SAFECARE

Integrated cyber-physical security for health services

AIRBUS · isep Instituto Superior de Engenharia do Porto · FORESCOUT · Beia CONSULT INTERNATIONAL · milestone

SAFECARE – Detection Systems

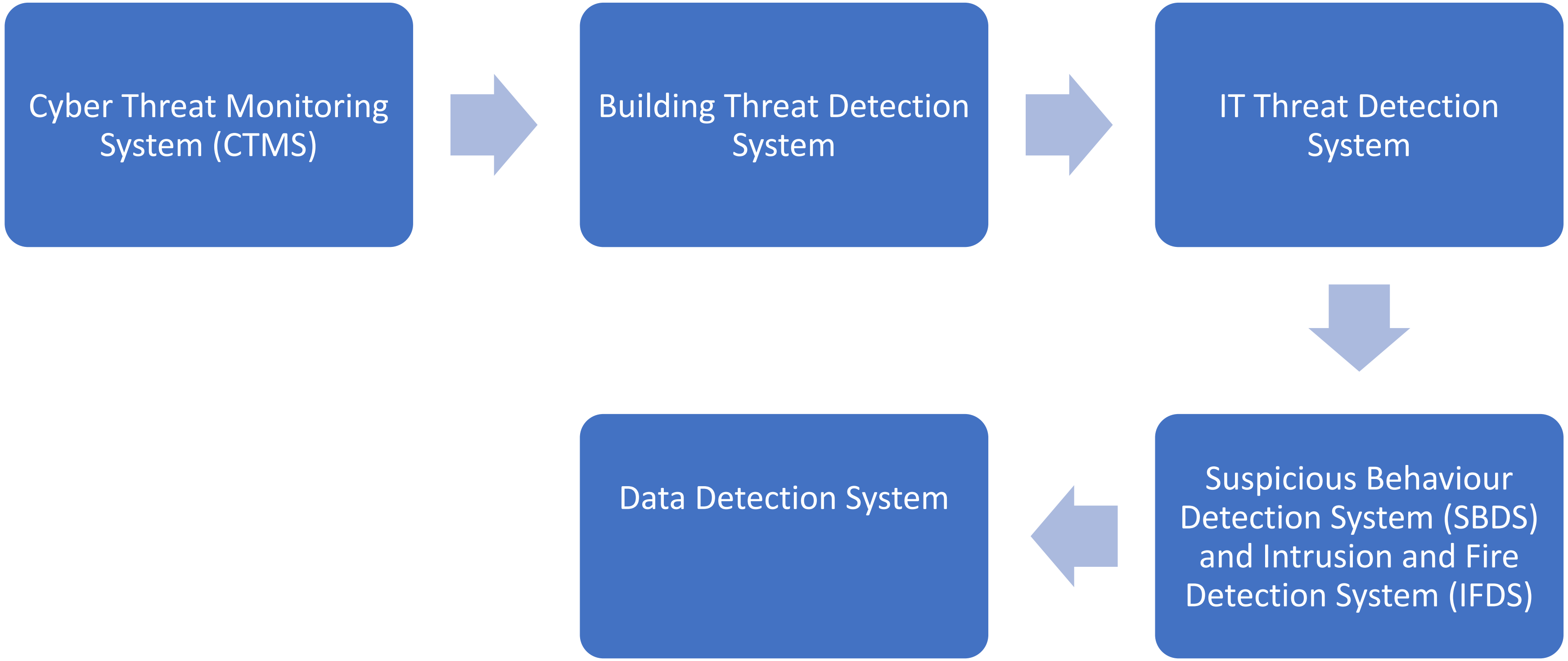
MARI-ANAIS SACHIAN

BEIA CONSULT INTERNATIONAL

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

Summary



Cyber Threat Monitoring System (CTMS)

Building Threat Detection System

IT Threat Detection System

Suspicious Behaviour Detection System (SBDS) and Intrusion and Fire Detection System (IFDS)

Data Detection System

SAFECARE

Integrated cyber-physical security for health services

SAFECARE

Integrated cyber-physical security for health services

Cyber Threat Monitoring System (CTMS)

Cyber Threat Monitoring System

CTMS is the cybersecurity user interface of the SAFECARE global solution for monitoring cyber threats.

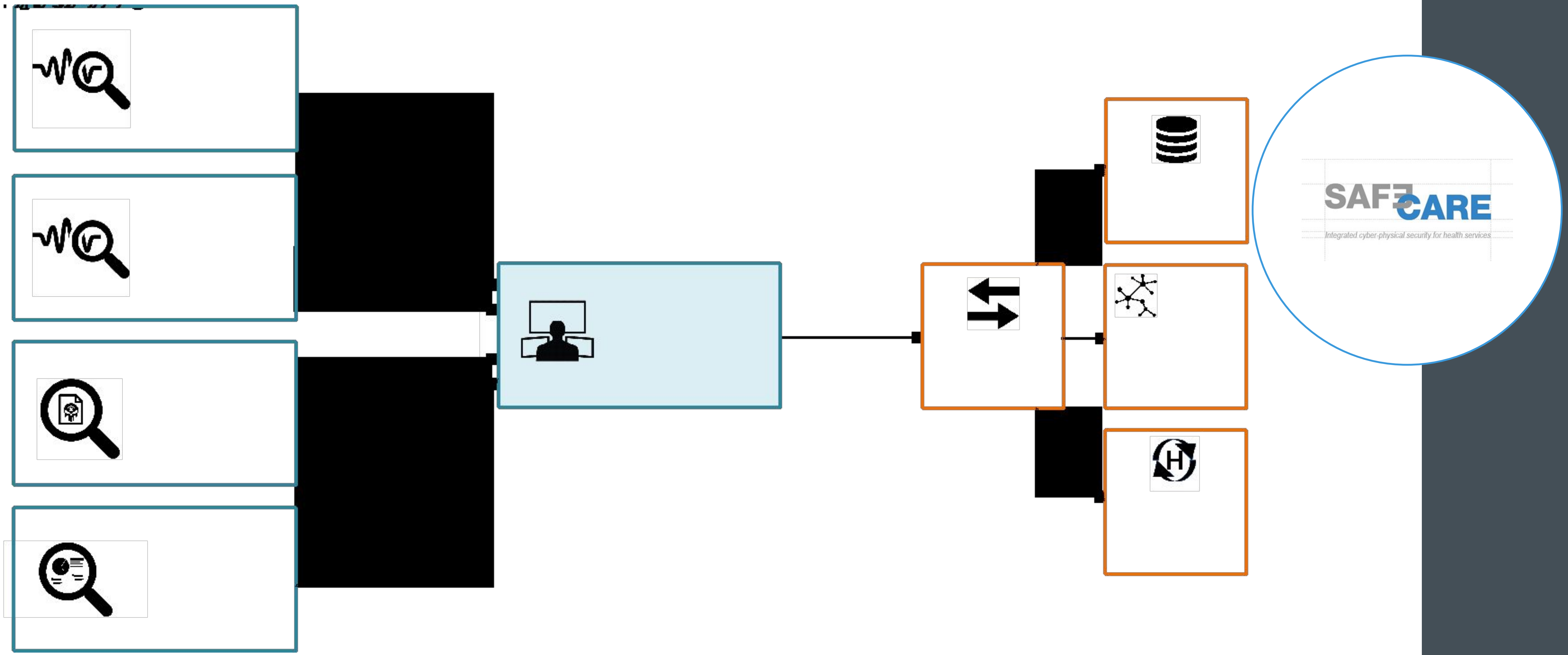
CTMS **centralizes and monitors the alerts** from the IT, BMS and medical networks, displays information in an organized way and provides **user-friendly interfaces** to SOC analysts and operators

SOC analysts and operators:

- correlate information between IT, BMS and medical networks
- analyze and qualify cyber threats
- visualize impacts of physical and cyber incidents on assets
- improve response capacities and shorten time response

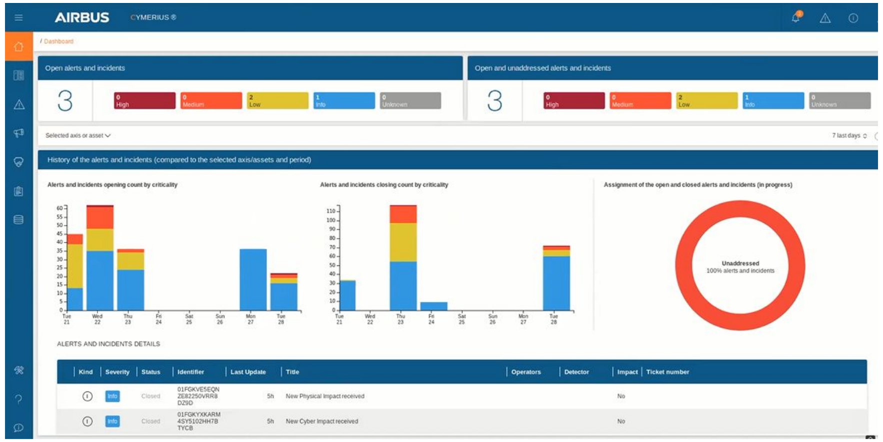
Cyber Threat Monitoring System

CTMS interoperates with the following subsystems:



Cyber Threat Monitoring System

AIRBUS



AIRBUS CYMERIUS ®

/ Dashboard

Open alerts and incidents

3 — 0 High, 0 Medium, 2 Low, 1 Info, 0 Unknown

Open and unaddressed alerts and incidents

3 — 0 High, 0 Medium, 2 Low, 1 Info, 0 Unknown

Selected axis or asset

7 last days

History of the alerts and incidents (compared to the selected axis/assets and period)

Alerts and incidents opening count by criticality

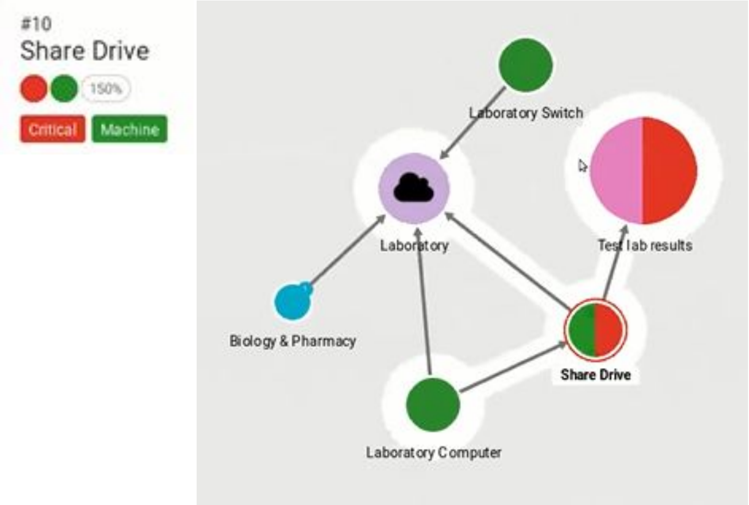
Alerts and incidents closing count by criticality

Assignment of the open and closed alerts and incidents (in progress)

ALERTS AND INCIDENTS DETAILS

Kind	Severity	Status	Identifier	Last Update	Title	Operators	Detector	Impact	Ticket number
ⓘ	Info	Closed	01FGKVE5EQN ZE82250VRR8 DZ9D	5h	New Physical Impact received			No	
ⓘ	Info	Closed	01FGKYXKARM 4SY5102HH7B TYCB	5h	New Cyber Impact received			No	

Alerts and incidents handling system (based on Cymerius) AIRBUS



Based-graph visualization of assets relationships (based on Linkurious)

SAFECARE

Integrated cyber-physical security for health services

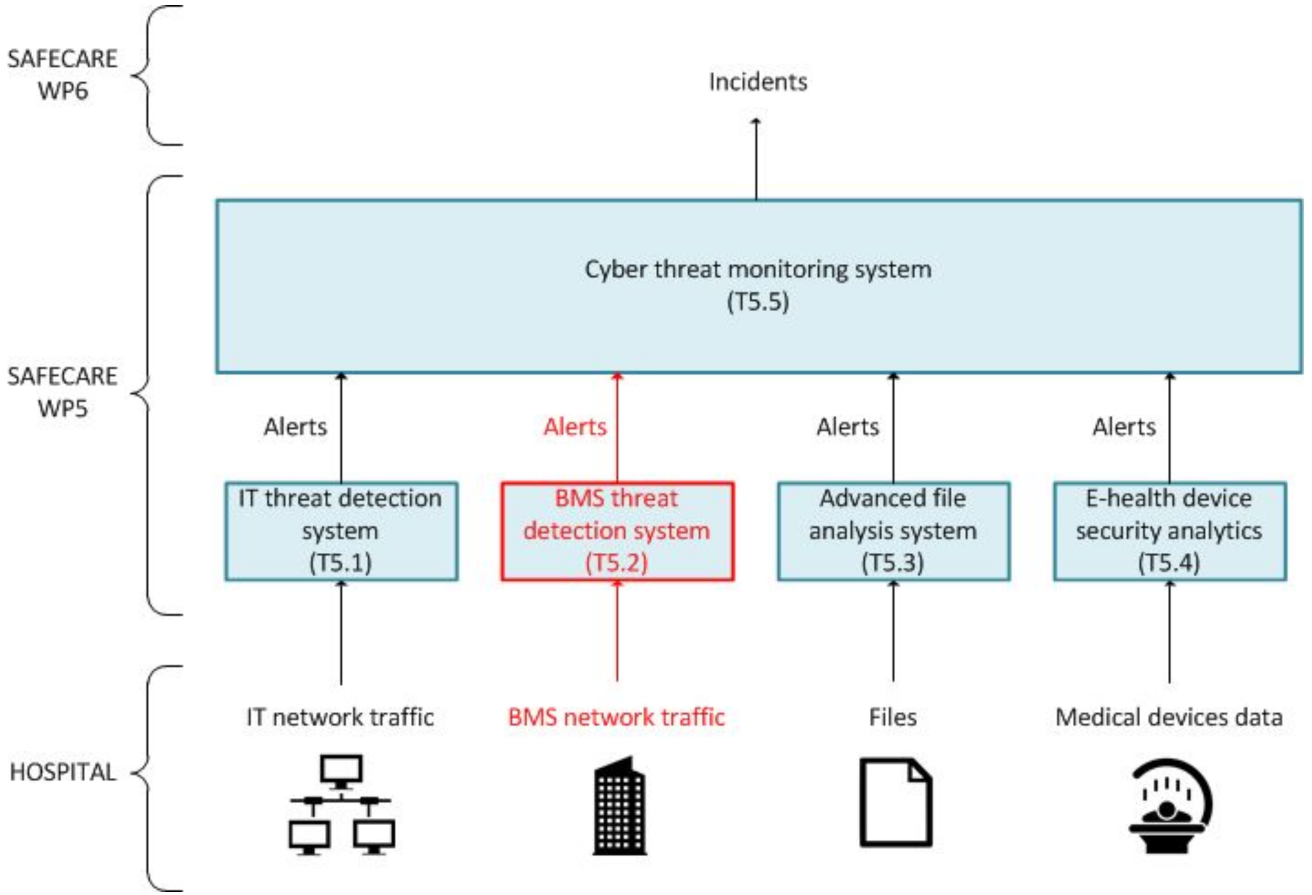
Building Threat Detection System (BTDS)

Building threat detection system – Objectives

- Detect cyber-security events concerning the safety of Building Management Systems in healthcare

- Forward detected events to CTMS

- Forward detected malicious files to AFAS



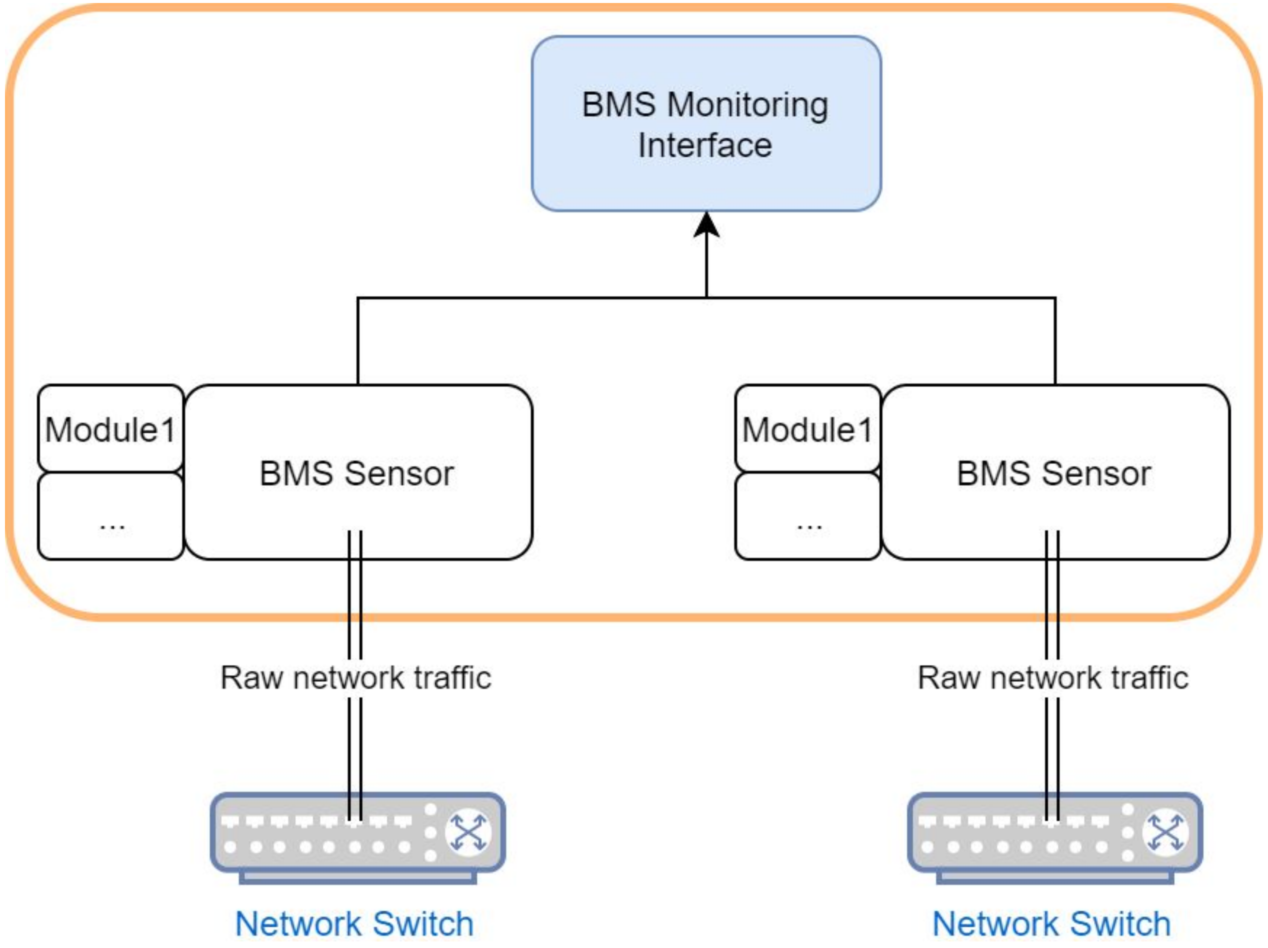
SAFECARE WP6
Incidents
SAFECARE WP5
Cyber threat monitoring system (T5.5)
Alerts
Alerts
Alerts
Alerts
IT threat detection system (T5.1)
BMS threat detection system (T5.2)
Advanced file analysis system (T5.3)
E-health device security analytics (T5.4)
HOSPITAL
IT network traffic
BMS network traffic
Files
Medical devices data

Building threat detection system - Solution

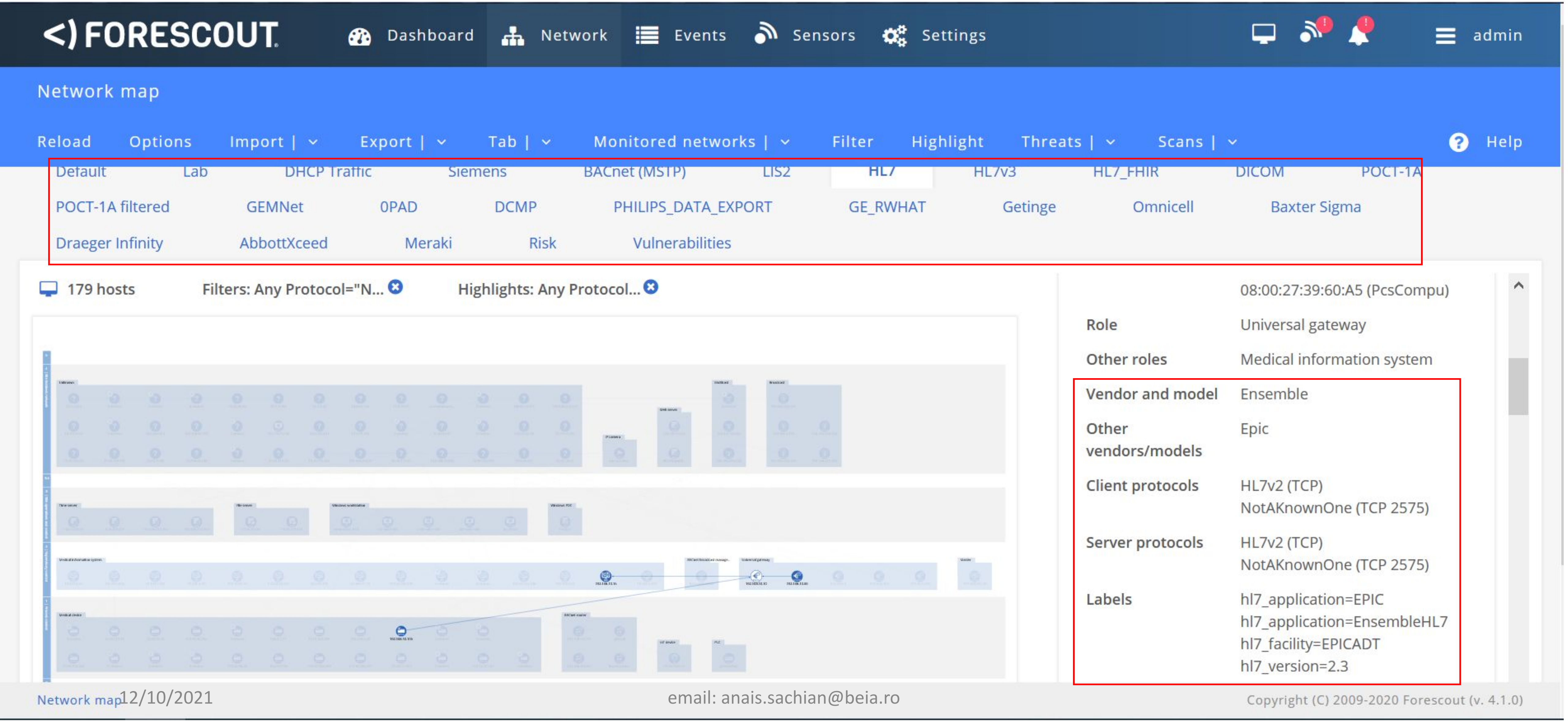
- **Monitoring Interface**
  - Asset Inventory
  - Vulnerable Devices
  - Security Alerts

- **Detection Modules**
  - Signature-based
  - Anomaly-based
  - Malformed packets
  - Port scan
  - Man-in-the-middle

- **Protocol Support**
  - Standard and proprietary protocols used in BMS and healthcare
  - E.g.: BACnet, LonWorks, Tridium, DICOM, HL7, ...



Demo – Asset Inventory



Default Lab DHCP Traffic Siemens BACnet (MSTP) LIS2 HL7 HL7v3 HL7_FHIR DICOM POCT-1A
POCT-1A filtered GEMNet 0PAD DCMP PHILIPS_DATA_EXPORT GE_RWHAT Getinge Omnicell Baxter Sigma
Draeger Infinity AbbottXceed Meraki Risk Vulnerabilities

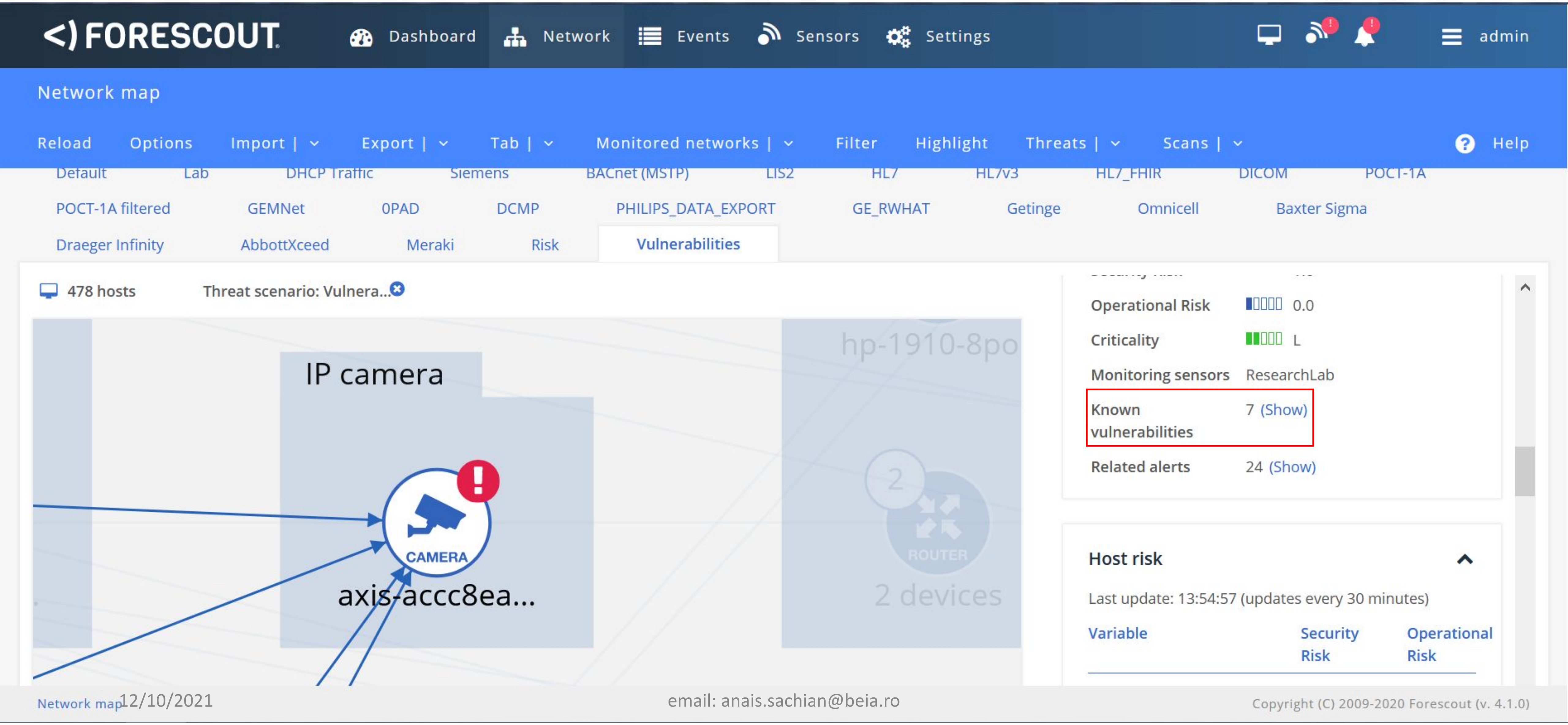
179 hosts Filters: Any Protocol="N... Highlights: Any Protocol...

	08:00:27:39:60:A5 (PcsCompu)
Role	Universal gateway
Other roles	Medical information system
Vendor and model	Ensemble
Other vendors/models	Epic
Client protocols	HL7v2 (TCP) NotAKnownOne (TCP 2575)
Server protocols	HL7v2 (TCP) NotAKnownOne (TCP 2575)

Labels	hl7_application=EPIC
	hl7_application=EnsembleHL7
	hl7_facility=EPICADT
	hl7_version=2.3

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

Demo – Vulnerable Devices



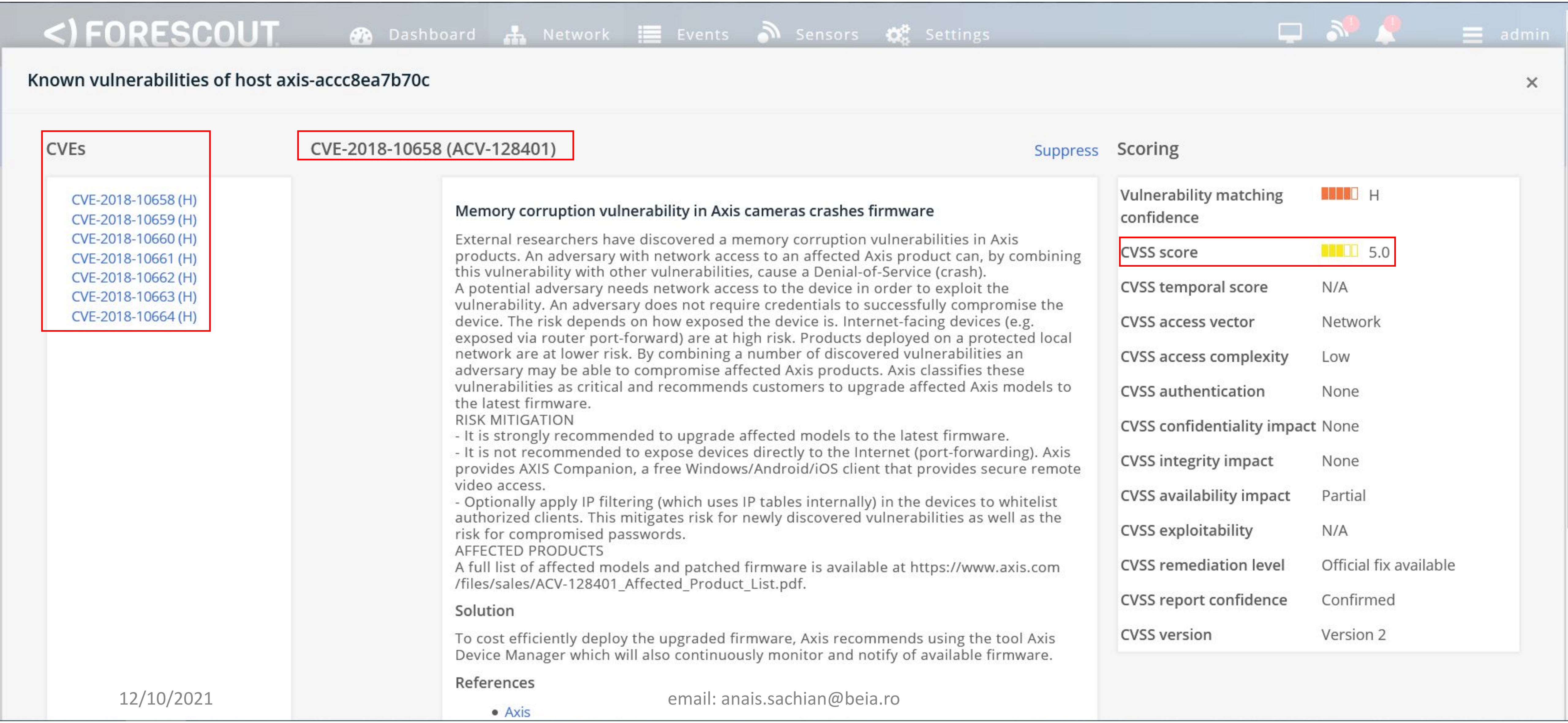
Operational Risk	0.0
Criticality	L
Monitoring sensors	ResearchLab
Known vulnerabilities	7 (Show)
Related alerts	24 (Show)

Host risk

Last update: 13:54:57 (updates every 30 minutes)

Variable	Security Risk	Operational Risk

Demo – Vulnerable Devices



Known vulnerabilities of host axis-accc8ea7b70c

CVEs

- CVE-2018-10658 (H)
- CVE-2018-10659 (H)
- CVE-2018-10660 (H)
- CVE-2018-10661 (H)
- CVE-2018-10662 (H)
- CVE-2018-10663 (H)
- CVE-2018-10664 (H)

CVE-2018-10658 (ACV-128401)

Suppress

Memory corruption vulnerability in Axis cameras crashes firmware

External researchers have discovered a memory corruption vulnerabilities in Axis products. An adversary with network access to an affected Axis product can, by combining this vulnerability with other vulnerabilities, cause a Denial-of-Service (crash).
A potential adversary needs network access to the device in order to exploit the vulnerability. An adversary does not require credentials to successfully compromise the device. The risk depends on how exposed the device is. Internet-facing devices (e.g. exposed via router port-forward) are at high risk. Products deployed on a protected local network are at lower risk. By combining a number of discovered vulnerabilities an adversary may be able to compromise affected Axis products. Axis classifies these vulnerabilities as critical and recommends customers to upgrade affected Axis models to the latest firmware.
RISK MITIGATION
- It is strongly recommended to upgrade affected models to the latest firmware.
- It is not recommended to expose devices directly to the Internet (port-forwarding). Axis provides AXIS Companion, a free Windows/Android/iOS client that provides secure remote video access.
- Optionally apply IP filtering (which uses IP tables internally) in the devices to whitelist authorized clients. This mitigates risk for newly discovered vulnerabilities as well as the risk for compromised passwords.
AFFECTED PRODUCTS
A full list of affected models and patched firmware is available at https://www.axis.com/files/sales/ACV-128401_Affected_Product_List.pdf.

Solution

To cost efficiently deploy the upgraded firmware, Axis recommends using the tool Axis Device Manager which will also continuously monitor and notify of available firmware.

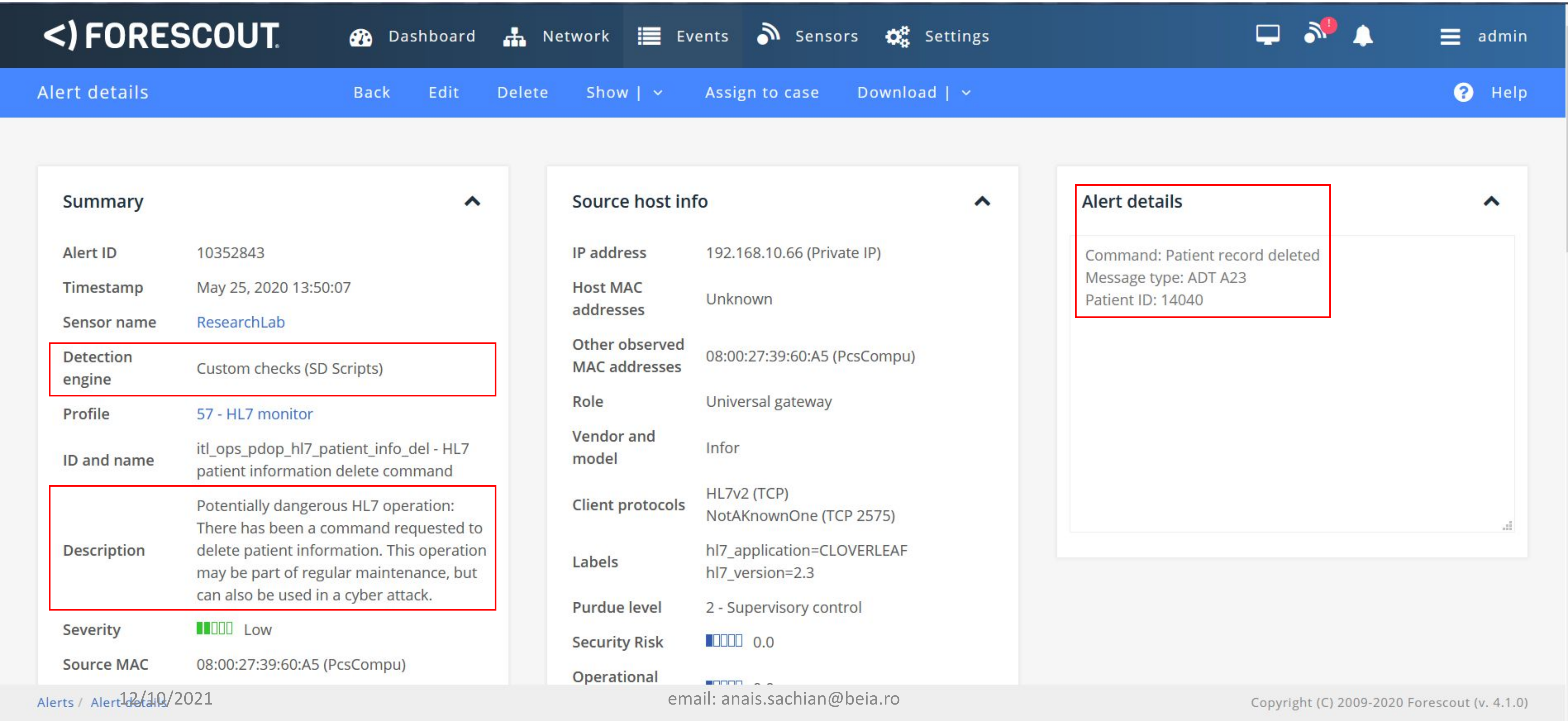
References

- Axis

Scoring

Vulnerability matching confidence	H
CVSS score	5.0
CVSS temporal score	N/A
CVSS access vector	Network
CVSS access complexity	Low
CVSS authentication	None
CVSS confidentiality impact	None
CVSS integrity impact	None
CVSS availability impact	Partial
CVSS exploitability	N/A
CVSS remediation level	Official fix available
CVSS report confidence	Confirmed
CVSS version	Version 2

Demo – Anomaly-based Detection



Summary

Alert ID	10352843
Timestamp	May 25, 2020 13:50:07
Sensor name	ResearchLab
Detection engine	Custom checks (SD Scripts)
Profile	57 - HL7 monitor
ID and name	itl_ops_pdop_hl7_patient_info_del - HL7 patient information delete command
Description	Potentially dangerous HL7 operation: There has been a command requested to delete patient information. This operation may be part of regular maintenance, but can also be used in a cyber attack.
Severity	▮▯▯▯ Low
Source MAC	08:00:27:39:60:A5 (PcsCompu)

Source host info

IP address	192.168.10.66 (Private IP)
Host MAC addresses	Unknown
Other observed MAC addresses	08:00:27:39:60:A5 (PcsCompu)
Role	Universal gateway
Vendor and model	Infor
Client protocols	HL7v2 (TCP) NotAKnownOne (TCP 2575)

Labels	hl7_application=CLOVERLEAF
	hl7_version=2.3

Purdue level	2 - Supervisory control
Security Risk	▮▯▯▯ 0.0
Operational	

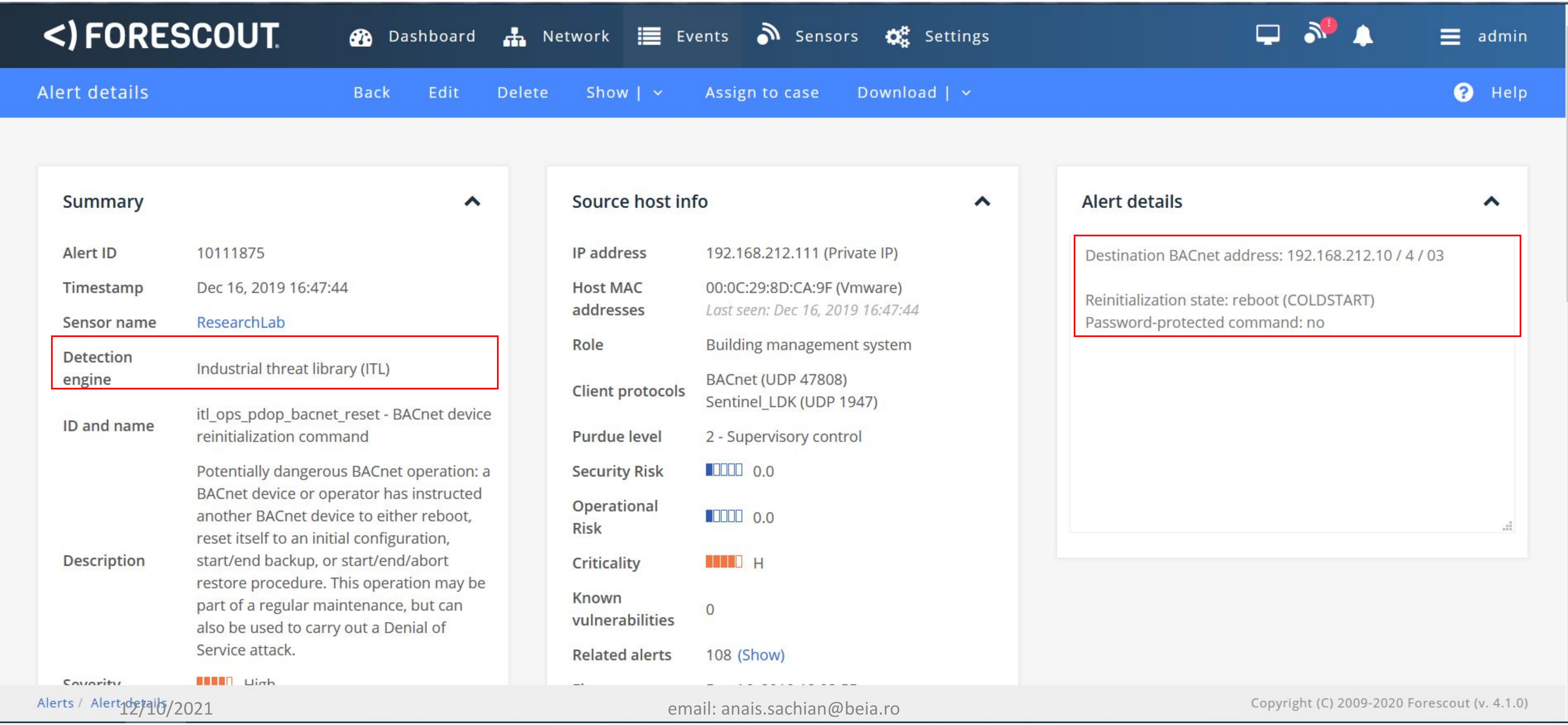
Alert details

Command: Patient record deleted
Message type: ADT A23
Patient ID: 14040

Alerts / Alert details

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

Demo – Signature-based Detection



Summary

Alert ID	10111875
Timestamp	Dec 16, 2019 16:47:44
Sensor name	ResearchLab
Detection engine	Industrial threat library (ITL)
ID and name	itl_ops_pdop_bacnet_reset - BACnet device reinitialization command
Description	Potentially dangerous BACnet operation: a BACnet device or operator has instructed another BACnet device to either reboot, reset itself to an initial configuration, start/end backup, or start/end/abort restore procedure. This operation may be part of a regular maintenance, but can also be used to carry out a Denial of Service attack.
Severity	■■■■□ High

Source host info

IP address	192.168.212.111 (Private IP)
Host MAC addresses	00:0C:29:8D:CA:9F (Vmware) *Last seen: Dec 16, 2019 16:47:44*
Role	Building management system
Client protocols	BACnet (UDP 47808) Sentinel_LDK (UDP 1947)
Purdue level	2 - Supervisory control
Security Risk	■□□□□ 0.0
Operational Risk	■□□□□ 0.0
Criticality	■■■■□ H
Known vulnerabilities	0
Related alerts	108 (Show)

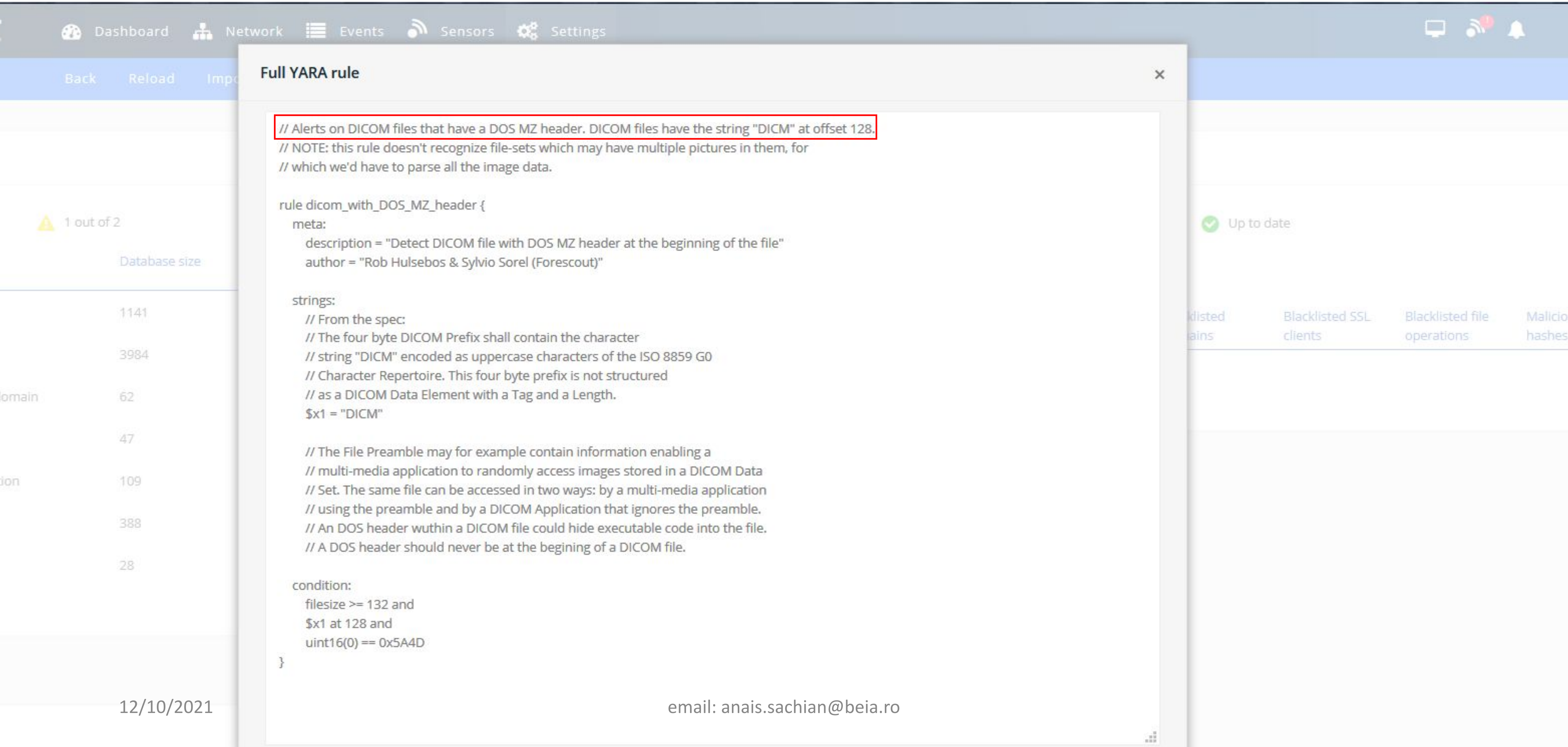
Alert details

Destination BACnet address: 192.168.212.10 / 4 / 03

Reinitialization state: reboot (COLDSTART)
Password-protected command: no

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

Demo – Signature-based Detection



Full YARA rule ×

```
// Alerts on DICOM files that have a DOS MZ header. DICOM files have the string "DICM" at offset 128.
// NOTE: this rule doesn't recognize file-sets which may have multiple pictures in them, for
// which we'd have to parse all the image data.

rule dicom_with_DOS_MZ_header {
  meta:
    description = "Detect DICOM file with DOS MZ header at the beginning of the file"
    author = "Rob Hulsebos & Sylvio Sorel (Forescout)"

  strings:
    // From the spec:
    // The four byte DICOM Prefix shall contain the character
    // string "DICM" encoded as uppercase characters of the ISO 8859 G0
    // Character Repertoire. This four byte prefix is not structured
    // as a DICOM Data Element with a Tag and a Length.
    $x1 = "DICM"

    // The File Preamble may for example contain information enabling a
    // multi-media application to randomly access images stored in a DICOM Data
    // Set. The same file can be accessed in two ways: by a multi-media application
    // using the preamble and by a DICOM Application that ignores the preamble.
    // An DOS header wuthin a DICOM file could hide executable code into the file.
    // A DOS header should never be at the begining of a DICOM file.

  condition:
    filesize >= 132 and
    $x1 at 128 and
    uint16(0) == 0x5A4D
}
```

SAFECARE

Integrated cyber-physical security for health services

IT Threat Detection System (ITDS)

IT Threat Detection System

ITDS is a **keystone** system of the SAFECARE ecosystem

- Part of the threat detection systems of the SAFECARE global solutions and belongs to the cyber security tools set

ITDS concentrates the **functions** to detect security events.

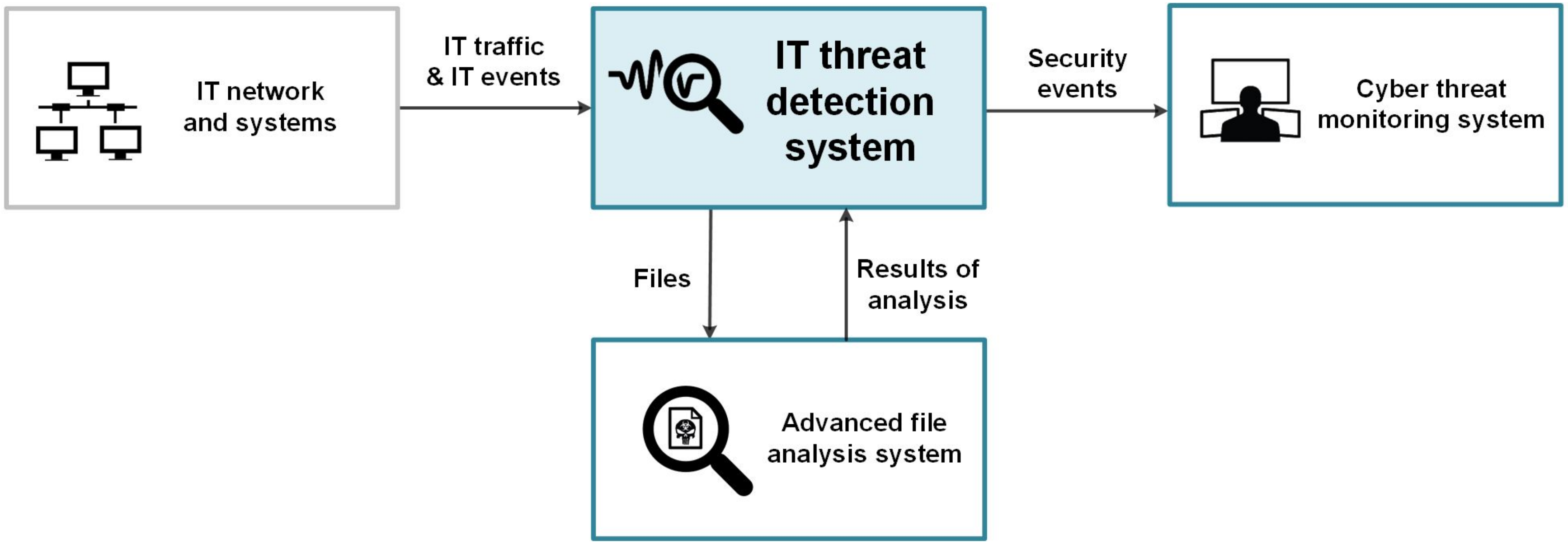
- offers both common non-supervised IDS/IPS methods and innovative supervised ML methods

SOC's analysts:

- correlate information
- understand threats
- improve response capacities and shorten time response
- mitigate the consequences of attacks, especially in case of large data and APT.

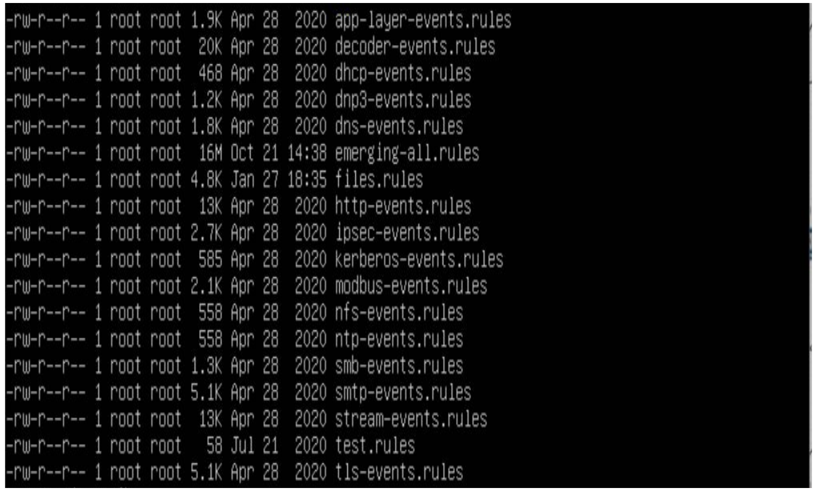
IT Threat Detection System

ITDS interoperates with the following subsystems:

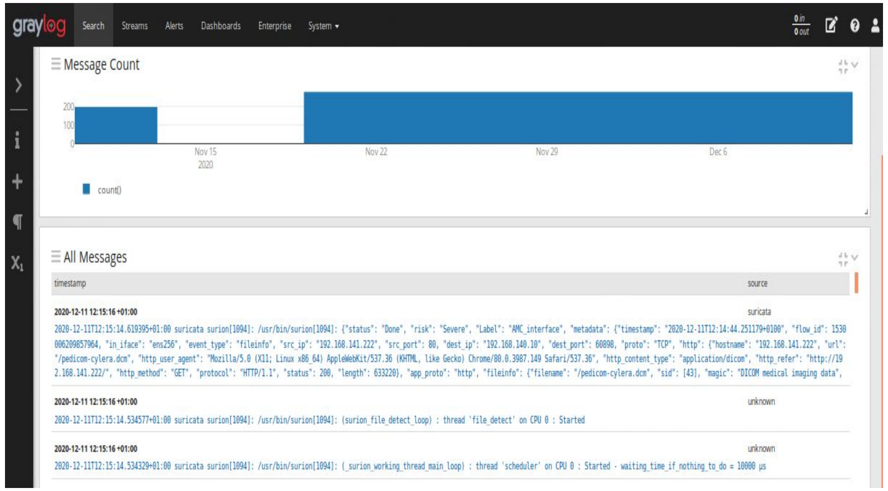


SAFECARE
Integrated cyber-physical security for health services

IT Threat Detection System



```
-rw-r--r-- 1 root root 1.9K Apr 28  2020 app-layer-events.rules
-rw-r--r-- 1 root root  20K Apr 28  2020 decoder-events.rules
-rw-r--r-- 1 root root  468 Apr 28  2020 dhcp-events.rules
-rw-r--r-- 1 root root 1.2K Apr 28  2020 dnp3-events.rules
-rw-r--r-- 1 root root 1.8K Apr 28  2020 dns-events.rules
-rw-r--r-- 1 root root  16M Oct 21 14:38 emerging-all.rules
-rw-r--r-- 1 root root 4.8K Jan 27 18:35 files.rules
-rw-r--r-- 1 root root  13K Apr 28  2020 http-events.rules
-rw-r--r-- 1 root root 2.7K Apr 28  2020 ipsec-events.rules
-rw-r--r-- 1 root root  585 Apr 28  2020 kerberos-events.rules
-rw-r--r-- 1 root root 2.1K Apr 28  2020 modbus-events.rules
-rw-r--r-- 1 root root  558 Apr 28  2020 nfs-events.rules
-rw-r--r-- 1 root root  558 Apr 28  2020 ntp-events.rules
-rw-r--r-- 1 root root 1.3K Apr 28  2020 smb-events.rules
-rw-r--r-- 1 root root 5.1K Apr 28  2020 smtp-events.rules
-rw-r--r-- 1 root root  13K Apr 28  2020 stream-events.rules
-rw-r--r-- 1 root root   58 Jul 21  2020 test.rules
-rw-r--r-- 1 root root 5.1K Apr 28  2020 tls-events.rules
```

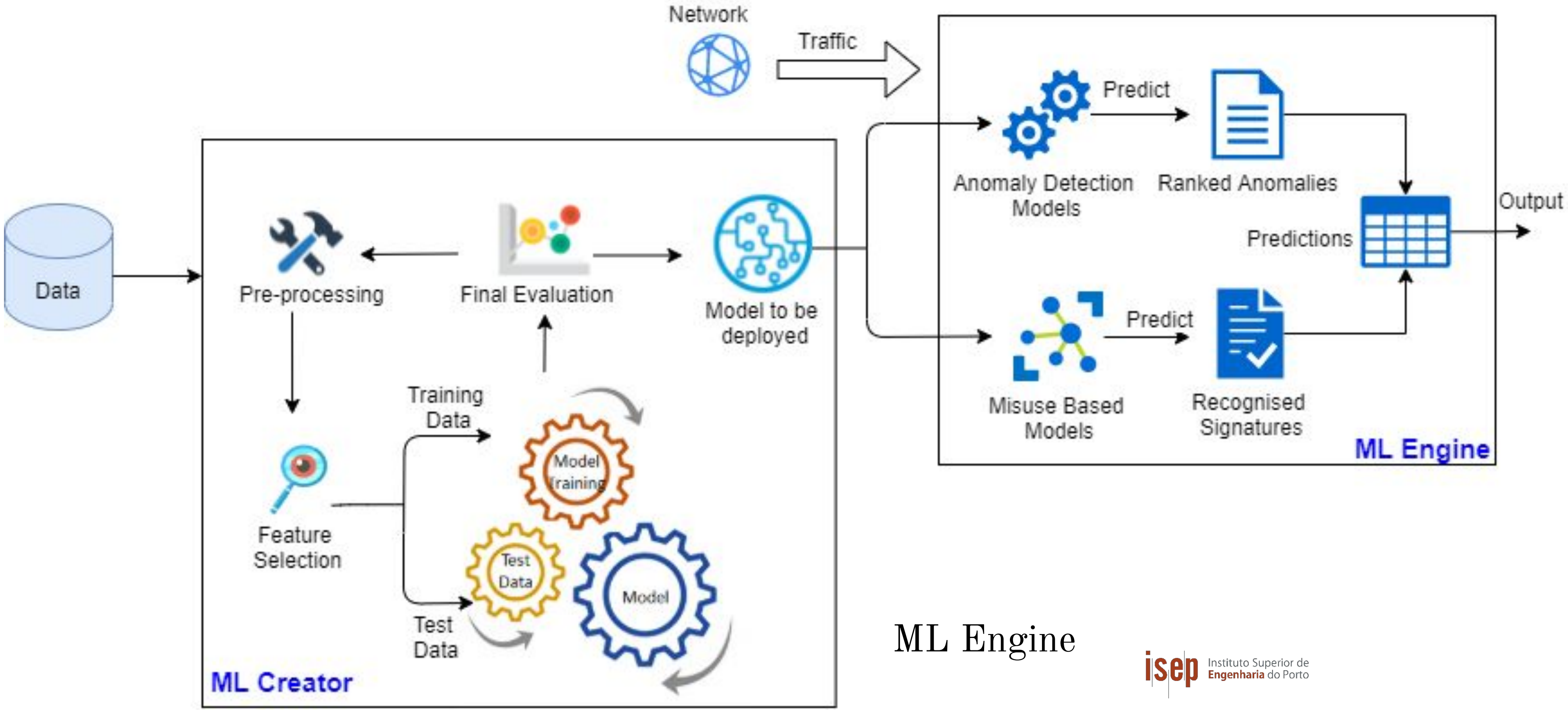


```
2020-12-11 12:15:16 +01:00                                                                 suricata
2020-12-11T12:15:14.619395+01:00 suricata surion[1094]: /usr/bin/surion[1094]: {"status": "Done", "risk": "Severe", "Label": "AMC_interface", "metadata": {"timestamp": "2020-12-11T12:14:44.251179+0100", "flow_id": 1530006209857964, "in_iface": "ens256", "event_type": "fileinfo", "src_ip": "192.168.141.222", "src_port": 80, "dest_ip": "192.168.140.10", "dest_port": 60898, "proto": "TCP", "http": {"hostname": "192.168.141.222", "url": "/pedicom-cylera.dcm", "http_user_agent": "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.149 Safari/537.36", "http_content_type": "application/dicom", "http_refer": "http://192.168.141.222/", "http_method": "GET", "protocol": "HTTP/1.1", "status": 200, "length": 633220}, "app_proto": "http", "fileinfo": {"filename": "/pedicom-cylera.dcm", "sid": [43], "magic": "DICOM medical imaging data",

2020-12-11 12:15:16 +01:00                                                                 unknown
2020-12-11T12:15:14.534577+01:00 suricata surion[1094]: /usr/bin/surion[1094]: (surion_file_detect_loop) : thread 'file_detect' on CPU 0 : Started

2020-12-11 12:15:16 +01:00                                                                 unknown
2020-12-11T12:15:14.534329+01:00 suricata surion[1094]: /usr/bin/surion[1094]: (_surion_working_thread_main_loop) : thread 'scheduler' on CPU 0 : Started - waiting_time_if_nothing_to_do = 10000 µs
```

Network threat detection engine (based on Suricata)

Correlation engine (based on Graylog)

IT Threat Detection System

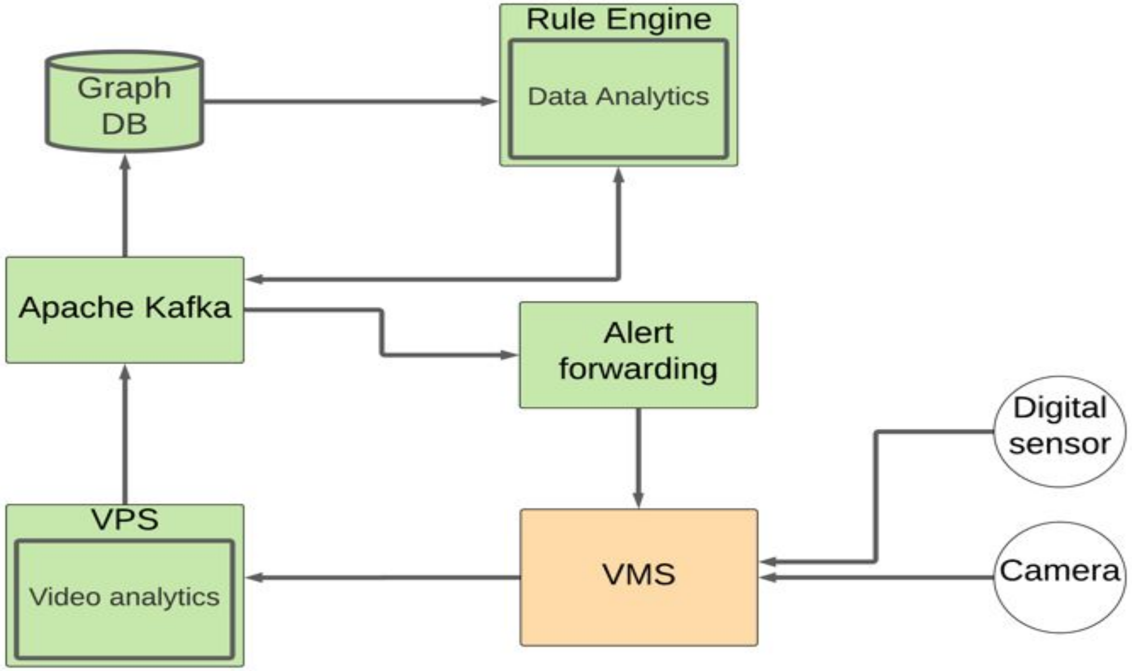


ML Engine

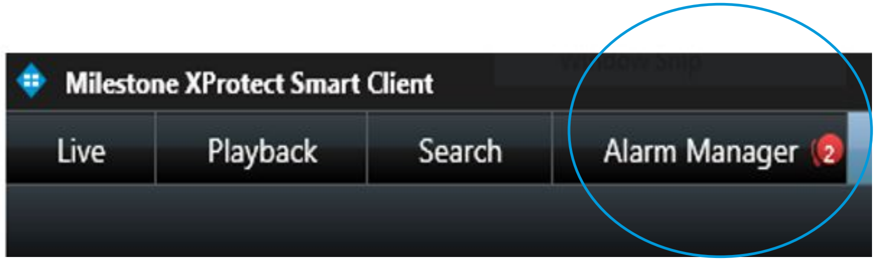
isep Instituto Superior de Engenharia do Porto

Suspicious Behaviour Detection System (SBDS) and Intrusion and Fire Detection System (IFDS)

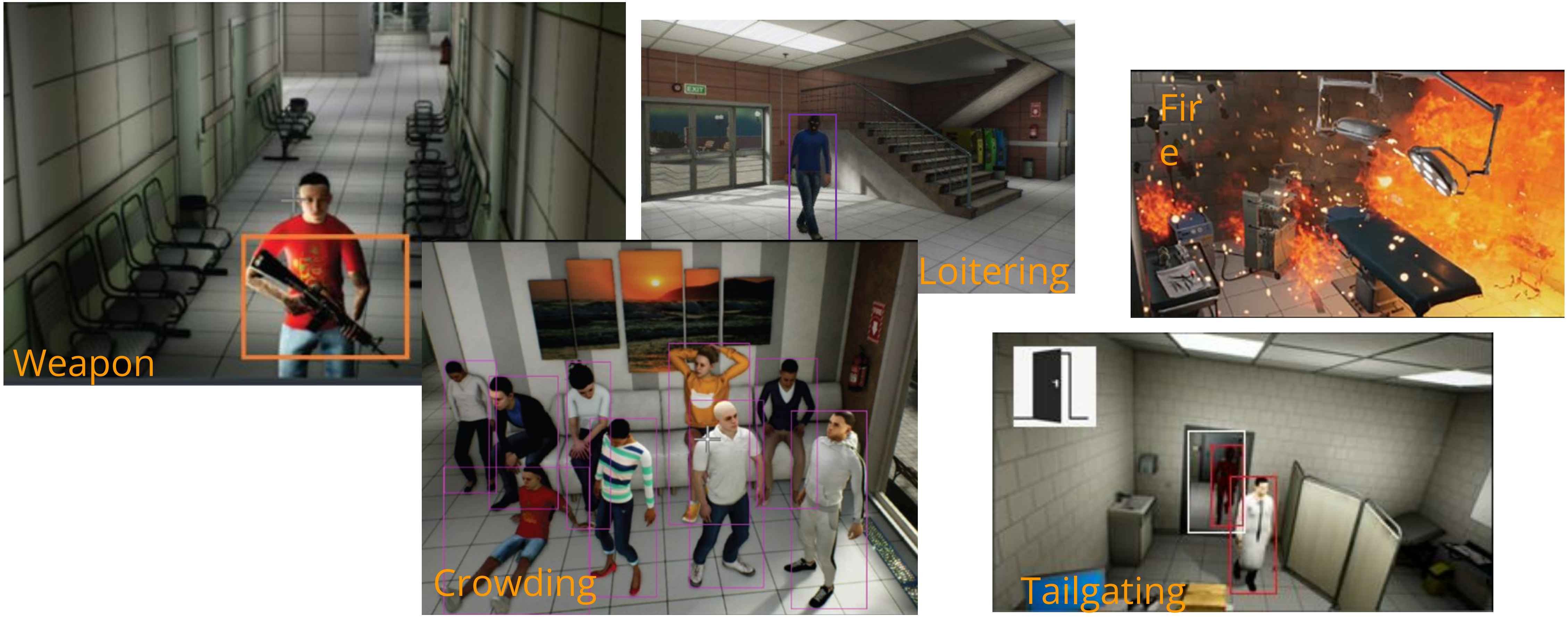
Architecture diagram for SBDS and IFDS



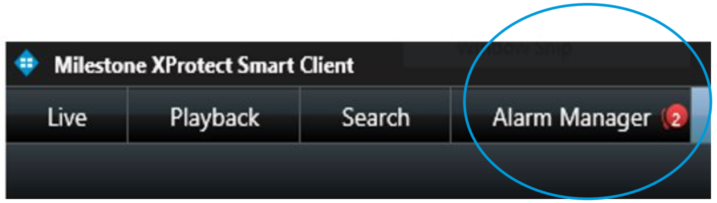
- Video analytics component
- Rule engine
- Video Management System (VMS)



Physical threat examples

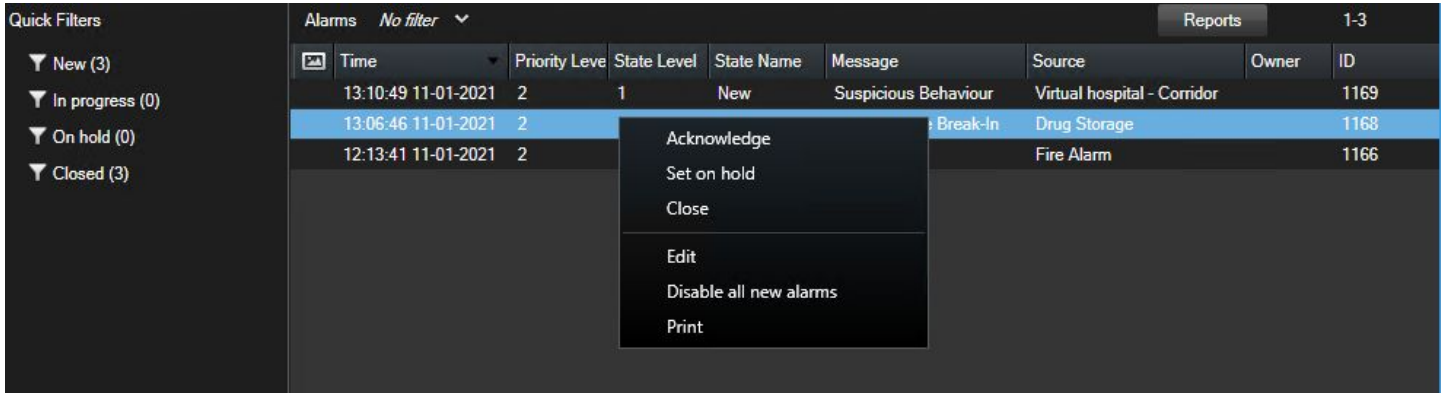


Alarms visualized for users



Milestone XProtect Smart Client

Live | Playback | Search | Alarm Manager 2



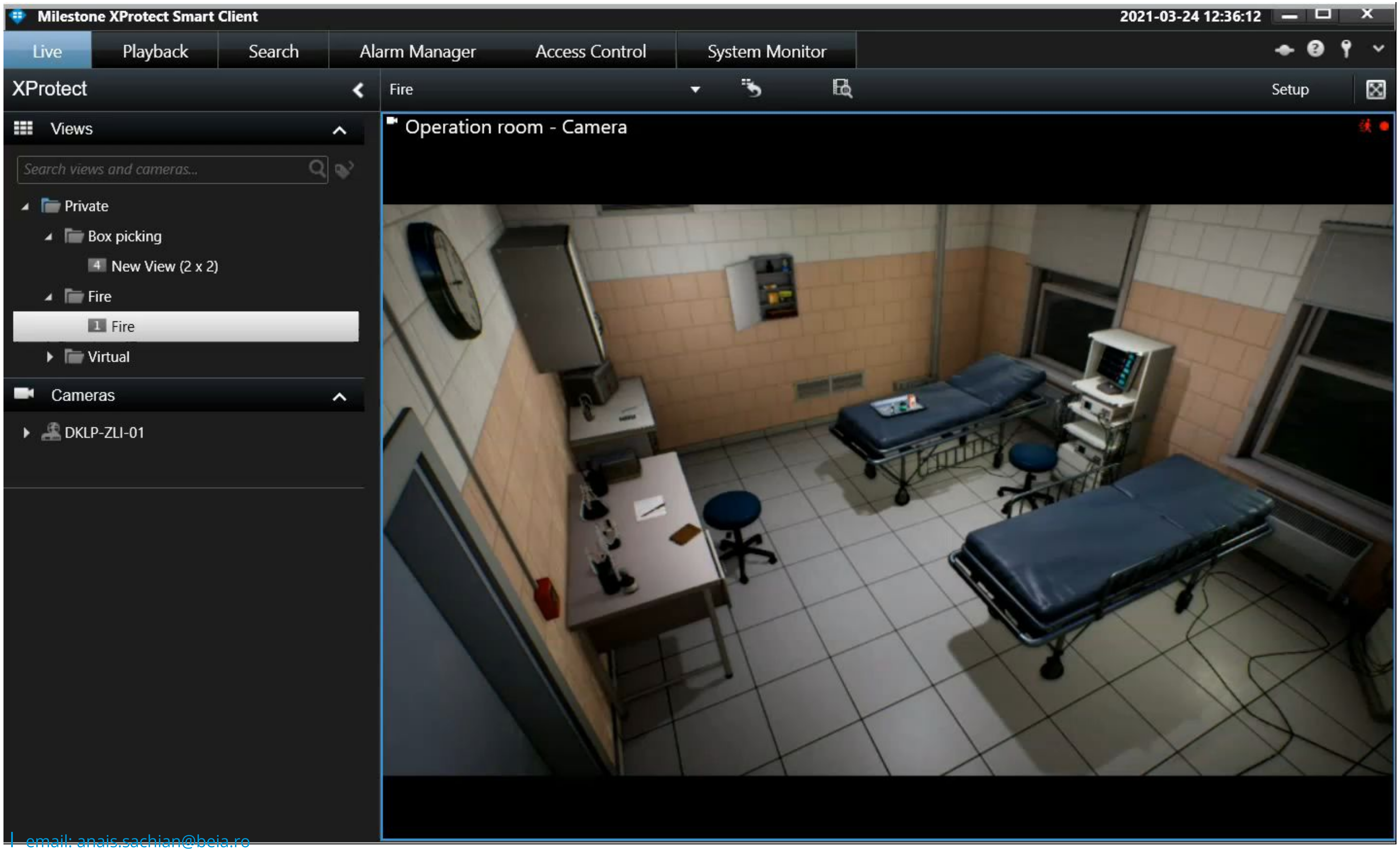
Quick Filters

- New (3)
- In progress (0)
- On hold (0)
- Closed (3)

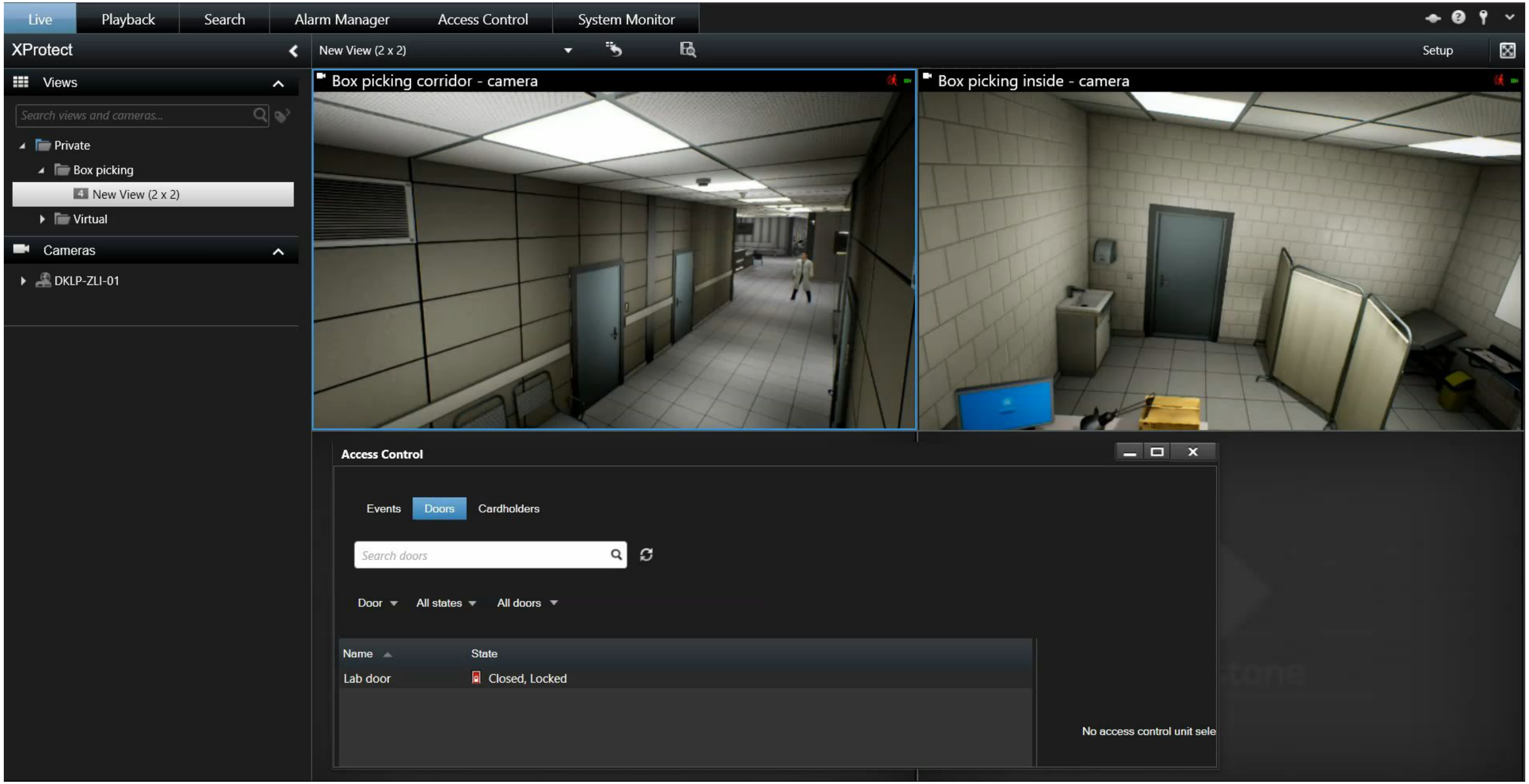
Alarms *No filter* | Reports | 1-3

Time	Priority Leve	State Level	State Name	Message	Source	Owner	ID
13:10:49 11-01-2021	2	1	New	Suspicious Behaviour	Virtual hospital - Corridor		1169
13:06:46 11-01-2021	2			Break-In	Drug Storage		1168
12:13:41 11-01-2021	2				Fire Alarm		1166

Simulation demo - Fire



Simulation demo - Tailgating



Name	State
Lab door	Closed, Locked

No access control unit sele

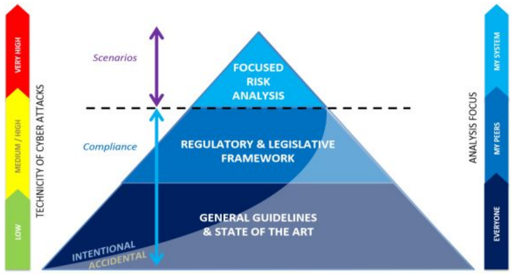
SAFECARE

Integrated cyber-physical security for health services

Data Detection System

email: anais.sachian@beia.ro

Scenarios of threat



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

Scenario 2 - Cyber-physical attack to steal patient data in the hospital;

Scenario 3 - Cyber-physical attack targeting the population, IT systems and medical devices in the hospital, and patient data base;

Scenario 4 - Cyber-physical attack targeting the air-cooling system of the hospital;

Scenario 5 - Shooting, explosive or sabotage in critical places (visible or invisible);

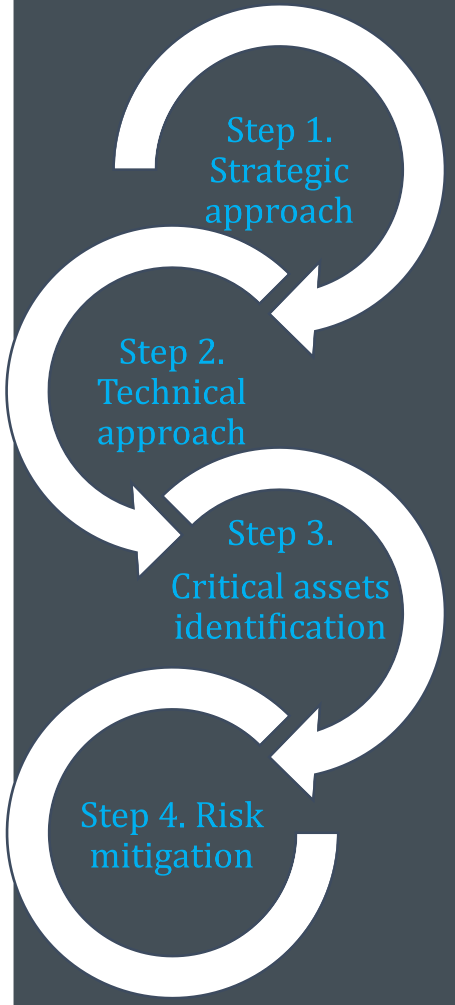
Scenario 6 - Theft at hospital equipment, access to hospital network and IT systems;

Scenario 7 – IoT medical wearable devices (outside / inside);

Scenario 8 - Distributed management over buildings, considering external stakeholders

Scenario 9 - Cyber-physical attack to block national crisis management.

EBIOS methodology has been used for scenario definition and risk assessment…
https://club-ebios.org/site/en/ebios-generic-approach/



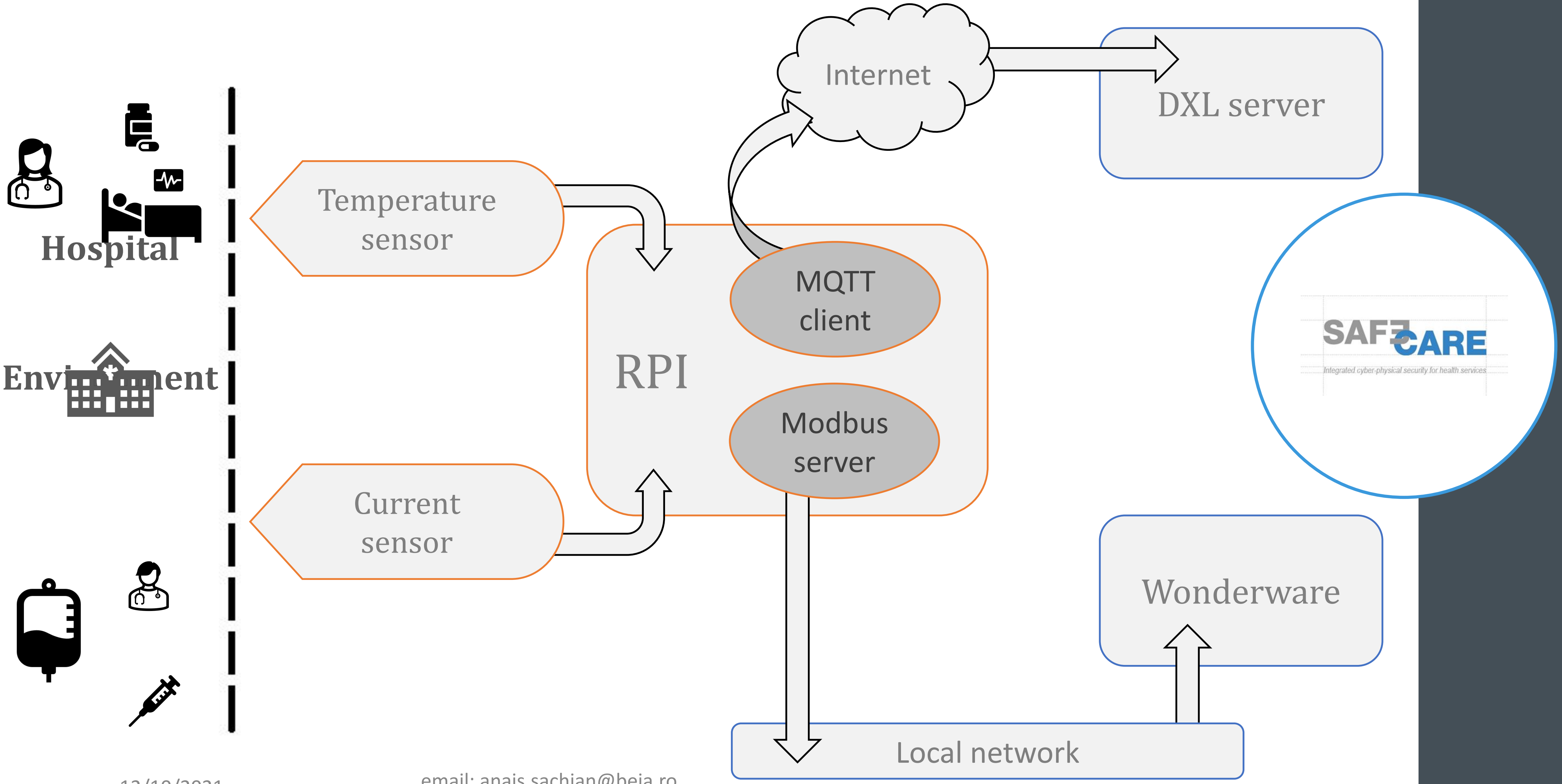
Step 1. Strategic approach

Step 2. Technical approach

Step 3. Critical assets identification

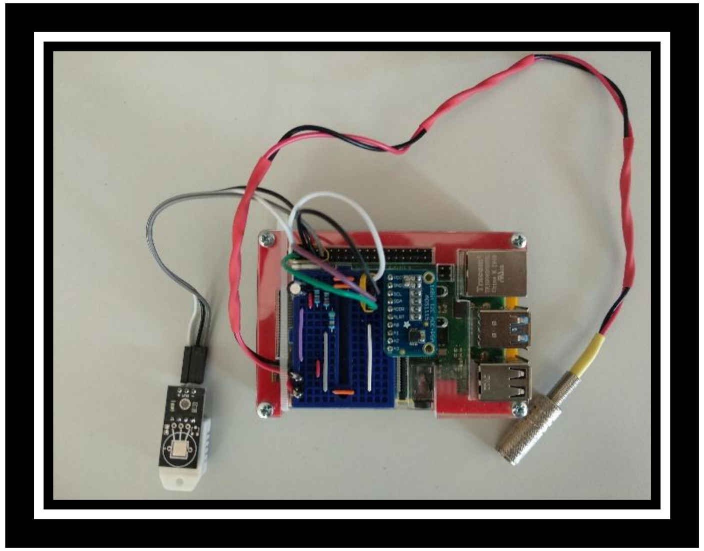
Step 4. Risk mitigation

Overall architecture of Marseille Demo

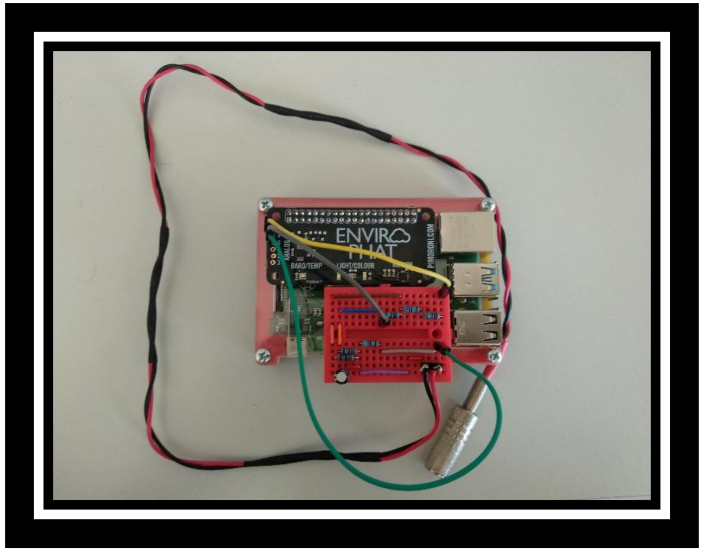


email: anais.sachian@beia.ro

Data acquisition modules



Module 1



Module 2

SAFECARE
Integrated cyber-physical security for health services

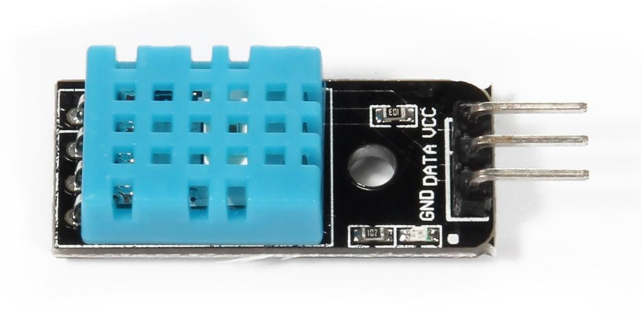
The main goals of each module are:

- Security
- Modularity
- Ease of installation

Temperature Sensor

- The DHT11 has a humidity and a temperature sensor incorporated.
  - Cost effective
  - Easy to replace
- This is a common use device that has a dedicated inbuilt 8-bit microcontroller

SAFECARE
Integrated cyber-physical security for health services

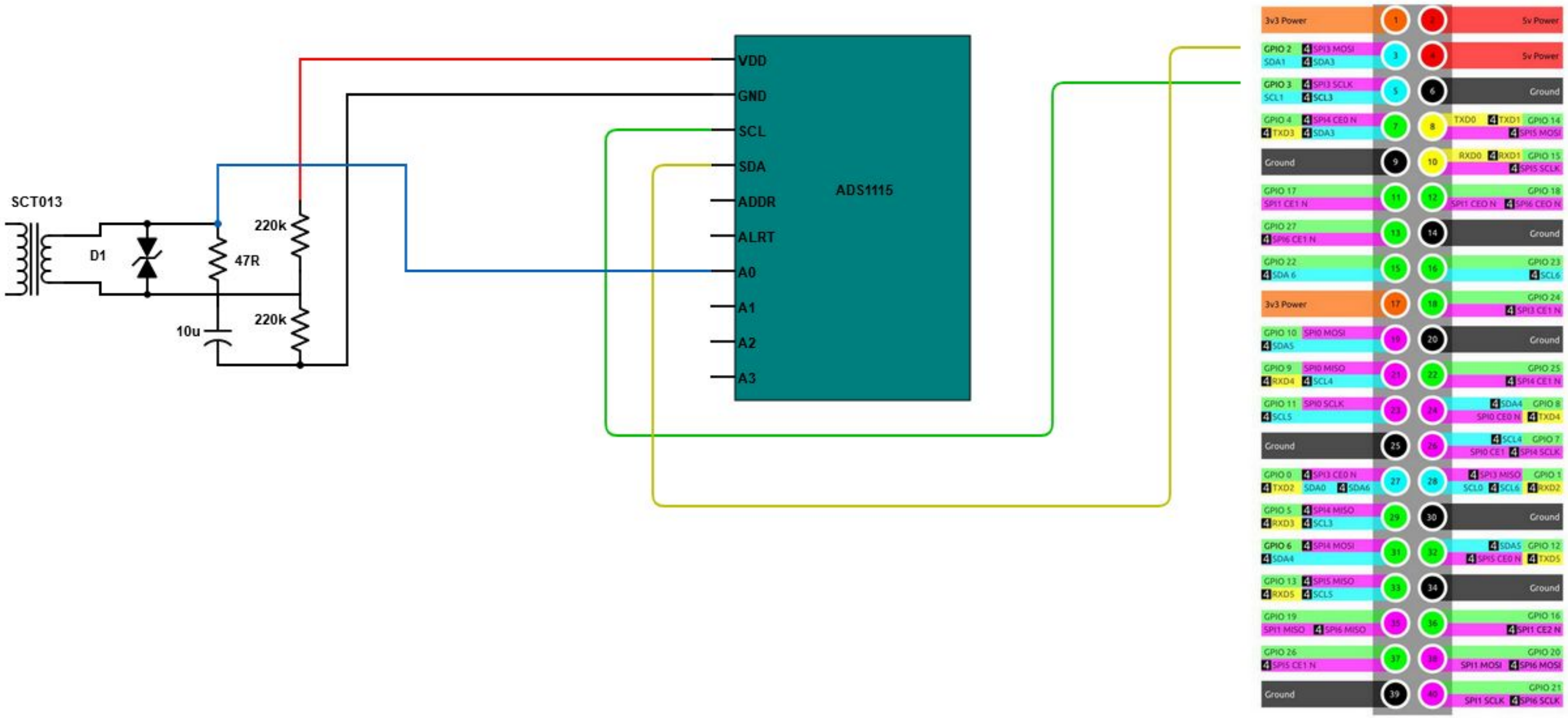


Current Sensor

- The current sensor which was used is SCT013000.
- A noninvasive sensor with a range of detection of 100A.

- Cost effective
- Easy to replace
- Modular

Hardware Design for Marseille Demo


SCT013
D1
47R
220k
220k
10u
ADS1115
VDD
GND
SCL
SDA
ADDR
ALRT
A0
A1
A2
A3
3v3 Power 1 2 5v Power
GPIO 2 SDA1 4 SPI3 MOSI 4 SDA3 3 4 5v Power
GPIO 3 SCL1 4 SPI3 SCLK 4 SCL3 5 6 Ground
GPIO 4 4 TXD3 4 SPI4 CE0 N 4 SDA3 7 8 TXD0 4 TXD1 GPIO 14 4 SPI5 MOSI
Ground 9 10 RXD0 4 RXD1 GPIO 15 4 SPI5 SCLK
GPIO 17 SPI1 CE1 N 11 12 GPIO 18 SPI1 CE0 N 4 SPI6 CE0 N
GPIO 27 4 SPI6 CE1 N 13 14 Ground
GPIO 22 4 SDA 6 15 16 GPIO 23 4 SCL6
3v3 Power 17 18 GPIO 24 4 SPI3 CE1 N
GPIO 10 SPI0 MOSI 4 SDA5 19 20 Ground
GPIO 9 SPI0 MISO 4 RXD4 4 SCL4 21 22 GPIO 25 4 SPI4 CE1 N
GPIO 11 SPI0 SCLK 4 SCL5 23 24 4 SDA4 GPIO 8 SPI0 CE0 N 4 TXD4
Ground 25 26 4 SCL4 GPIO 7 SPI0 CE1 4 SPI4 SCLK
GPIO 0 4 SPI3 CE0 N 4 TXD2 SDA0 4 SDA6 27 28 4 SPI3 MISO GPIO 1 SCL0 4 SCL6 4 RXD2
GPIO 5 4 SPI4 MISO 4 RXD3 4 SCL3 29 30 Ground
GPIO 6 4 SPI4 MOSI 4 SDA4 31 32 4 SDA5 GPIO 12 4 SPI5 CE0 N 4 TXD5
GPIO 13 4 SPI5 MISO 4 RXD5 4 SCL5 33 34 Ground
GPIO 19 SPI1 MISO 4 SPI6 MISO 35 36 GPIO 16 4 SPI1 CE2 N
GPIO 26 4 SPI5 CE1 N 37 38 GPIO 20 SPI1 MOSI 4 SPI6 MOSI
Ground 39 40 GPIO 21 SPI1 SCLK 4 SPI6 SCLK

Tested parameters for the APHM demo scenarios

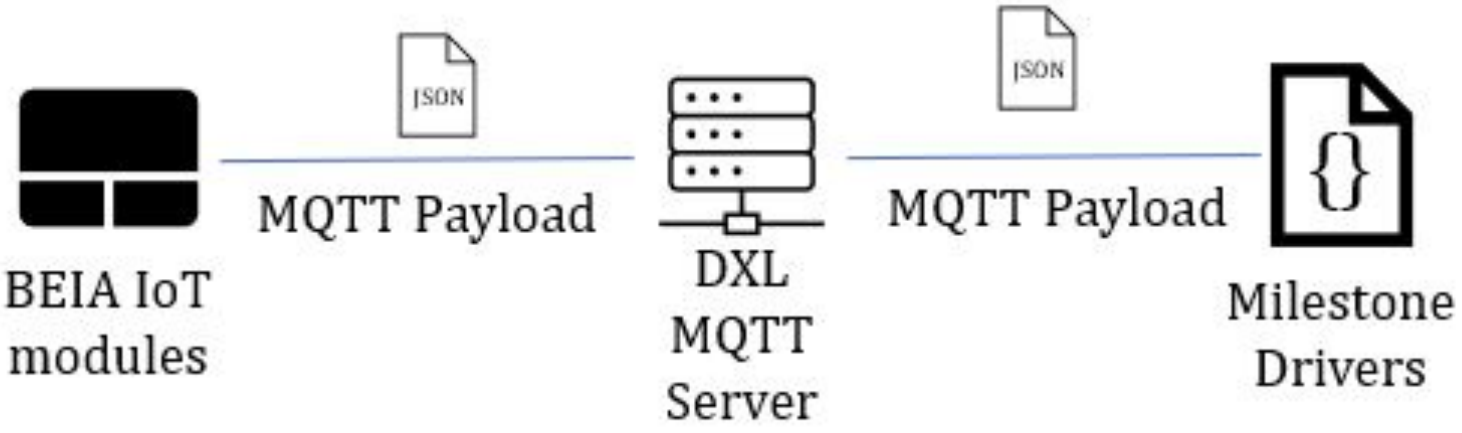
Power Surge

Monitored Device Off

Fire

Sensor Replacement

Secure MQTT Architecture with BTMS

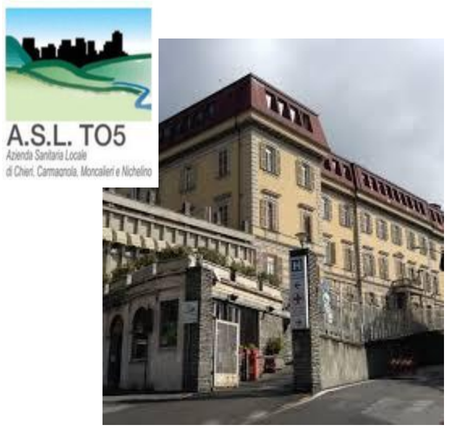


Test platform and pilots

Test Platform

Pilots

Marseille


A.S.L. TO5
Azienda Sanitaria Locale di Chieri, Carmagnola, Moncalieri e Nichelino

Turin

Amsterdam

SAFECARE
Integrated cyber-physical security for health services

Integrated cyber-physical security for health services

Thank you for your attention!

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

@SafecareP

SAFECARE Project

Mari-Anais Sachian

R&D Engineer
Cyber Security Expertise
BEIA Consult International
anais.sachian@beia.ro