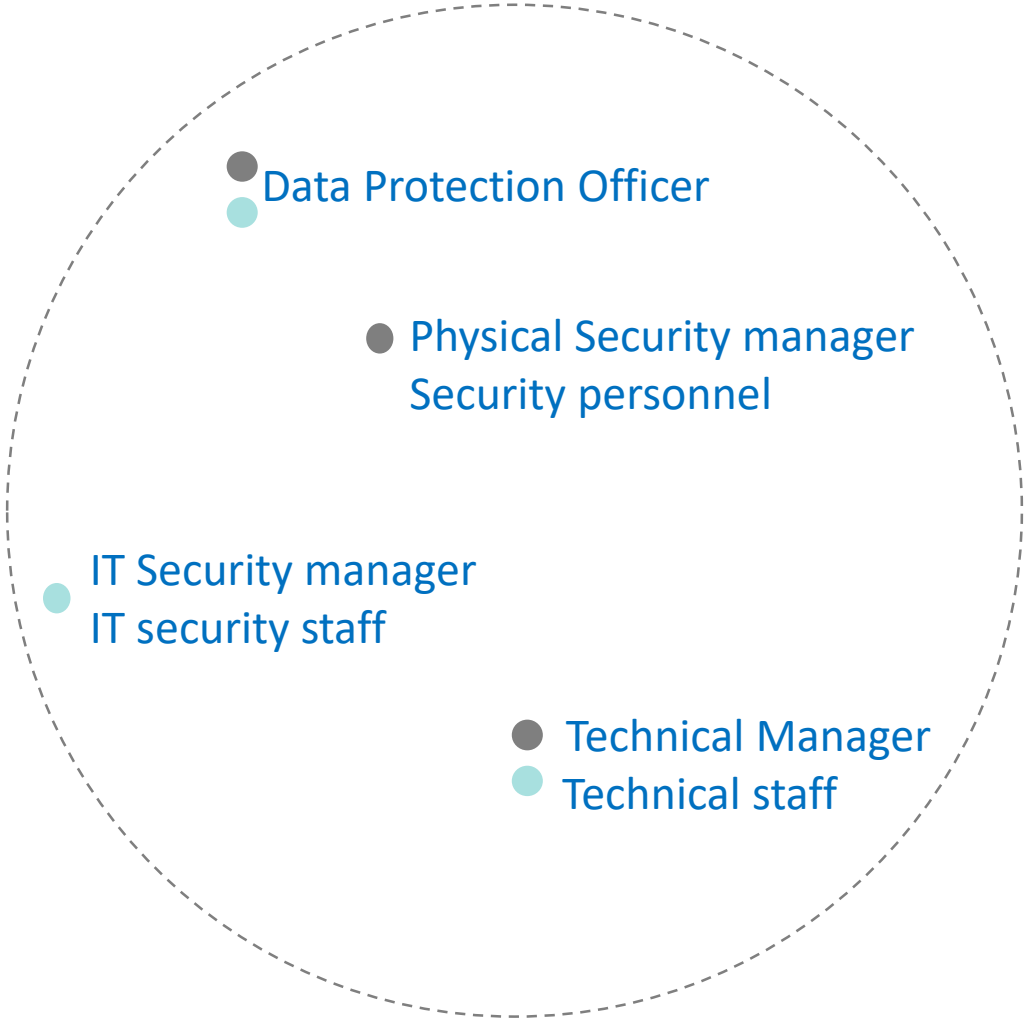


Critical assets main categories identified



Internal security stakeholders

Physical
Cyber



Internal security stakeholders requirements

- Physical
- Cyber

- Manage hospital operations, documents, data breaches and queries

Data Protection Officer

- Manage access rights
- Manage hospital suspicious behavior system
- Manage hospital threats and security events
- Manage security related documents
- Manage security personnel

Physical Security manager
Security personnel

- Manage access rights
- Manage suspicious behavior on IT infrastructure
- Manage IT infrastructure threats and security events
- Manage IT security related documents
- Manage IT security personnel

IT Security manager
IT security staff

Technical Manager
Technical staff

- Manage access rights
- Manage safety events
- Manage threats and security events on technical equipment and infrastructures
- Manage technical related documents
- Manage Technical personnel

External security stakeholders

- Physical
- Cyber

- Civil Protection and Administrative regions
- LEAs (e.g. Police)
- FRs (e.g. Fire Service)
- Radiological related authorities
- Biological related authorities

- Interconnected CIs and related Organisations (e.g. Ministry of Health, Telecommunication CIs)
- Emergency Management Services (e.g. ambulance service)
- Health Coordination/Operations Centre

External security stakeholders requirements

- Physical
- Cyber

- Civil Protection and Administrative regions

  Receive alerts and information on security events

- LEAs (e.g. Police)

  Receive alerts and information on suspicious behavior, threats and events

- FRs (e.g. Fire Service)

  Receive alerts and information on physical security incidents

- Radiological related authorities

  Receive alerts and information on radiological oriented security incidents

- Biological related authorities

  Receive alerts and information on biological incidents and medical records

- Interconnected CIs and related Organisations (e.g. Ministry of Health, Telecomunication Cis)

  Support incident management for physical and cyber threats and respond against respective security events

- Emergency Management Services (e.g. ambulance service)

  Receive alerts and information on physical security incidents that include human injuries an losses

- Health Coordination/Operations Centre

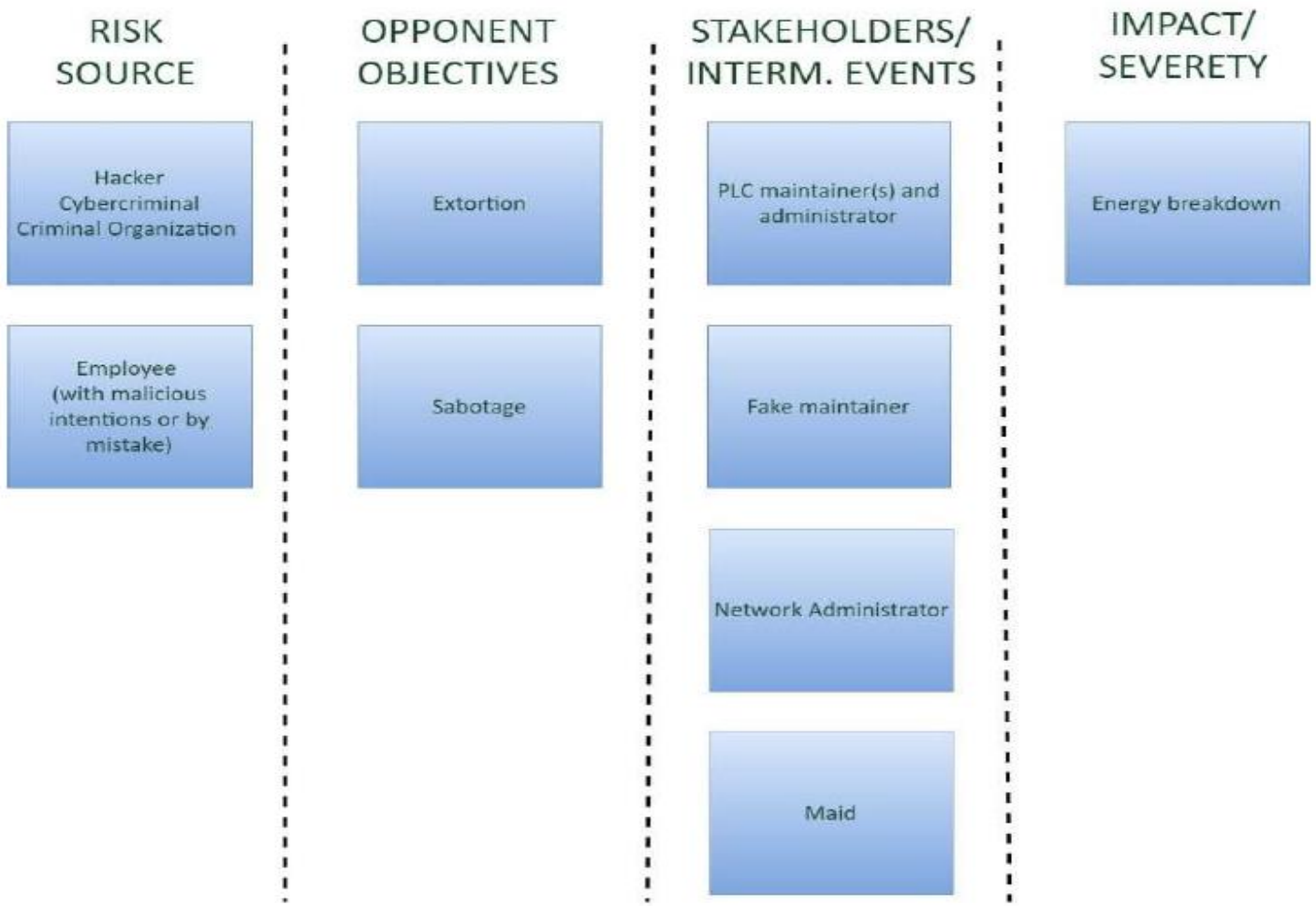
  Receive alerts and information on health emergency

SAFECARE Scenarios of threat

EBIOS methodology has been used for scenario definition and risk assessment…
https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/

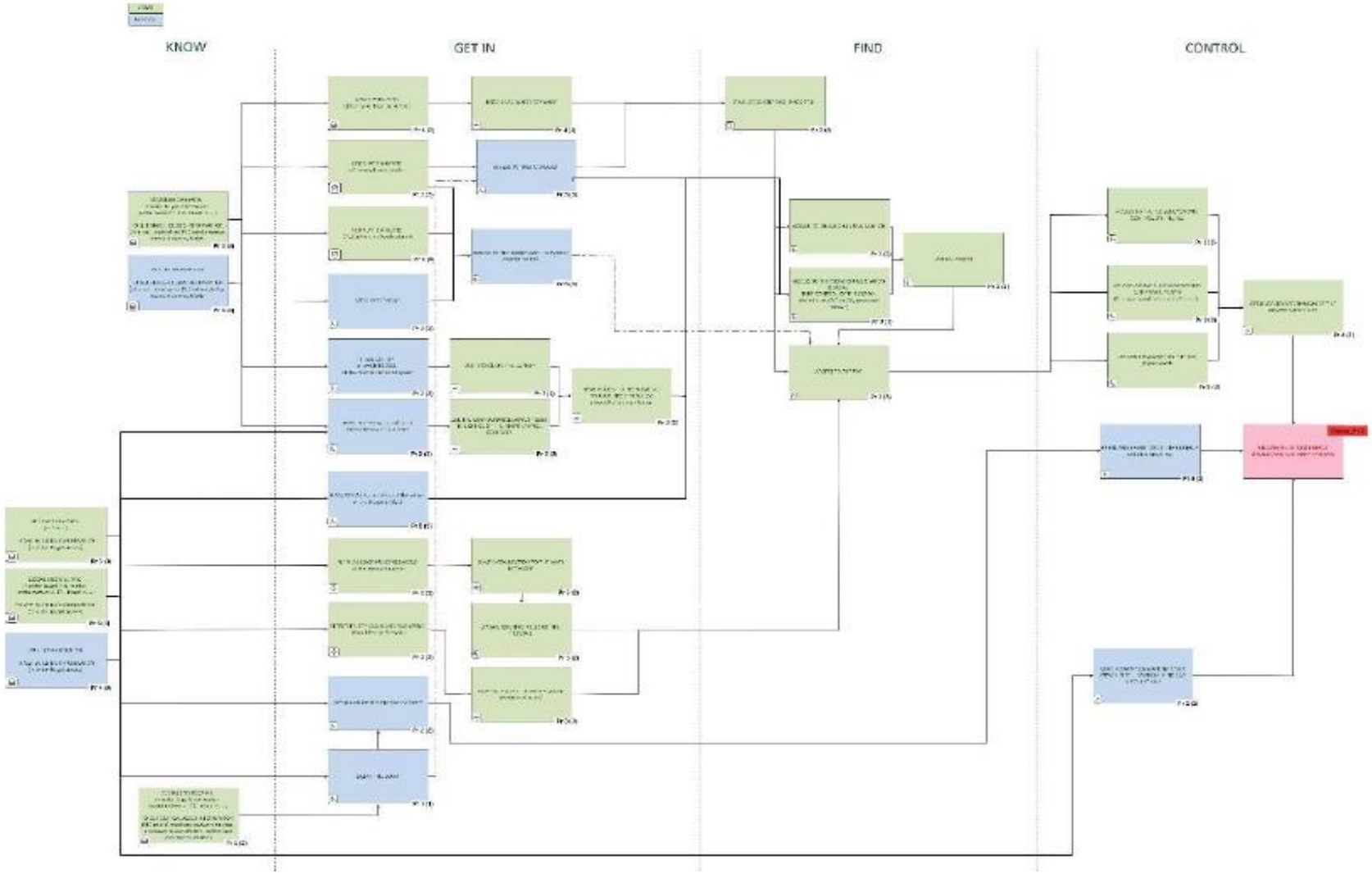
Indicative SAFECARE scenario of threat: *Strategic scenario view*

Scenario 1 - Cyber-physical attack targeting power supply of the hospital;



Indicative SAFECARE scenario of threat: *Technical scenario view*

Scenario 1 - Cyber-physical attack targeting power supply of the hospital;



Indicative SAFECARE scenario of threat: *Risk mitigation*

Scenario 1 - Cyber-physical attack targeting power supply of the hospital;

This attack could be partially **mitigated** if the following practices had been considered:

- ✓ Proper network segmentation to support a secure, scalable infrastructure;
- ✓ Pairing the access control system with the CCTV system;
- ✓ Appropriately deployed intrusion detection system to detect early signs that an attack is in progress;
- ✓ Train staff to recognize suspicious emails, never open e-mail attachments from unknown senders;
- ✓ Limit the rate of allowed authentication attempts to thwart brute-force attacks;
- ✓ Limit user who can login from remote desktop.

Current status of SAFECARE

- ✓ **Focus groups** with in-house experts to identify functional requirements related to threat prevention, threat identification, incident response and mitigation.

Descriptions of incident response processes and profiles of security practitioners

- ✓ For the requirements derived from the incident response processes
  - a systemic approach is used to define inputs, parameters, outputs and internal processing rules.

Thank you !

More details available on:

https://www.safecare-project.eu/

@SafecareP

SAFECARE Project

Eleni Darra

e.darra@kemea-research.gr

+302107710805 ext388