



# AIRBUS

## SAFEguard of Critical heAlth infrastruRE

# SAFECARE solution

David Lancelin

01/02/2021

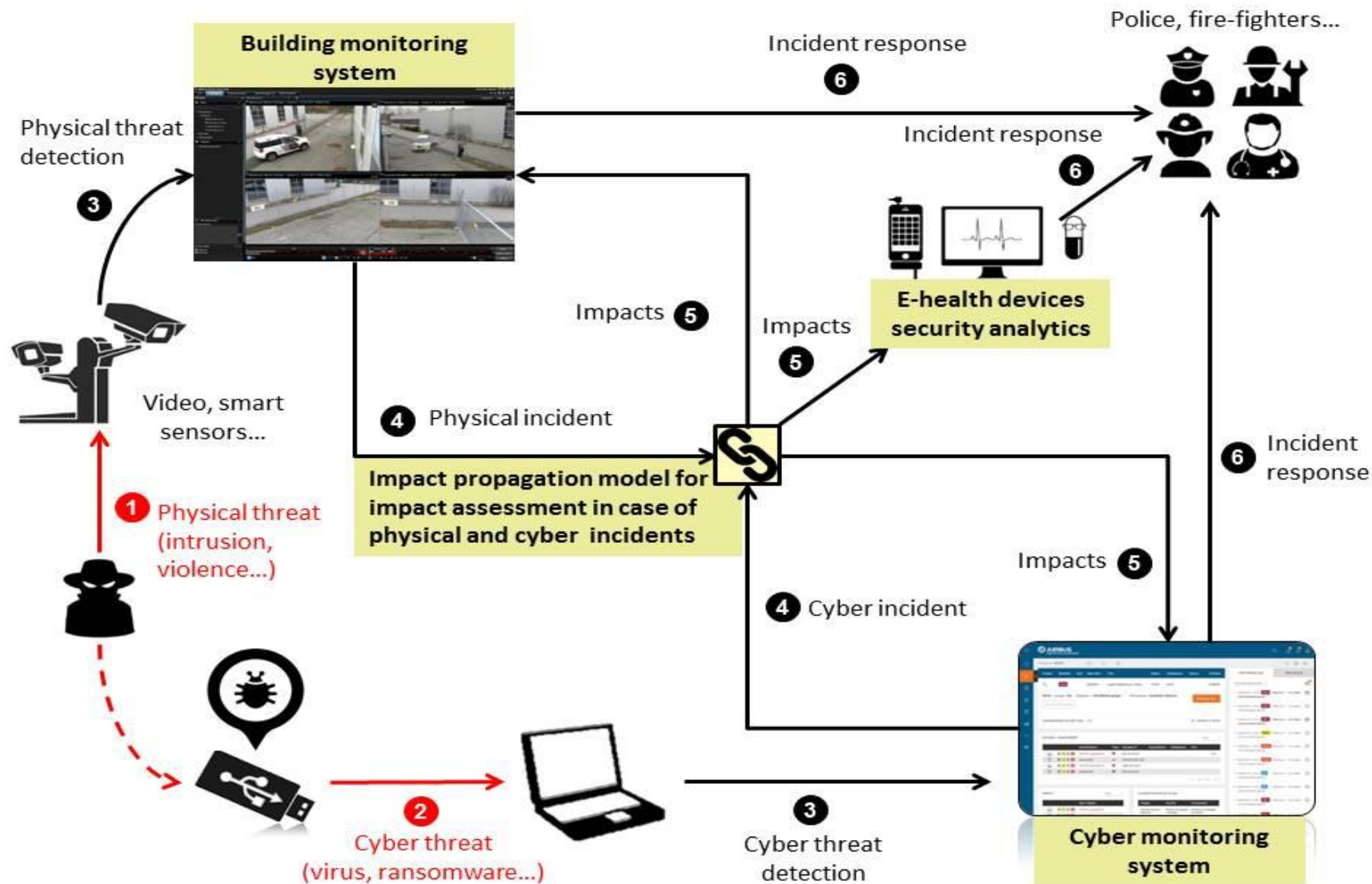
1. Global architecture overview
2. Physical security solutions
3. Cyber security solutions
4. Integrated cyber-physical security solutions



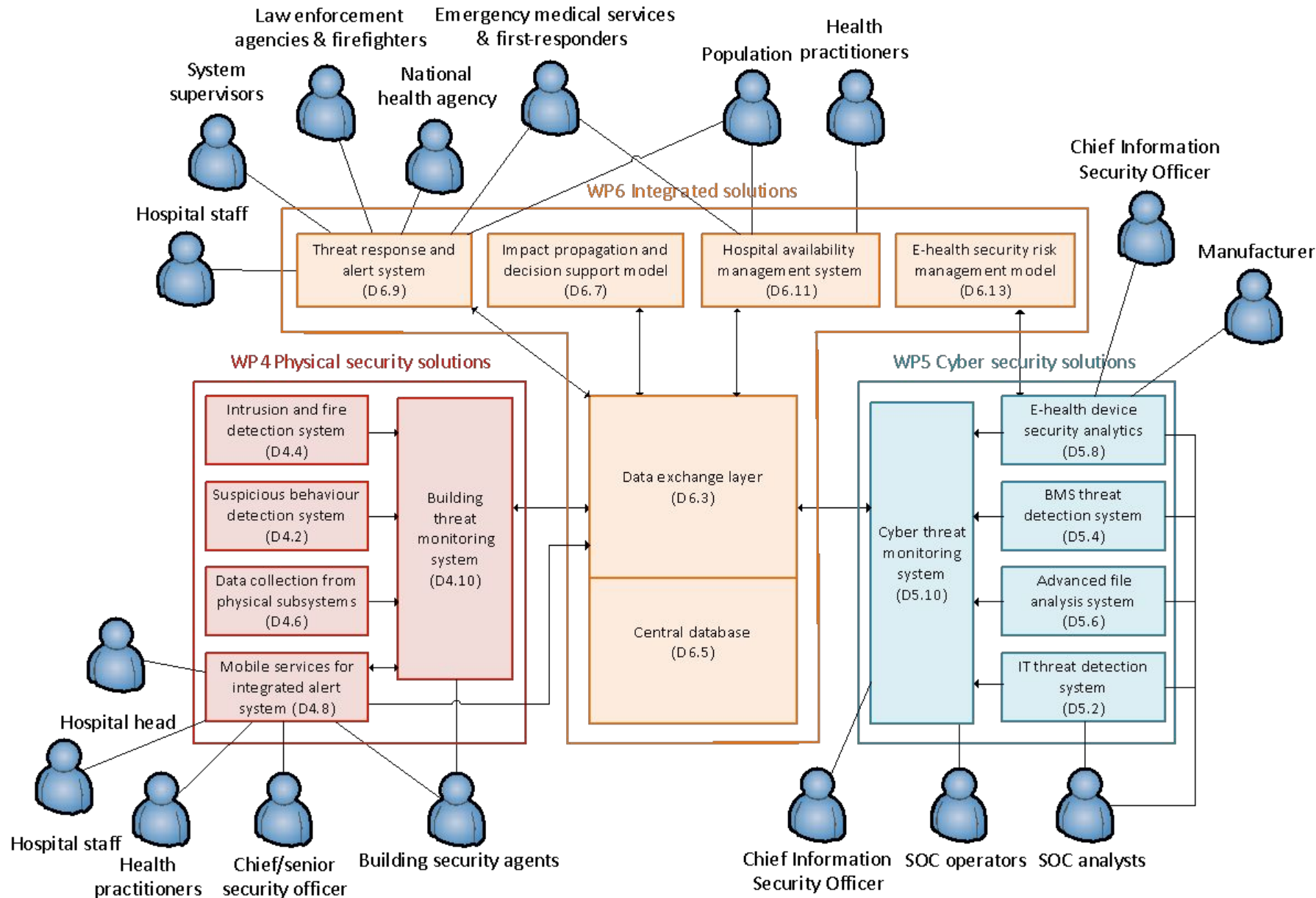
# 1. Global architecture overview



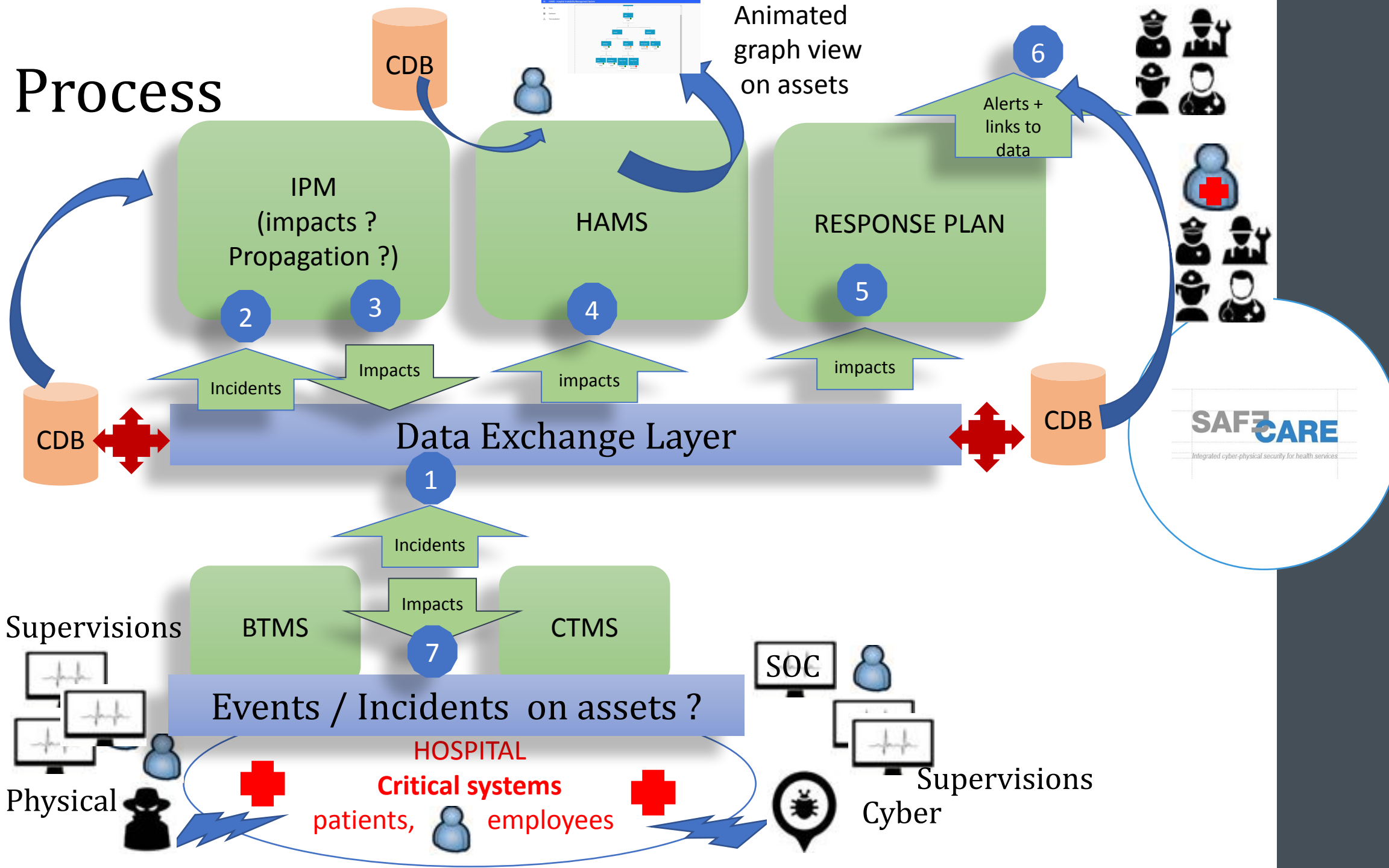
# Overall concept



# Global architecture



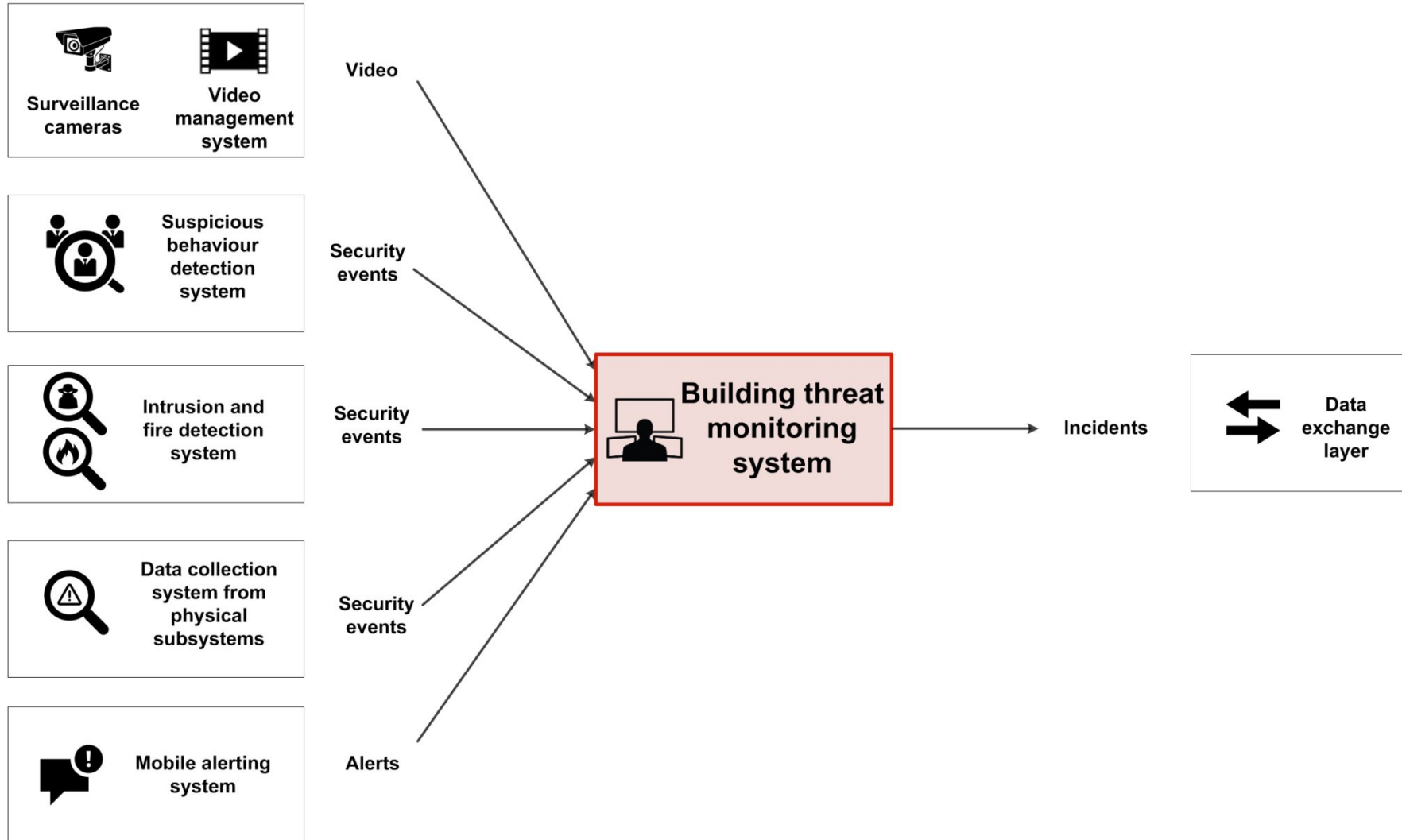
# Process



## 2. Physical security solutions

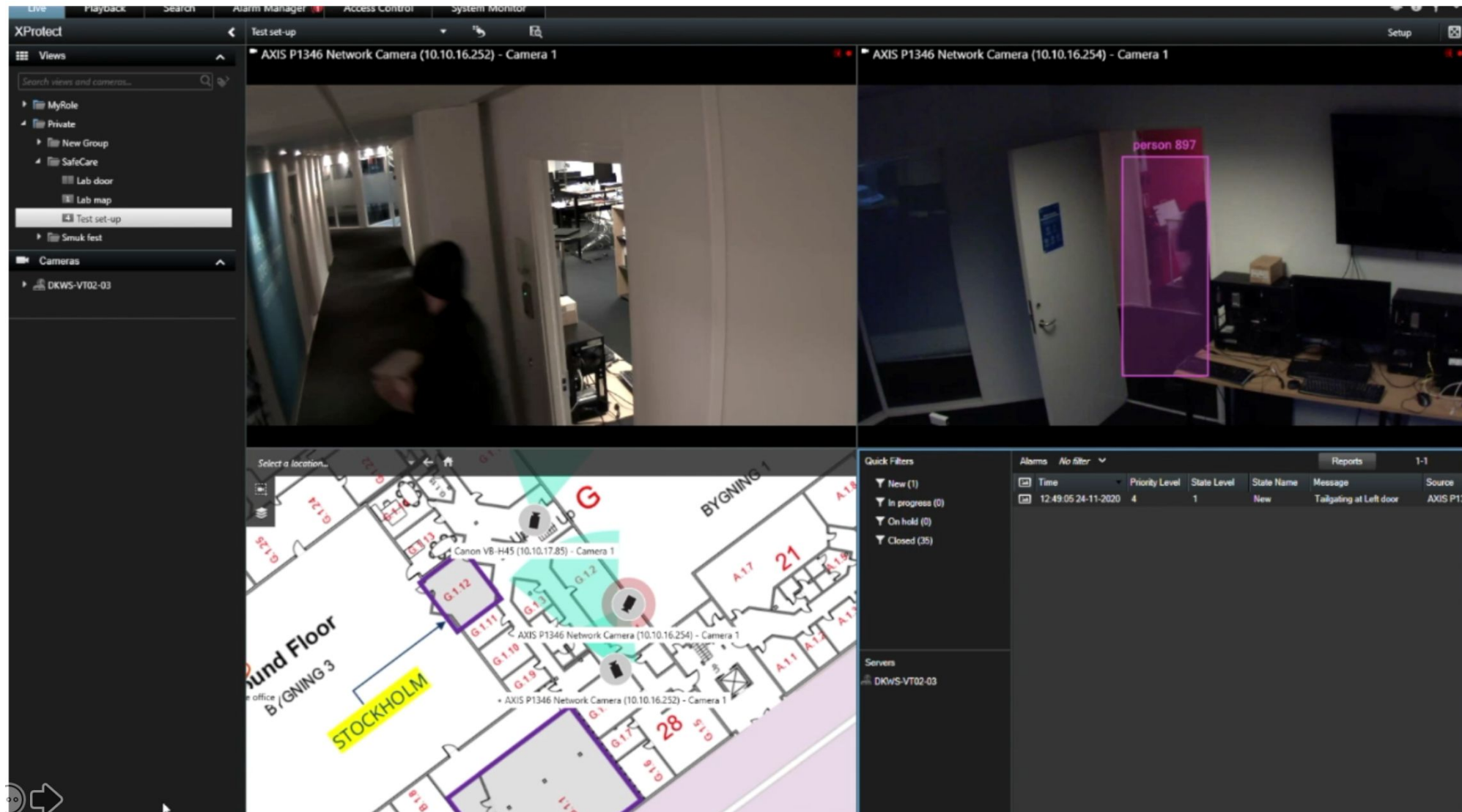


# Building threat monitoring system





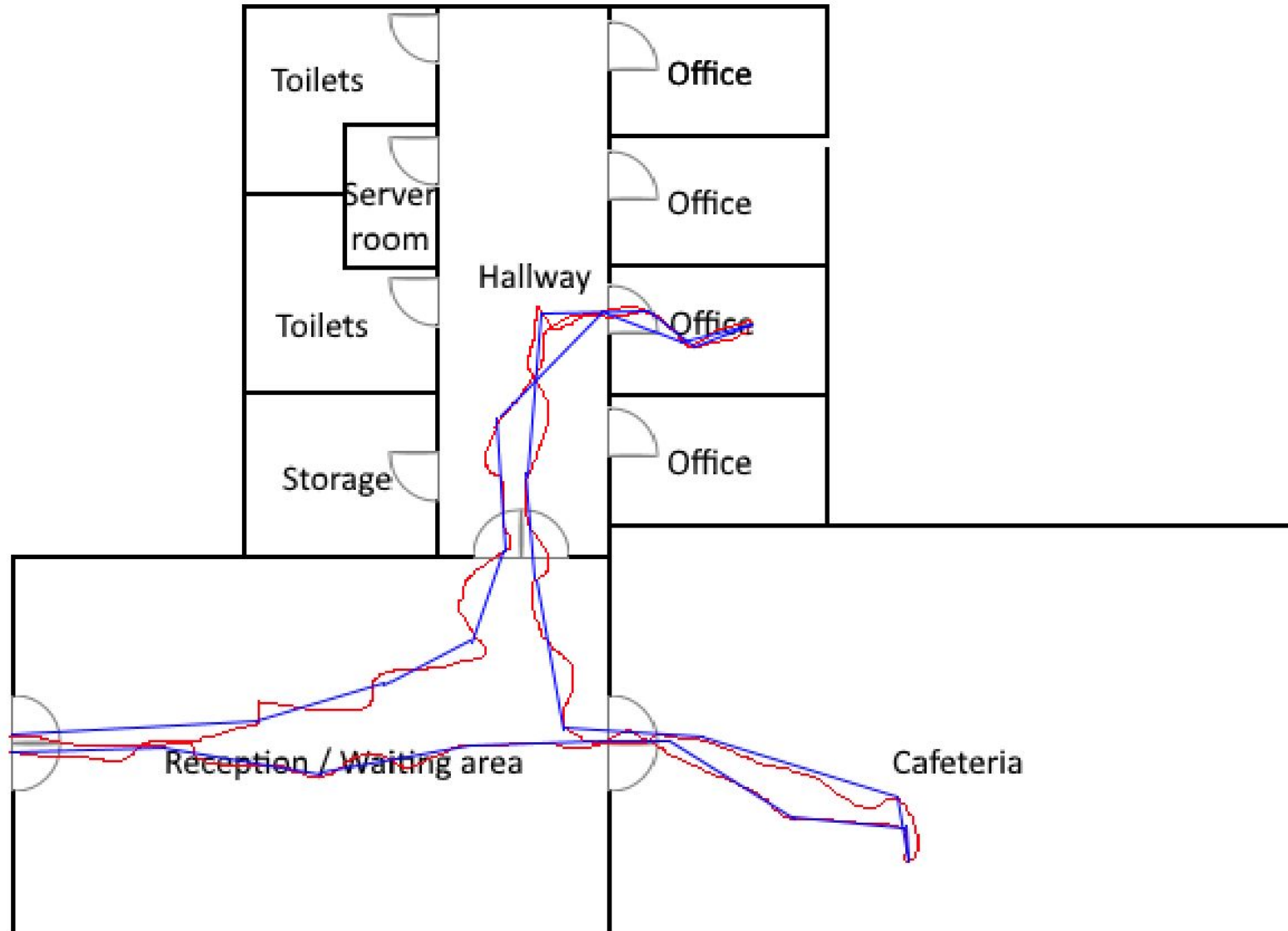
# Building threat monitoring system



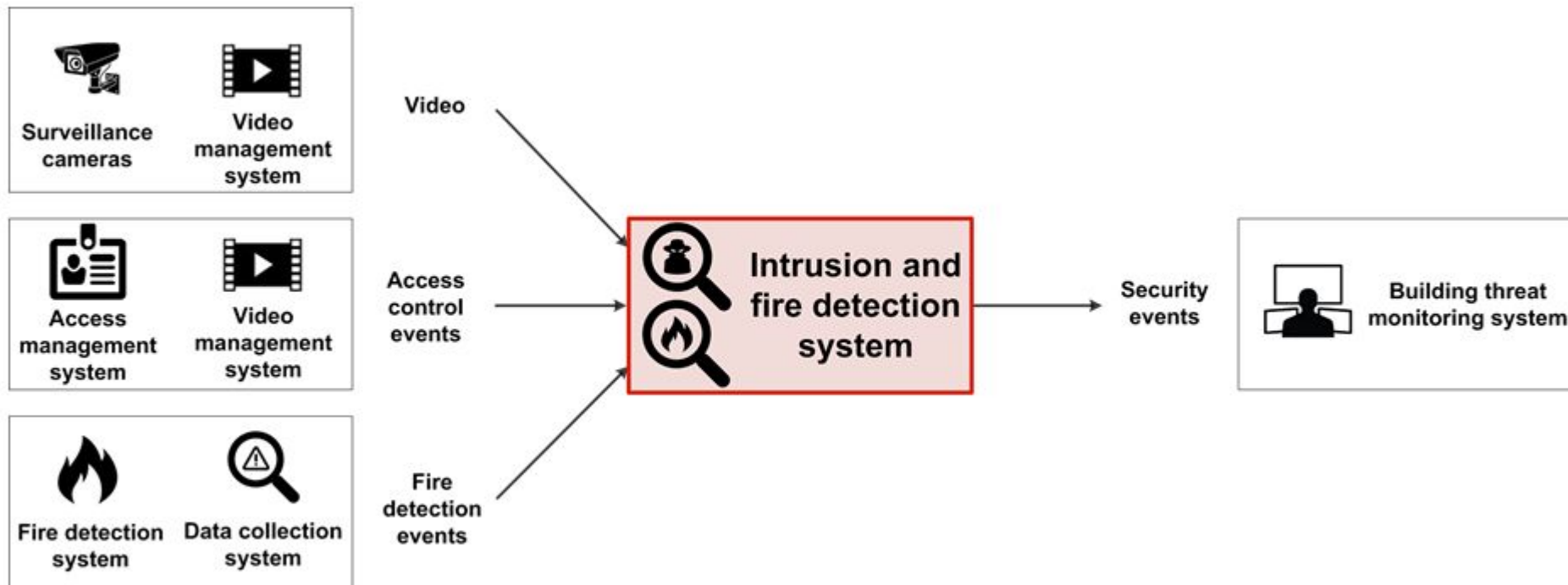
# Suspicious behaviour detection system



# Suspicious behaviour detection system



# Intrusion and fire detection system



# Intrusion and fire detection system



(a)



(b)

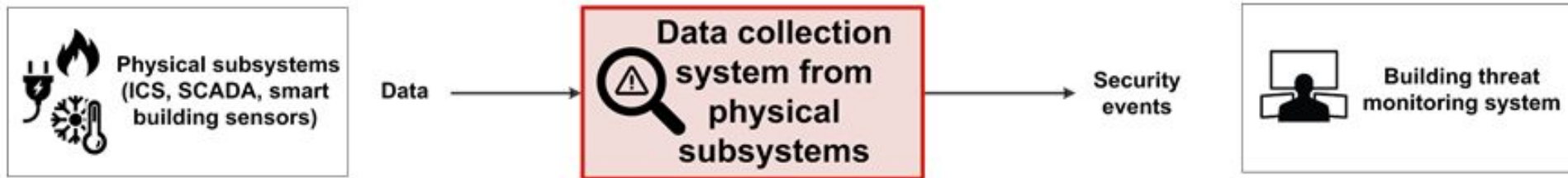


(c)



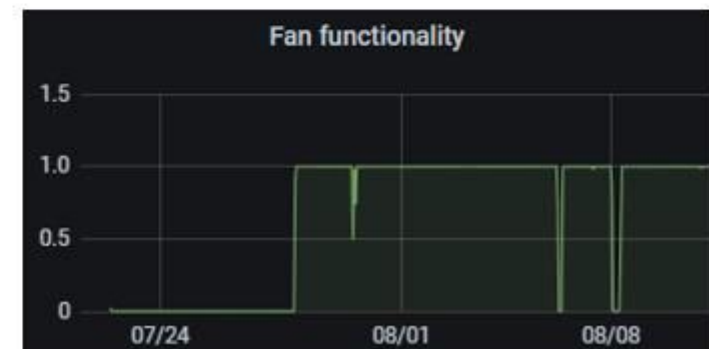
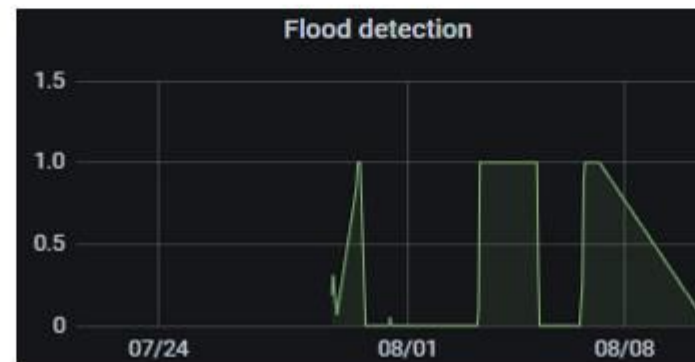
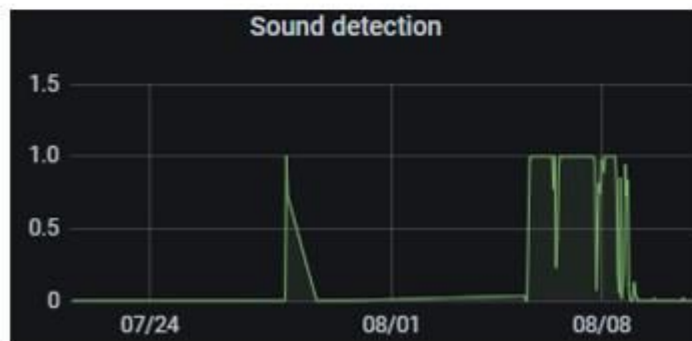
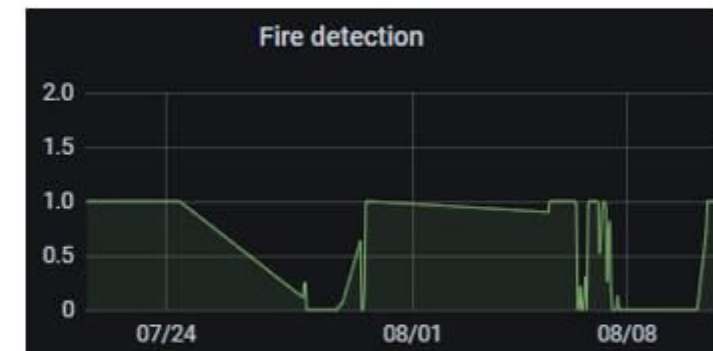
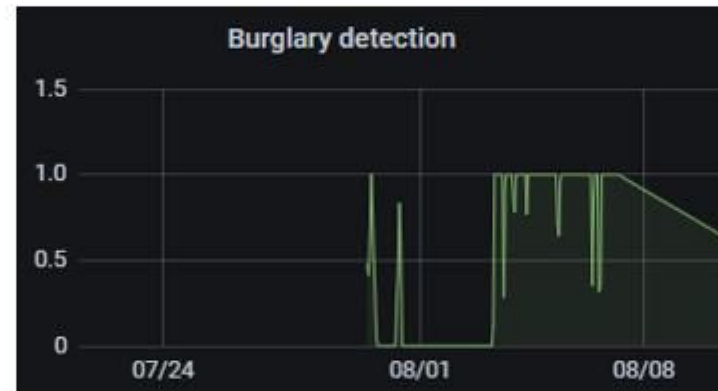
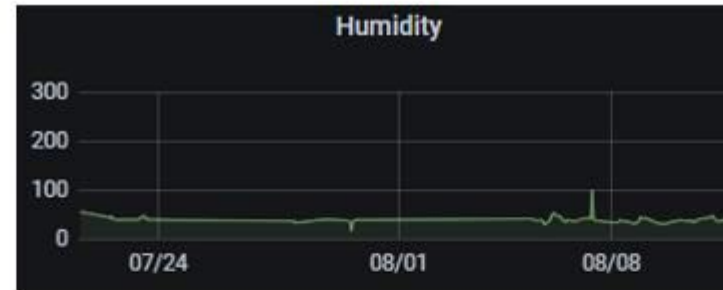
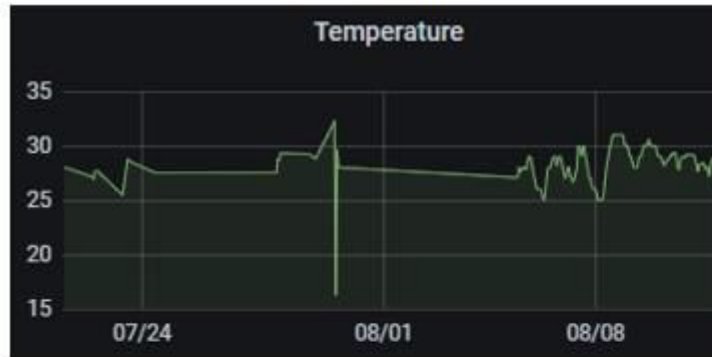
(d)

# Data collection system





# Data collection system

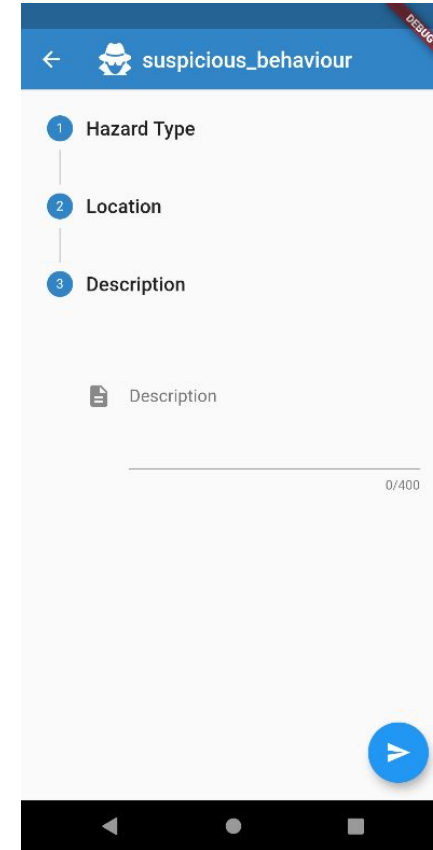
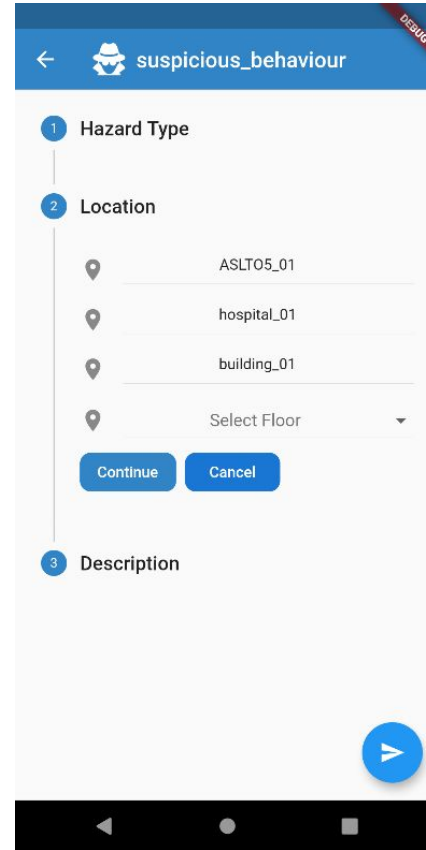
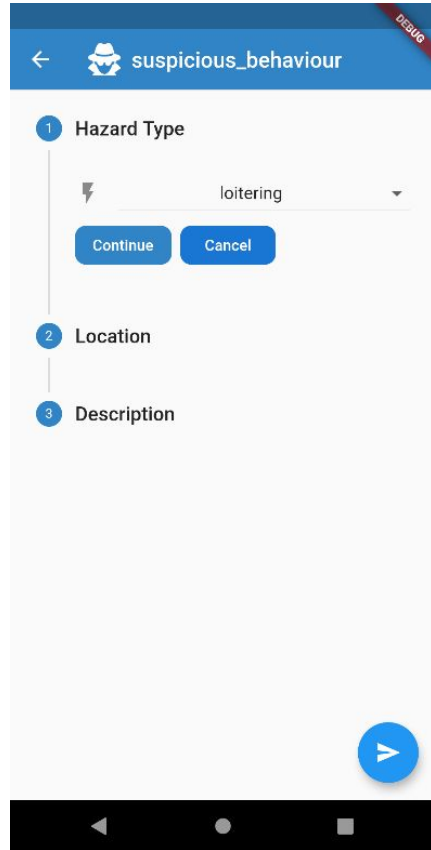
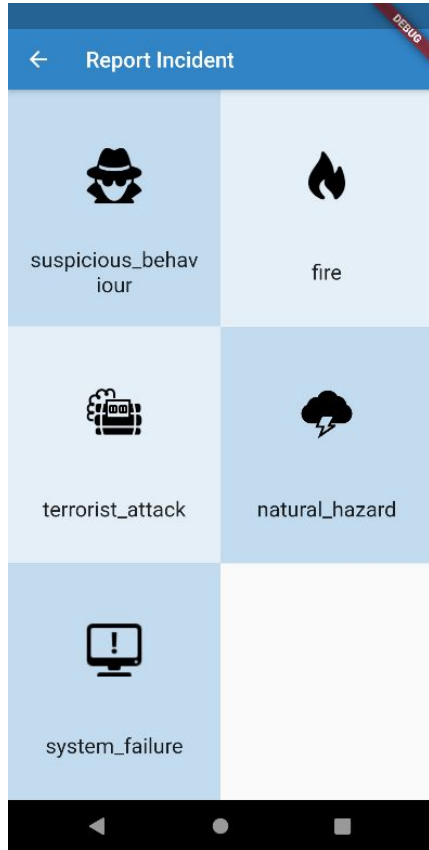


# Mobile alerting system

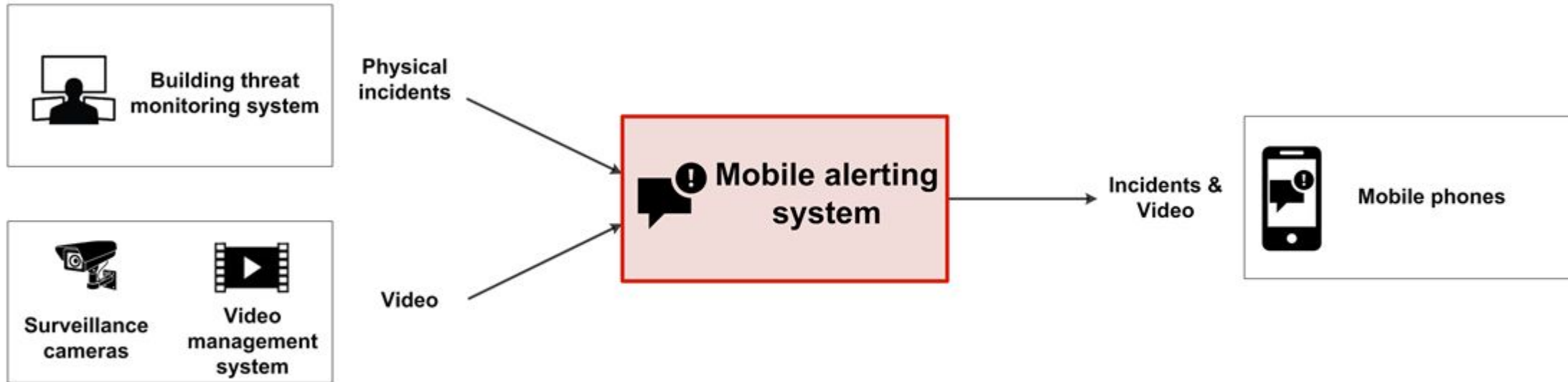




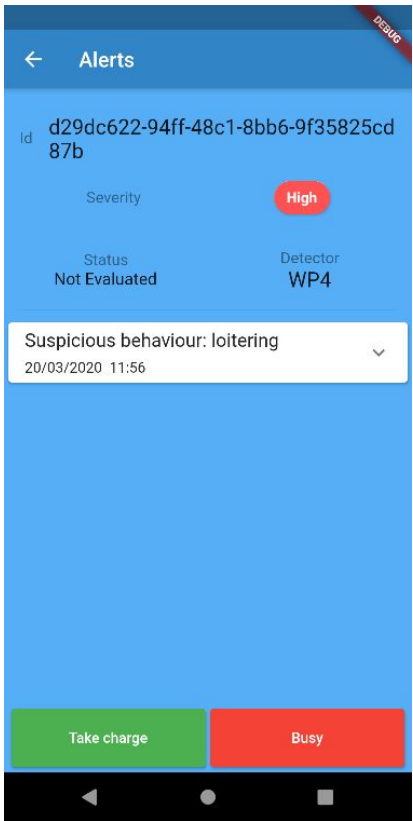
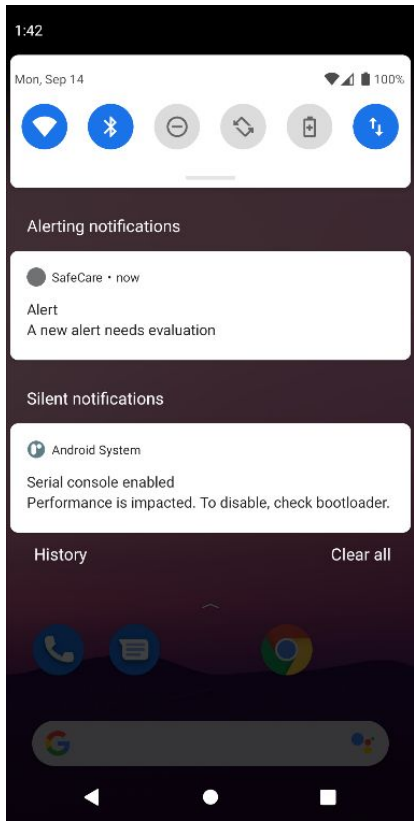
# Mobile alerting system



# Mobile alerting system



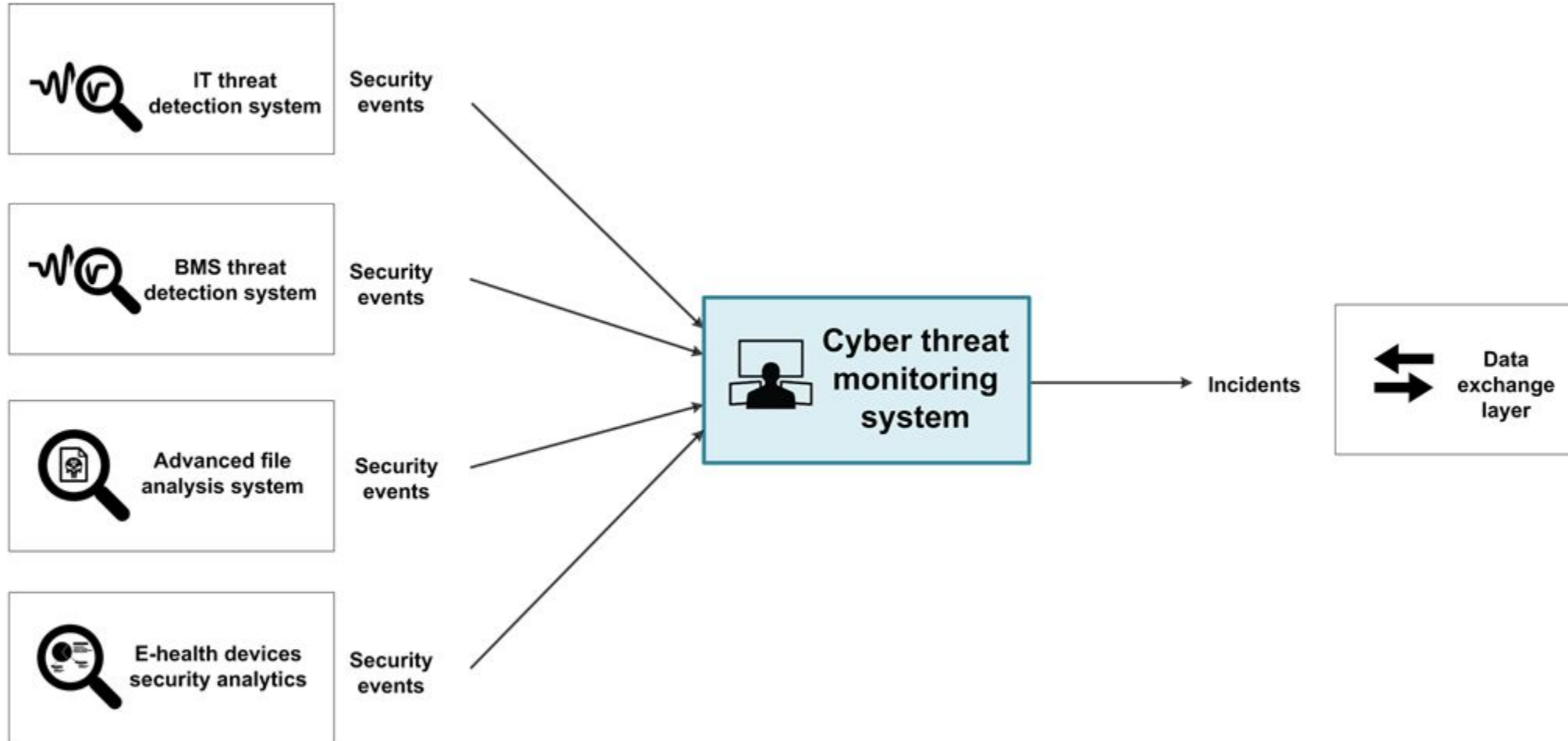
# Mobile alerting system



### 3. Cyber security solutions



# Cyber threat monitoring system



# Cyber threat monitoring system

**AIRBUS CYMERIUS**

/ Alerts and incidents

1-11 / 11 25

	Severity	Status	Identifier	Last Update	Title	Operators	Detector
<input type="checkbox"/>	High	Opened	01ES8RCRW78H4TC6CVJBZKEC2J	39d 3h	Malware detected		newgraylog1
<input type="checkbox"/>	Medium	Opened	01ES4V1KJ3K9NGR2KAB8Q8E57T	40d 16h	Network scan		newgraylog1
<input type="checkbox"/>	High	Opened	01ES4SP67F1FMHMDGT0Y7SRP7	40d 16h	Attempted Administrator Privilege Gain		newgraylog1
<input type="checkbox"/>	Medium	Opened	01ES4SKSY7J04TV6ZP25N1VBXP	40d 16h	Network scan		newgraylog1
<input type="checkbox"/>	High	Opened	01ES4QBKV57S5DK6M5H0QDSF78	40d 17h	Attempted Administrator Privilege Gain		newgraylog1
<input type="checkbox"/>	Medium	Opened	01ES4Q6XMHFG5WFBDB603PGZBQ	40d 17h	Network scan		newgraylog1
<input type="checkbox"/>	High	Opened	01ES4PG4K9TGB24Q65X1RM6SDE	40d 17h	Attempted Administrator Privilege Gain		newgraylog1
<input type="checkbox"/>	Medium	Opened	01ES4PEZ6RPRQQ03MTEF4M6JB3	40d 17h	Network scan		newgraylog1
<input type="checkbox"/>	High	Opened	01EQH7641Y9Z3851XH7VDDW2HC	60d 17h	Malware detected		newgraylog1

**Malware detected**

**LAST OPERATOR EVENT**  
There are no elements available.

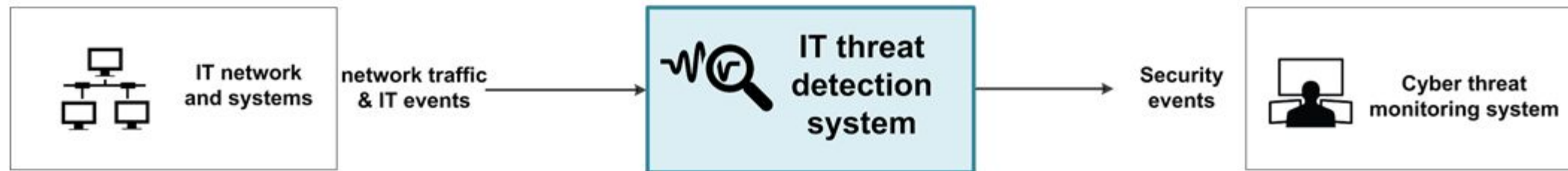
**ANALYSIS**  
No analysis written

**EQUIPMENTS (3)**

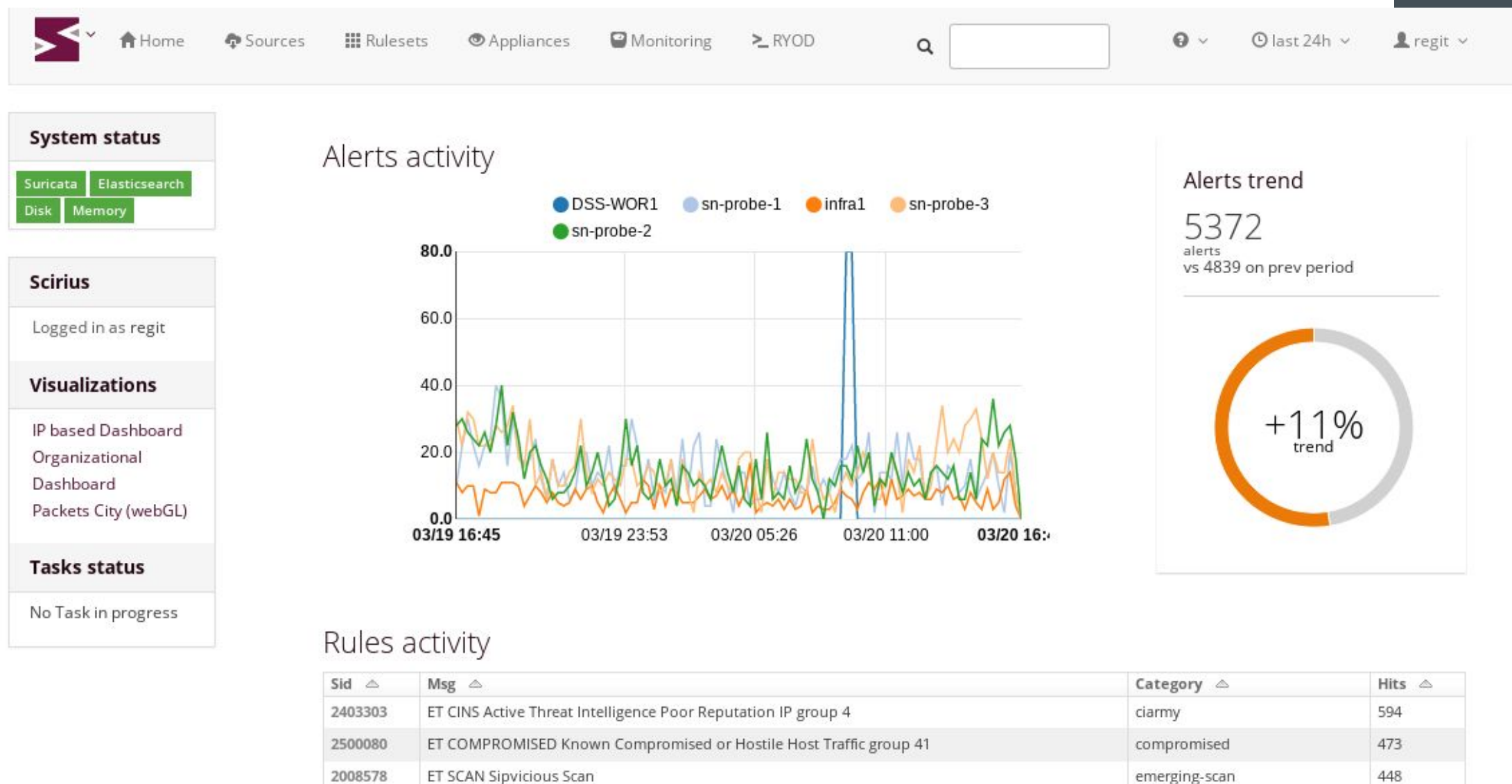
	Source	Target	Sensor
?	-	192.168.141.222	suricata
?	-	192.168.140.10	suricata
?	-	-	suricata

**REACTIONS**  
There are no elements available.

# IT threat detection system

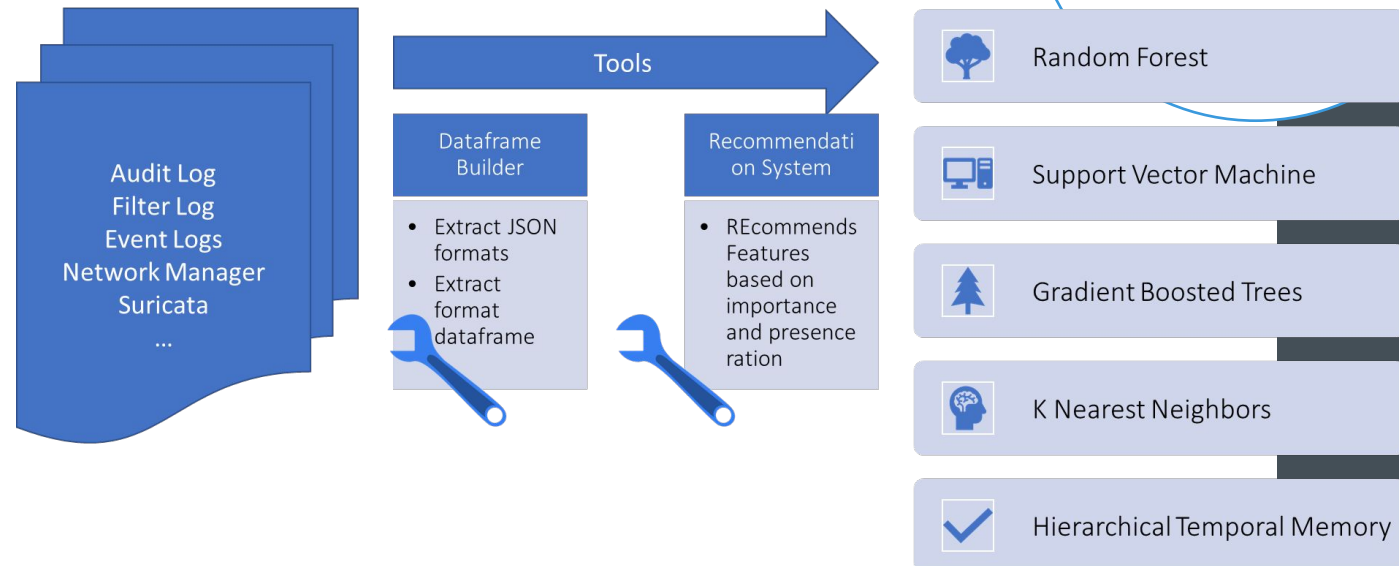
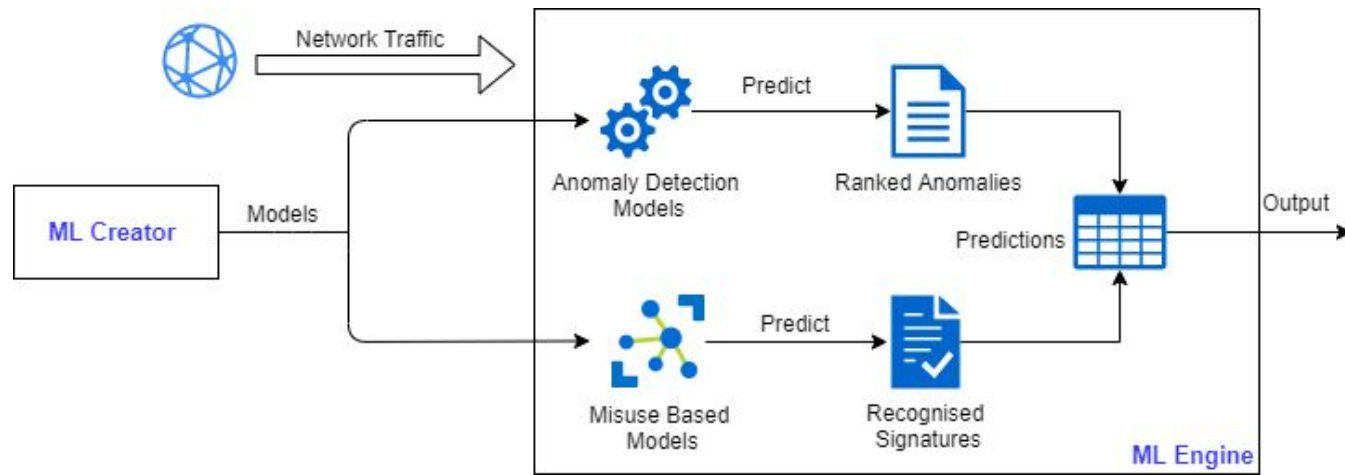


# IT threat detection system





# IT threat detection system



# BMS threat detection system



BMS: Building Management System

# BMS threat detection system

Dashboard
Network
Events
Sensors
Settings

admin

Network map

Reload
Options
Import | ▾
Export | ▾
Tab | ▾
Monitored networks | ▾
Filter
Highlight
Threats | ▾
Scans | ▾

?

 Help

Default
Lab
DHCP Traffic
Siemens
BACnet (MSTP)
LIS2
HL7
HL7v3
HL7\_FHIR
DICOM
POCT-1A

POCT-1A filtered
GEMNet
OPAD
DCMP
PHILIPS\_DATA\_EXPORT
GE\_RWHAT
Getinge
Omnicell
Baxter Sigma

Draeger Infinity
AbbottXceed
Meraki
Risk
Vulnerabilities

179 hosts
Filters: Any Protocol="N..." ✕
Highlights: Any Protocol... ✕

08:00:27:39:60:A5 (PcsCompu)

Role

Other roles

Vendor and model

Other vendors/models

Client protocols

Server protocols

Labels

Universal gateway

Medical information system

Ensemble

Epic

HL7v2 (TCP)

NotAKnownOne (TCP 2575)

HL7v2 (TCP)

NotAKnownOne (TCP 2575)

hl7\_application=EPIC

hl7\_application=EnsembleHL7

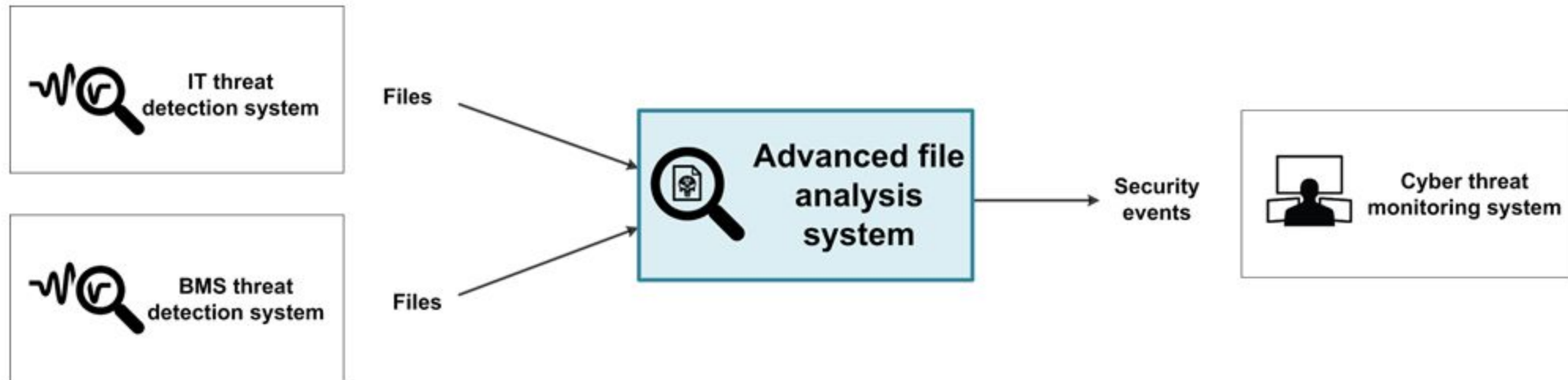
hl7\_facility=EPICADT

hl7\_version=2.3

Network map

Copyright (C) 2009-2020 Forescout (v. 4.1.0)

# Advanced file analysis system




# Advanced file analysis system

AIRBUS

Home Submit a file Search Documentation Terms of Service About

Orion Malware test user

Risk

  
Severe

Dynamic Environment

Windows 7

60 sec

Actions

Export PDF

View reports history

Export IOCs

Search MISP events

Add to whitelist


Resubmit

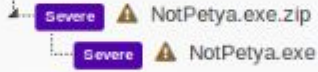
Download

More about


Overview Network Whitelist Antivirus Rules Scanner Dynamic

File Information



MD5	e27e6f066b0b439dbdabc50198a0c74e	File Size	305.9 KiB
SHA1	ccd5d3d0f3fac1614560ebcdd48885888c3fc470	First submission	Tue 19 Jan 2021 12:14:49
SHA256	e6231b7ffd231fd19f63cf670dd8fbdabe8635e5b445e78b8dbdc702f4042b05	Last updated	Tue 19 Jan 2021 12:20:49
File Type	Zip archive data, at least v2.0 to extract	Start analysis	Tue 19 Jan 2021 12:15:02
Filename	NotPetya.exe.zip	End analysis	Tue 19 Jan 2021 12:20:49
Payloads tree			

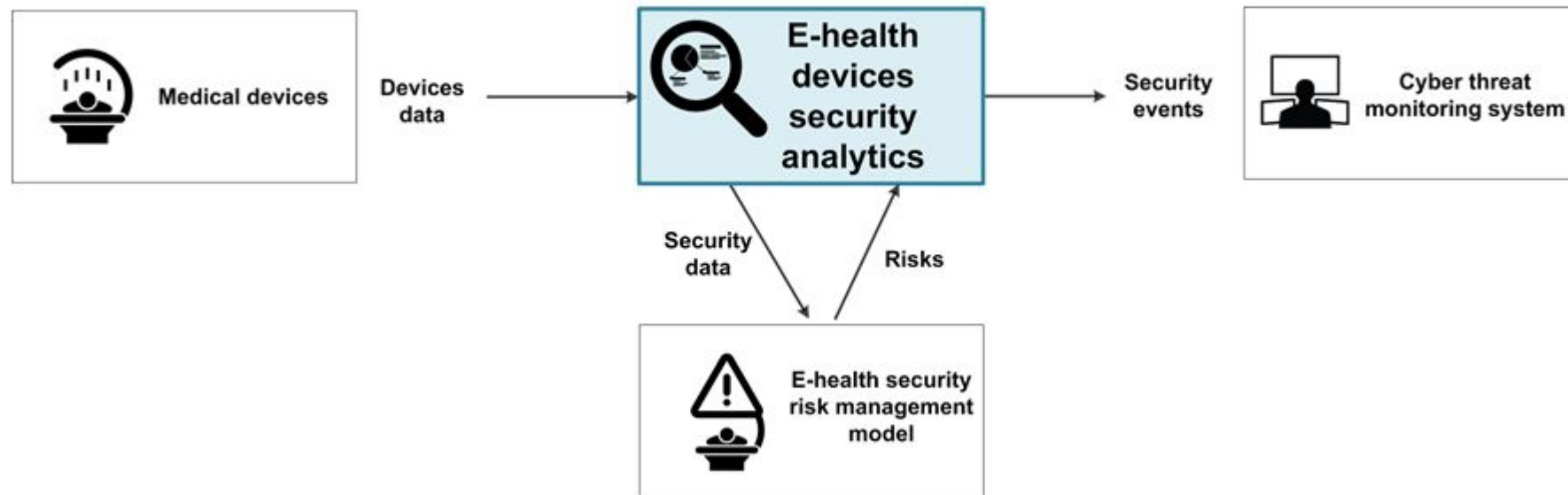
Communication



Domain/IP	Payload(s)
10.0.101.0	NotPetya.exe
10.0.101.1	NotPetya.exe
10.0.101.254	NotPetya.exe



# E-health devices security analytics





# E-health devices security analytics



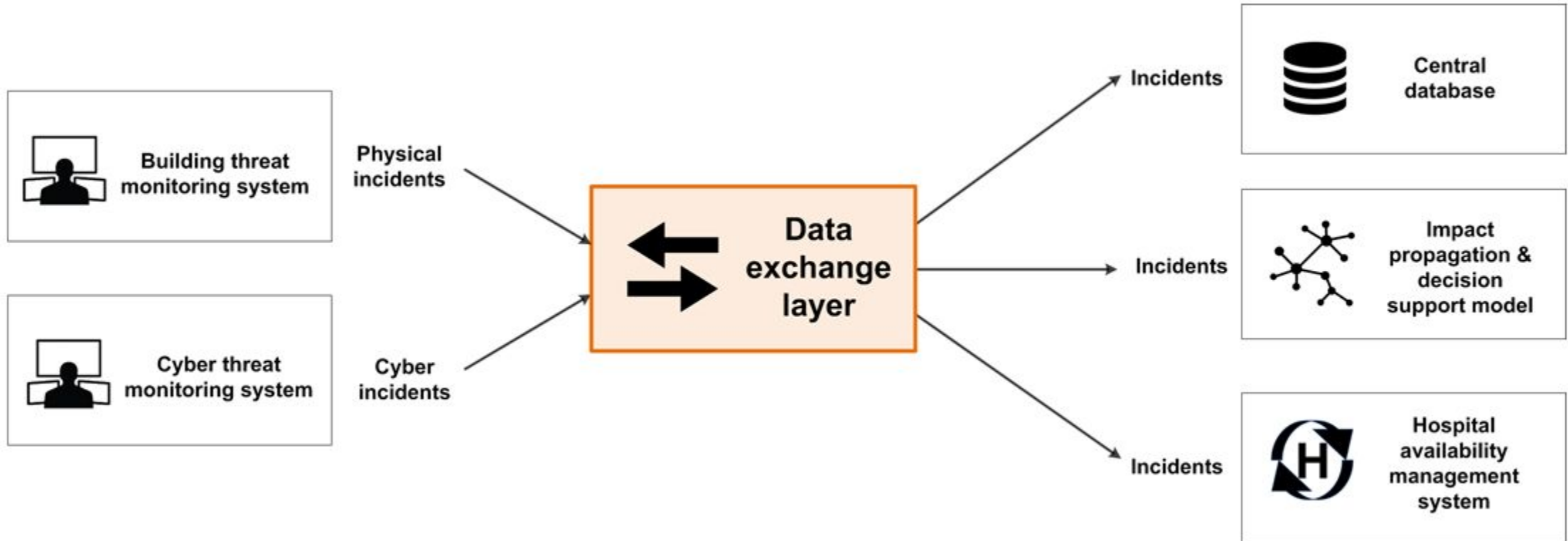
**ARE**  
ity for health services

## 4. Integrated cyber-physical security solutions

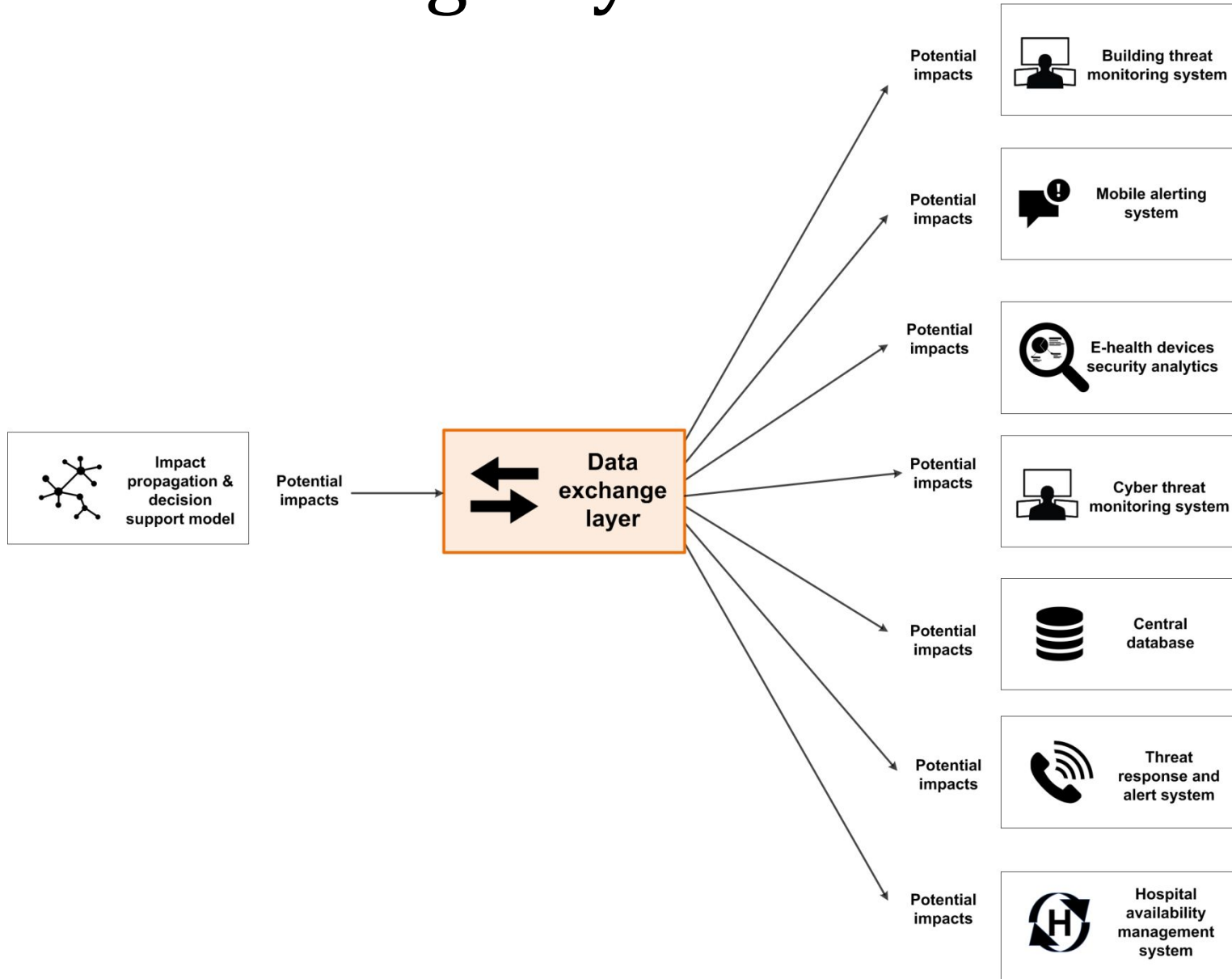




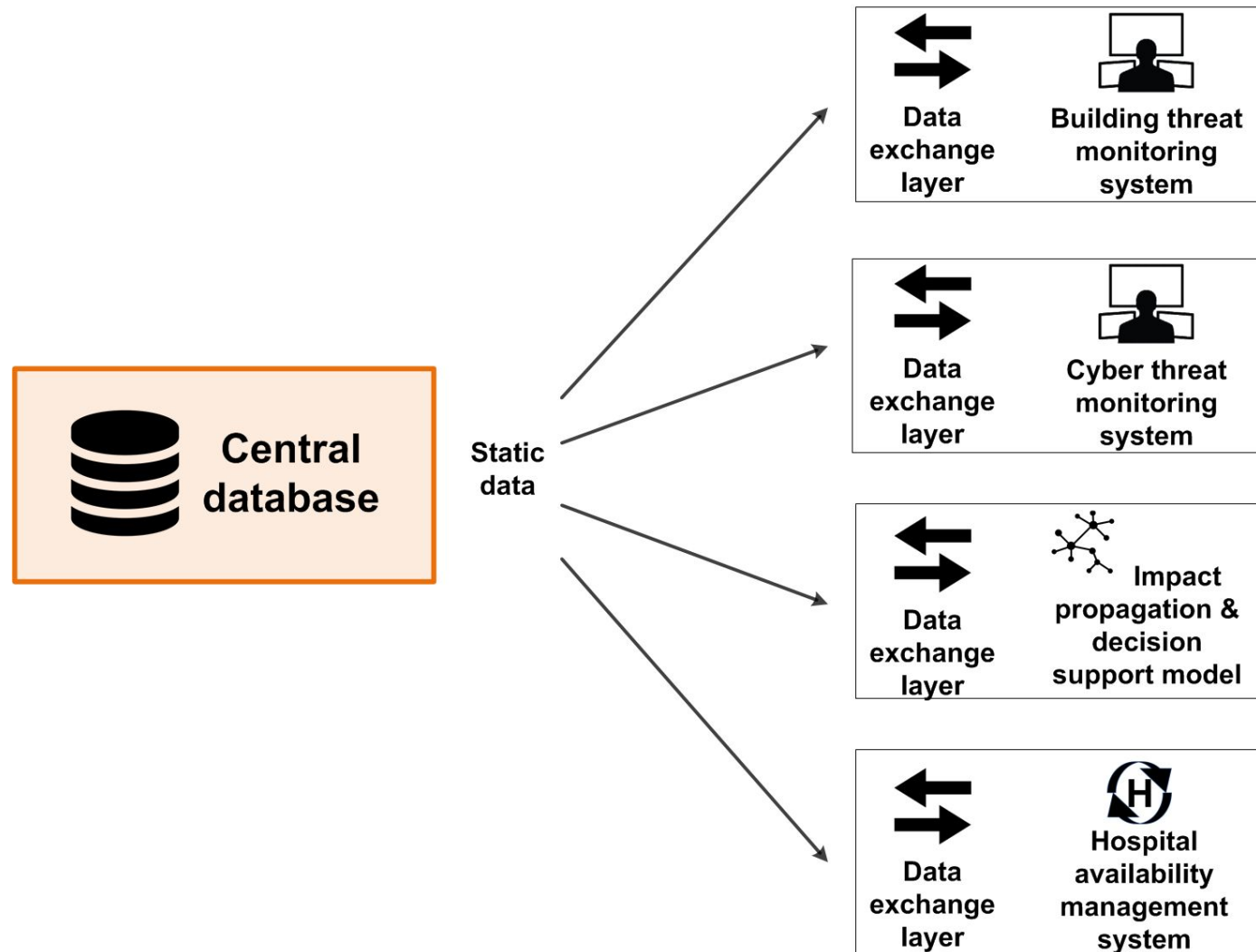
# Data exchange layer



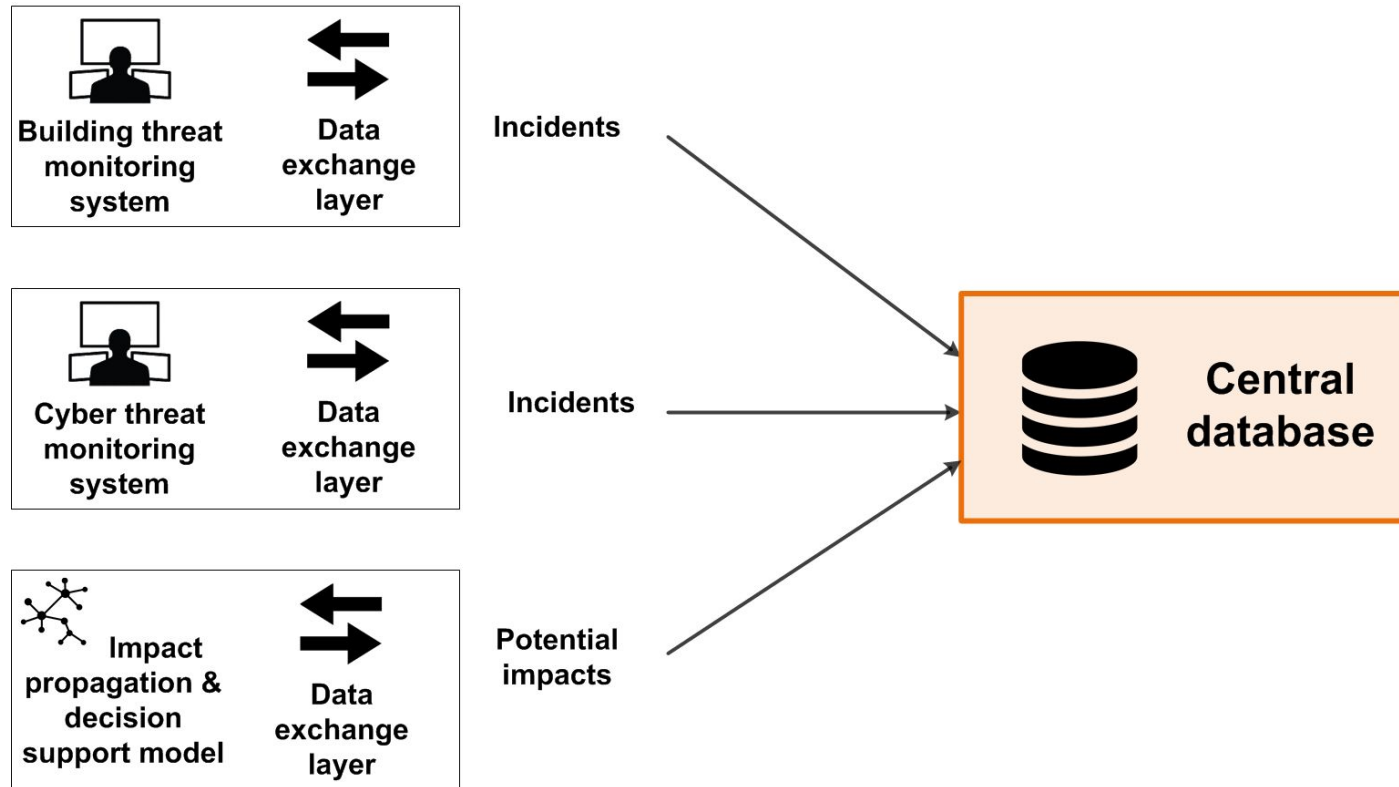
# Data exchange layer



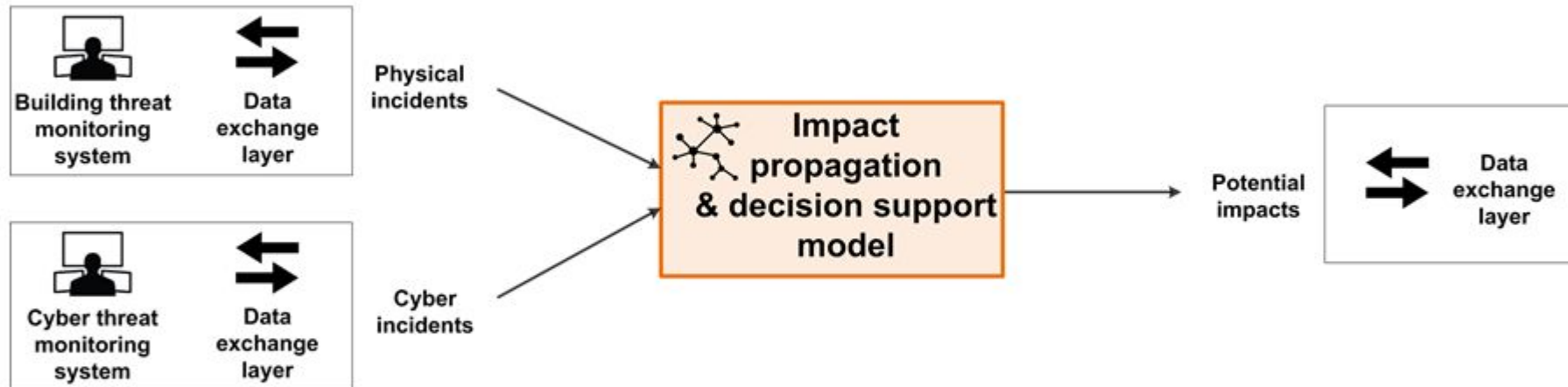
# Central database



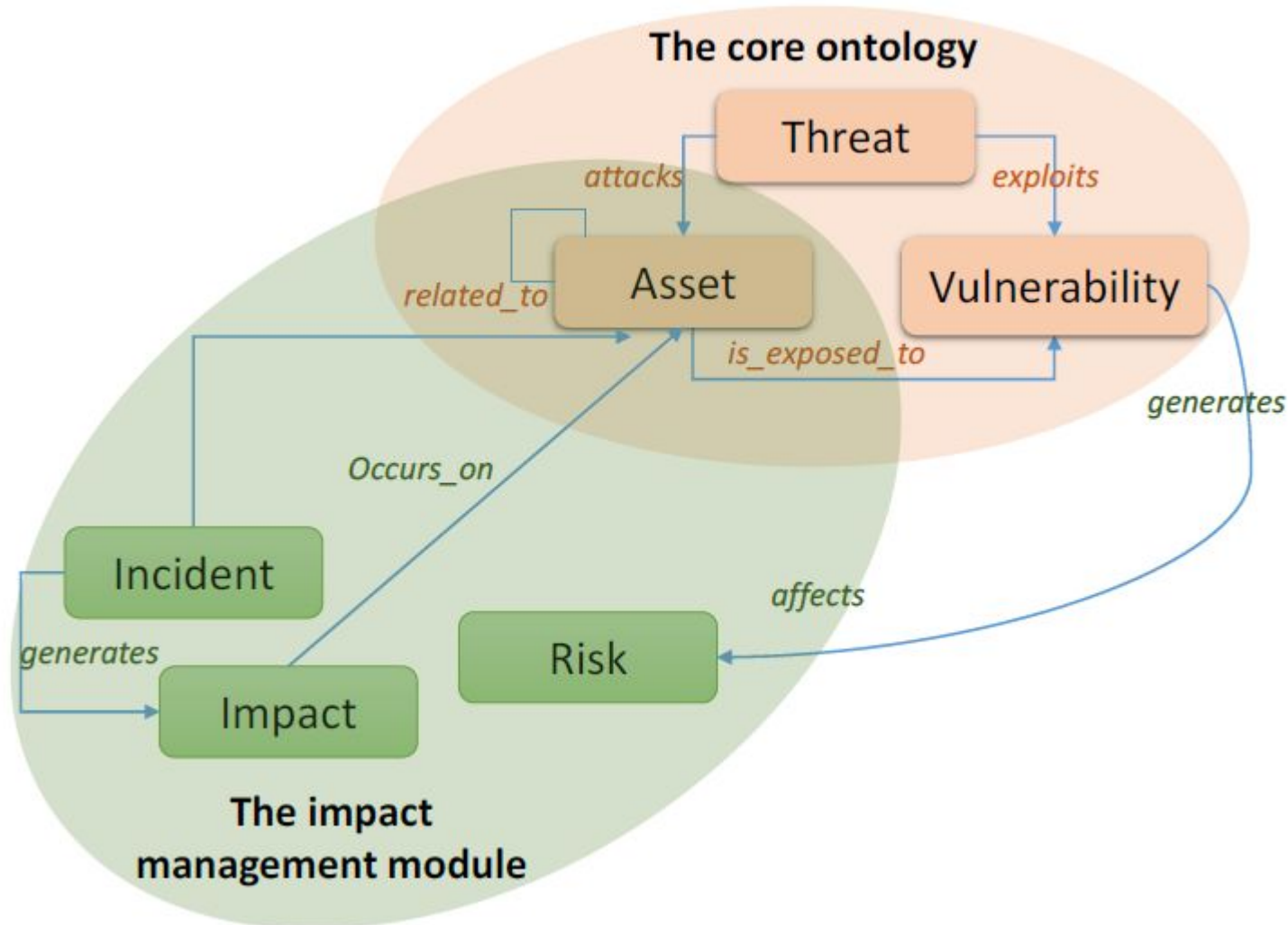
# Central database



# Impact propagation model and decision support model



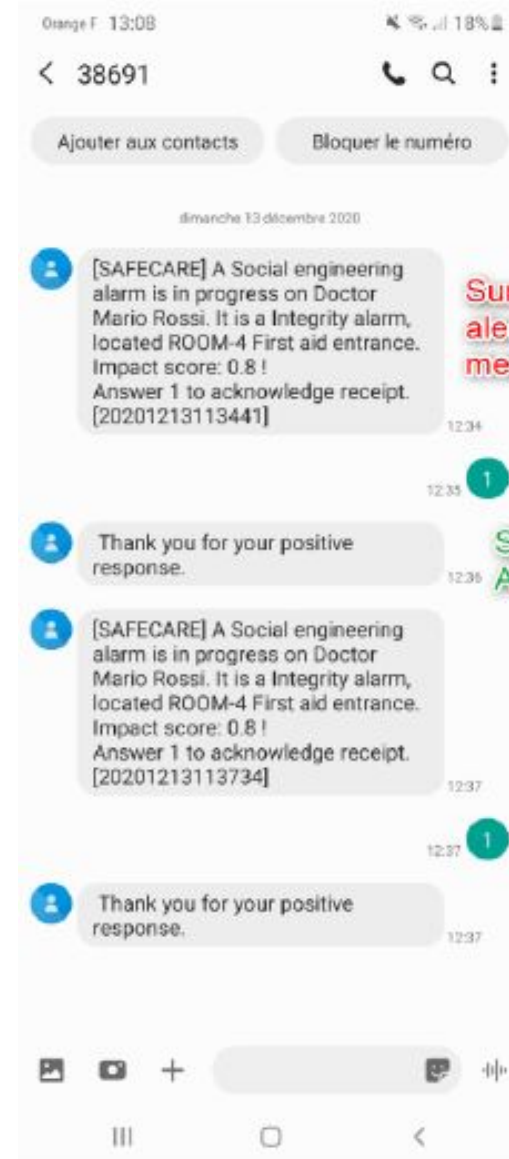
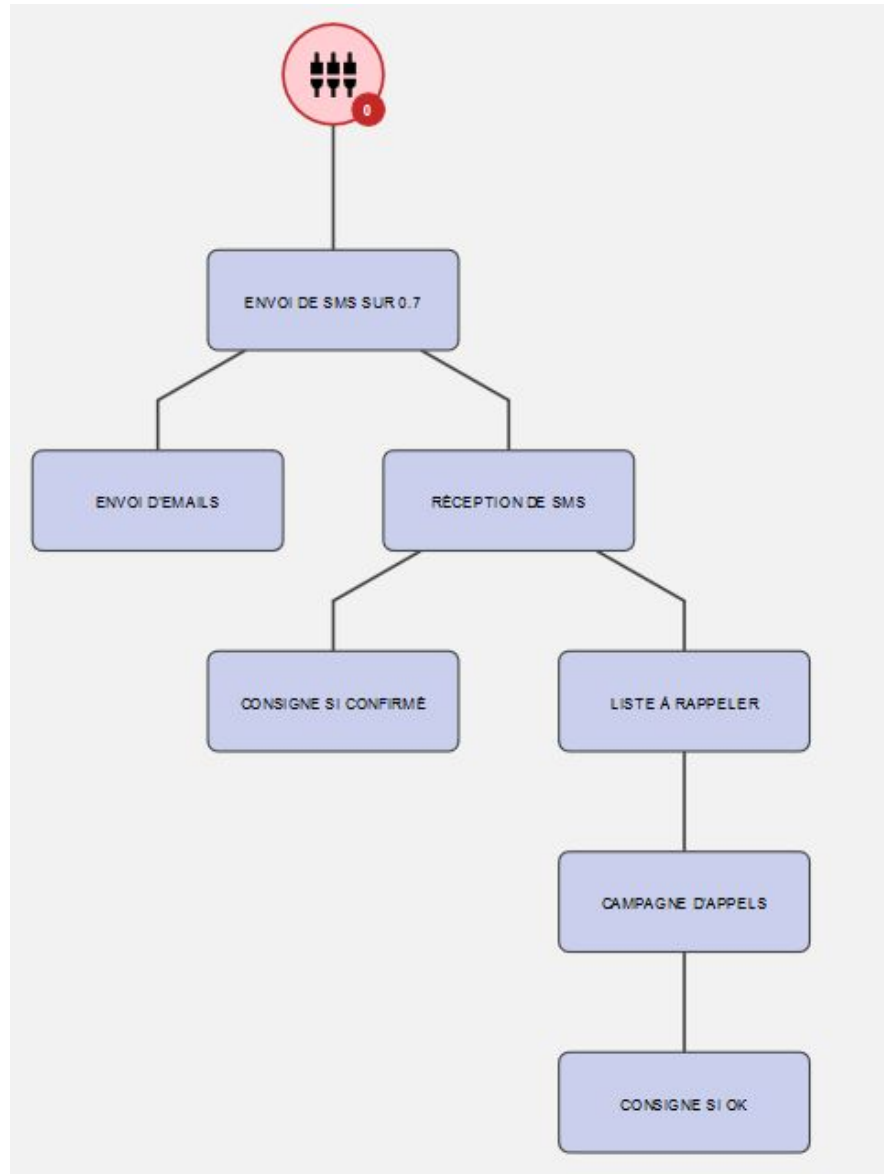
# Impact propagation model and decision support model



# Threat response and alert system

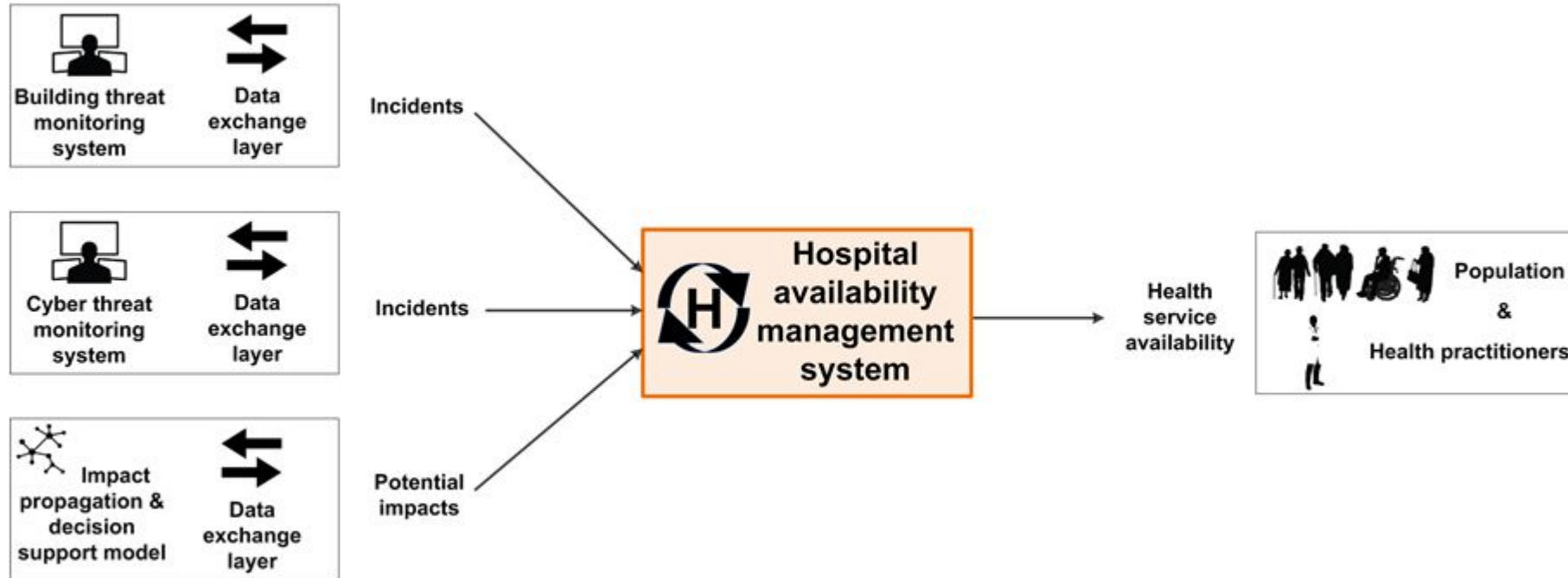


# Threat response and alert system





# Hospital Availability Management System



# Hospital Availability Management System

Home

Dashboard

Tree visualisation

Incidents & Impacts

Logout

HAVE

HAMS - Hospital Availability Management System

SAFECARE

Stop and prevent harm in health care

Main Building

Facility Status

REFRESH VIEW

UPDATE GDB

DEPARTMENTS

OPERATIONS

Department availability

Filter

Department	Availability	Status	Stability	Bed availability	Staff availability	Asset	Actions
Cardiology	Available	green	stable	20	10	▼	✎
Neurology	Available	green	stable	5	5	▲	✎

Resource ID	Resource Name	Availability	Status	Stability	Actions
310131	Cardio Monitor	Available	green	stable	✎
310132	Oxygen System	Available	green	stable	✎
310133	Magnetic Resonance Imaging	Available	green	stable	✎

Rows per page: 10 1-3 of 3 < >

Operating Rooms	Available	green	stable	1	4	▼	✎
Surgery	Available	green	stable	3	4	▼	✎

Rows per page: 10 1-4 of 4 < >

# E-health security risk management model



# Thank you !

More details available on:

- Our website: <https://www.safecare-project.eu/>
- Twitter: @SafecareP
- LinkedIn: SAFECARE Project

*David Lancelin*  
*david.lancelin@airbus.com*

