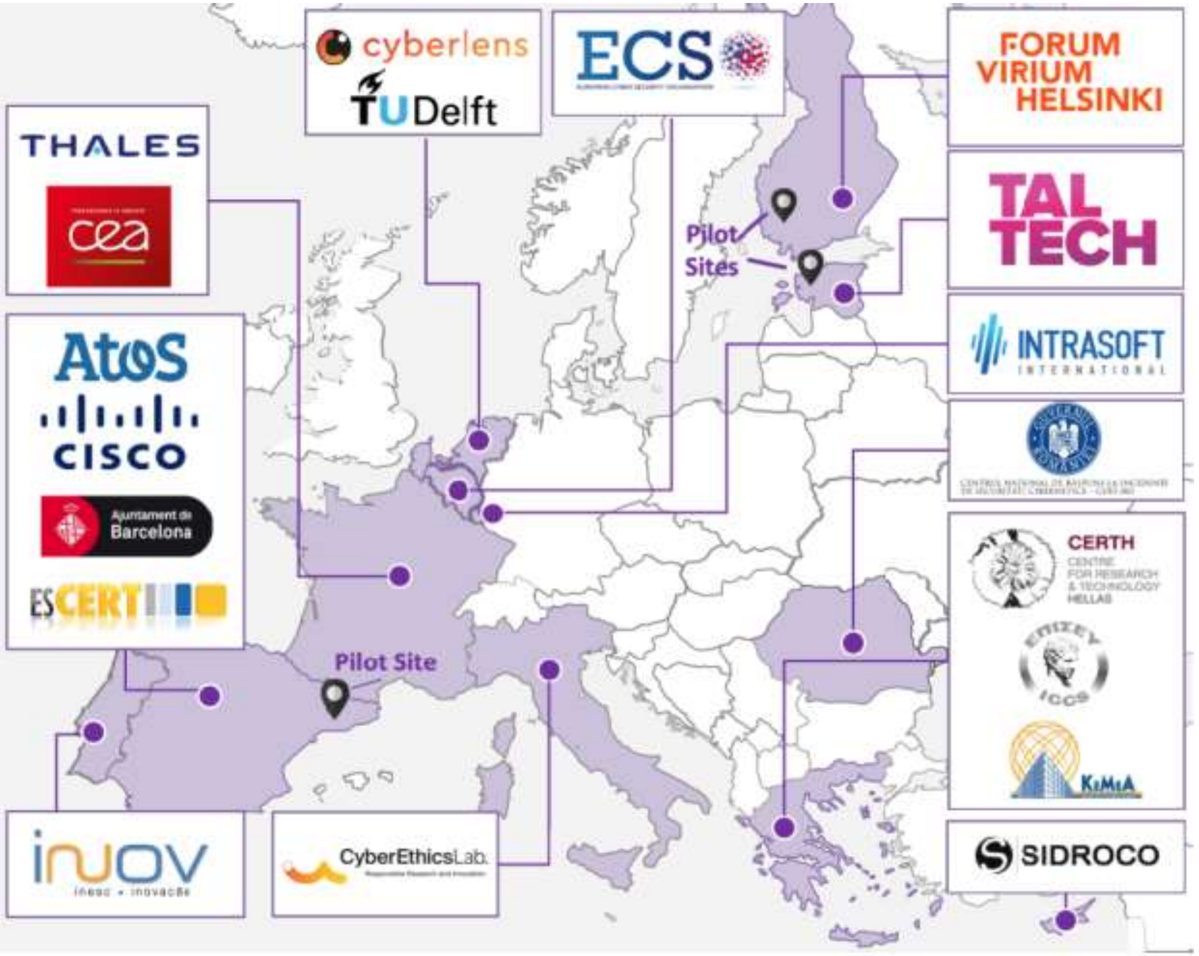
ETSI Security Conference 2022

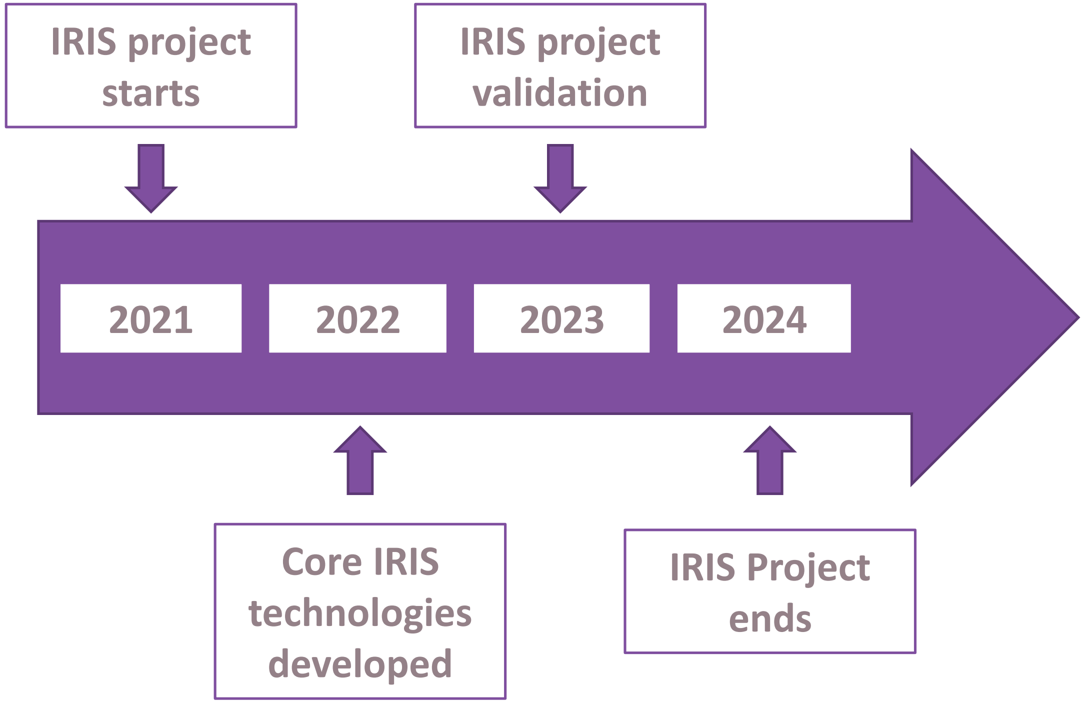
IRIS: a Framework for enhancing Response to Cyberattacks

Rene Serral-Gracia (UPC), Xavier Azemar (Cisco)

05/10/2022

Project at a Glance





IRIS project starts

IRIS project validation

2021

2022

2023

2024

Core IRIS technologies developed

IRIS Project ends

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

IRIS Motivation

Emerging Smartcities

IoT and AI-Enabled platforms

CYBER THREAT INTELLIGENCE
Grasp uncertainty
Know the threat for effective detection
Anticipate cyberthreats
Shift from reactive to proactive

New Cyber Threat Intelligence challenges

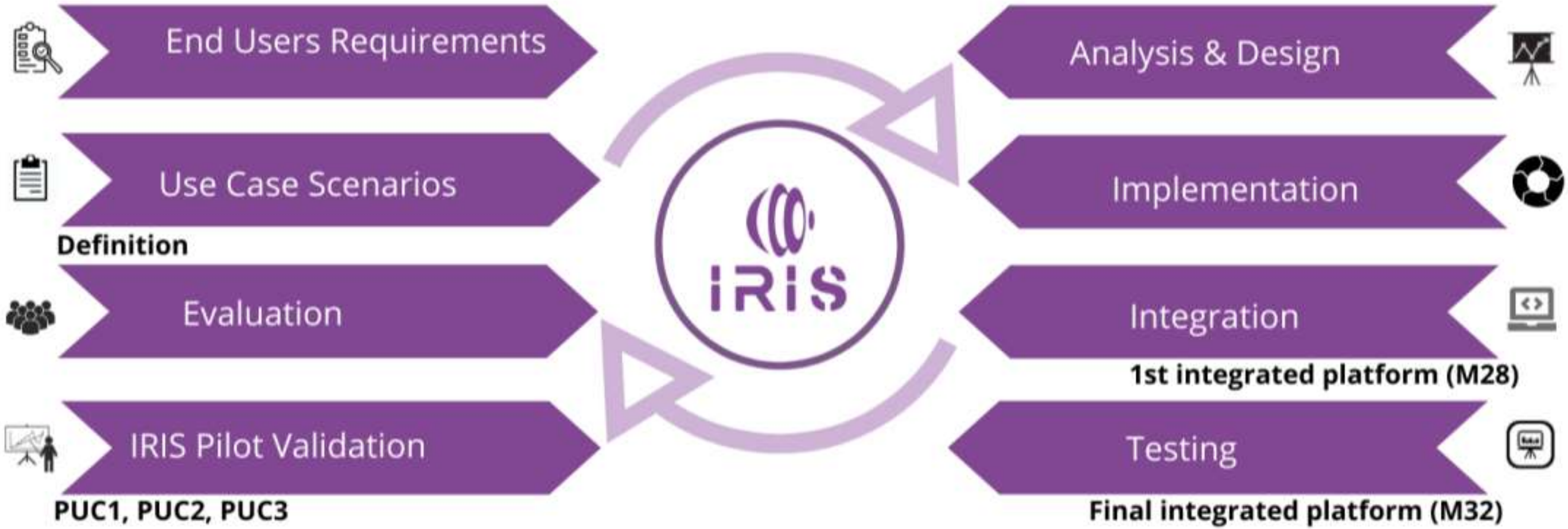
This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors’ view and European Commission is not responsible for any use that may be made of the information it contains.

IRIS Vision

- **Cyber Threat analysis**
  - ✓ Detecting
  - ✓ Sharing
  - ✓ Responding
  - ✓ Recovering
- On an IoT and AI-driven environment
- Considering privacy risks
- **Freely available** to European CERT and CSIRTs in 2024

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors’ view and European Commission is not responsible for any use that may be made of the information it contains.

How we do it?



This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors’ view and European Commission is not responsible for any use that may be made of the information it contains.

IRIS Objectives

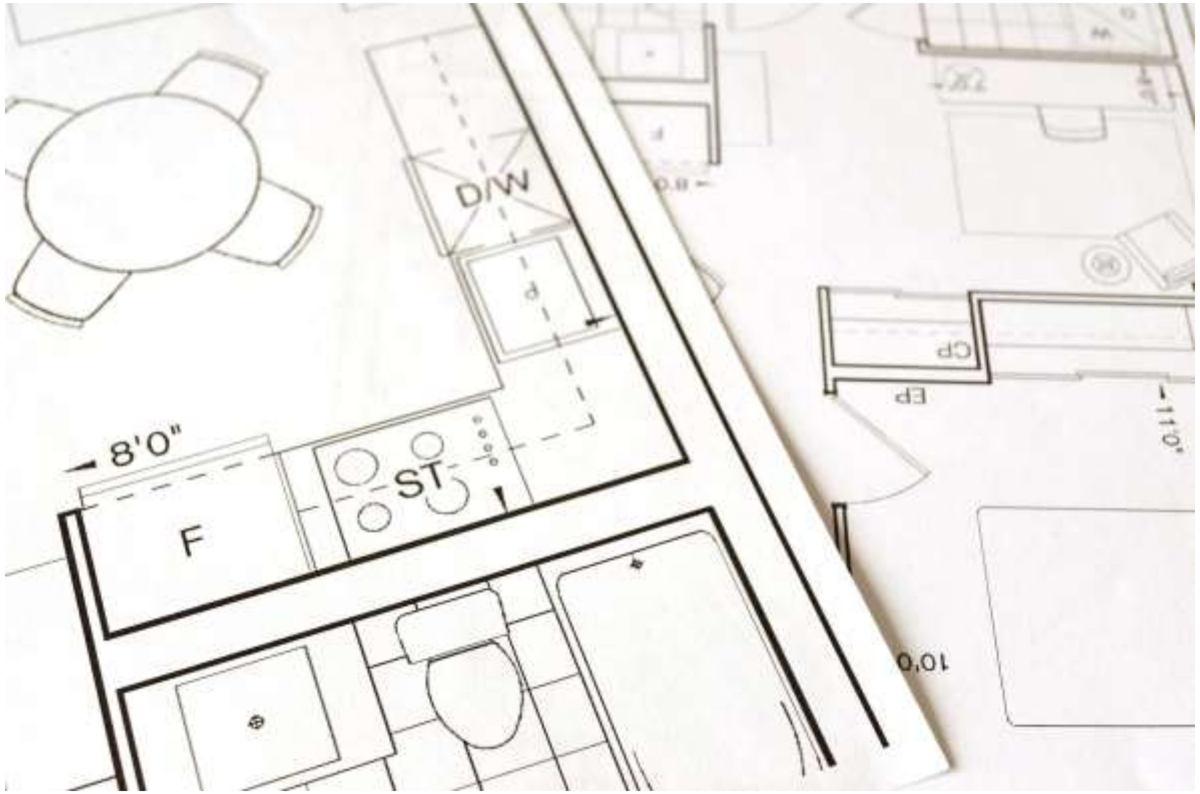
Identify user, technical and business requirements.

Flexible yet powerful architecture to mitigate security threats while driving business with a collaborative platform

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

IRIS Objectives

Design the architecture of an AI threat reporting and incident response system to provide an environment agnostic AI based threat detection and mitigation



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

IRIS Objectives

To **analyze** the relevant **ethics principles** and legal framework on privacy concerns

Guaranteeing its proper use and privacy requirements

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors’ view and European Commission is not responsible for any use that may be made of the information it contains.

IRIS Objectives

To **develop** a **collaborative** platform for ICT stakeholders and European CERTs/CSIRTs for the successful operation of IoT and AI-enabled ICT systems

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

IRIS Objectives

To **demonstrate** and **validate** the integrated IRIS platform across three realistic pilot demonstrators in three smart cities

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors’ view and European Commission is not responsible for any use that may be made of the information it contains.

IRIS Objectives

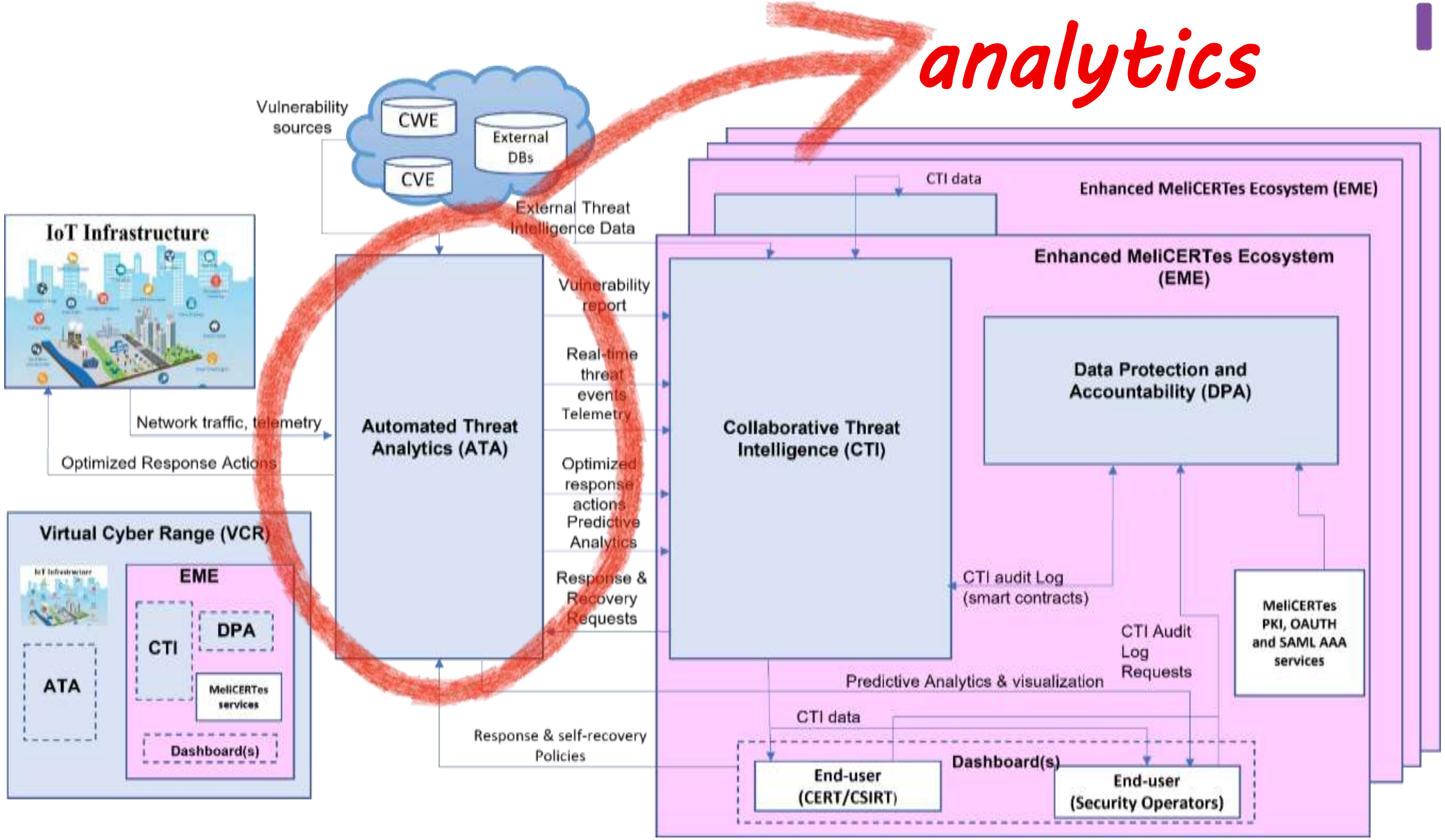
To **ensure** wide communication and scientific dissemination of the results, efficient exploitation and contribution to relevant standardization bodies

Democratize access to cybersecurity and threat intelligence

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

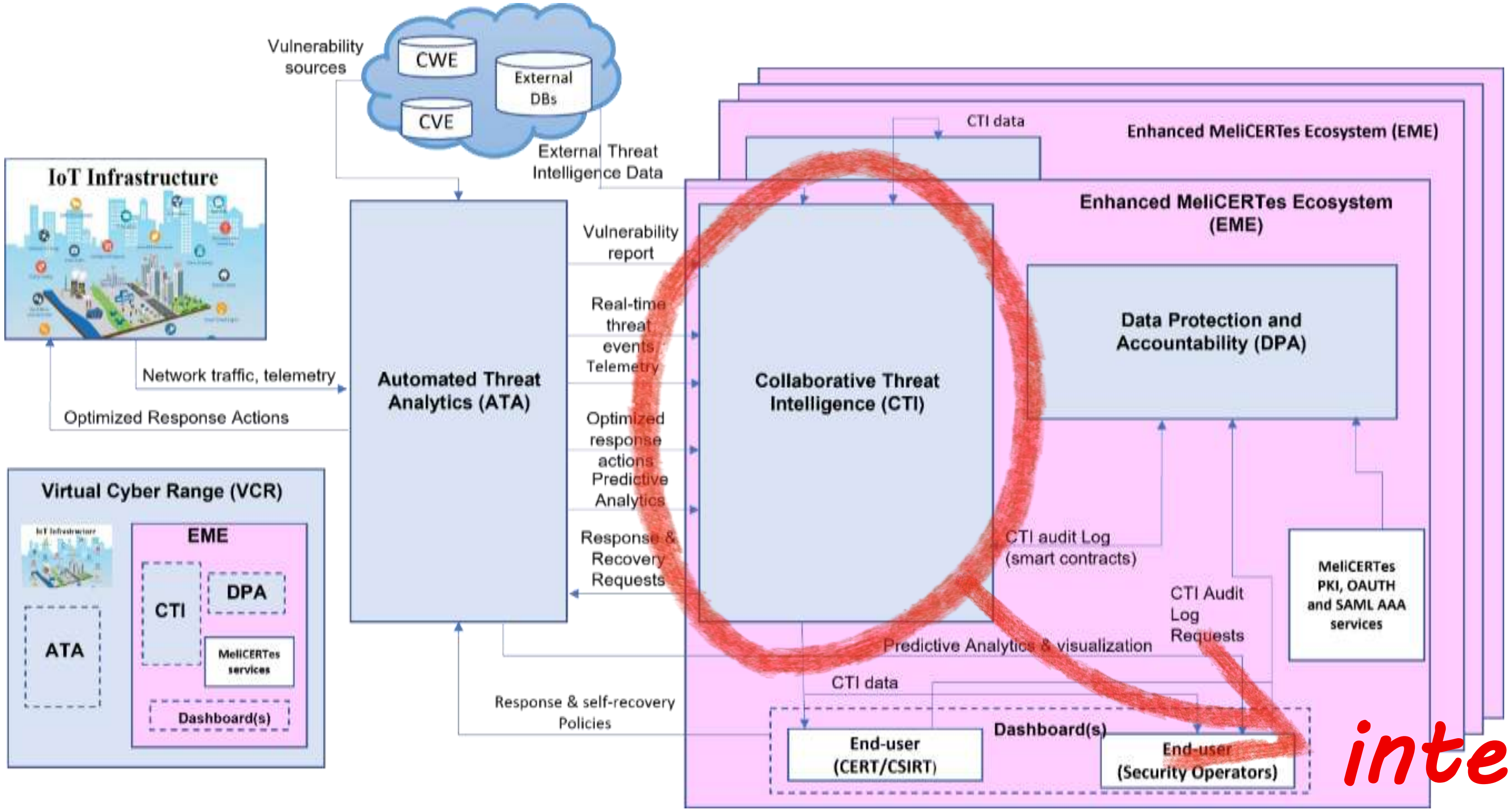
IRIS High Level Architecture

threat analytics


Vulnerability sources
CWE
CVE
External DBs
External Threat Intelligence Data
IoT Infrastructure
Network traffic, telemetry
Optimized Response Actions
Automated Threat Analytics (ATA)
Vulnerability report
Real-time threat events Telemetry
Optimized response actions Predictive Analytics
Response & Recovery Requests
Virtual Cyber Range (VCR)
IoT Infrastructure
EME
CTI
DPA
ATA
MeliCERTes services
Dashboard(s)
Response & self-recovery Policies
CTI data
Enhanced MeliCERTes Ecosystem (EME)
Enhanced MeliCERTes Ecosystem (EME)
Collaborative Threat Intelligence (CTI)
Data Protection and Accountability (DPA)
CTI audit Log (smart contracts)
CTI Audit Log Requests
MeliCERTes PKI, OAUTH and SAML AAA services
Predictive Analytics & visualization
CTI data
Dashboard(s)
End-user (CERT/CSIRT)
End-user (Security Operators)

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors’ view and European Commission is not responsible for any use that may be made of the information it contains.

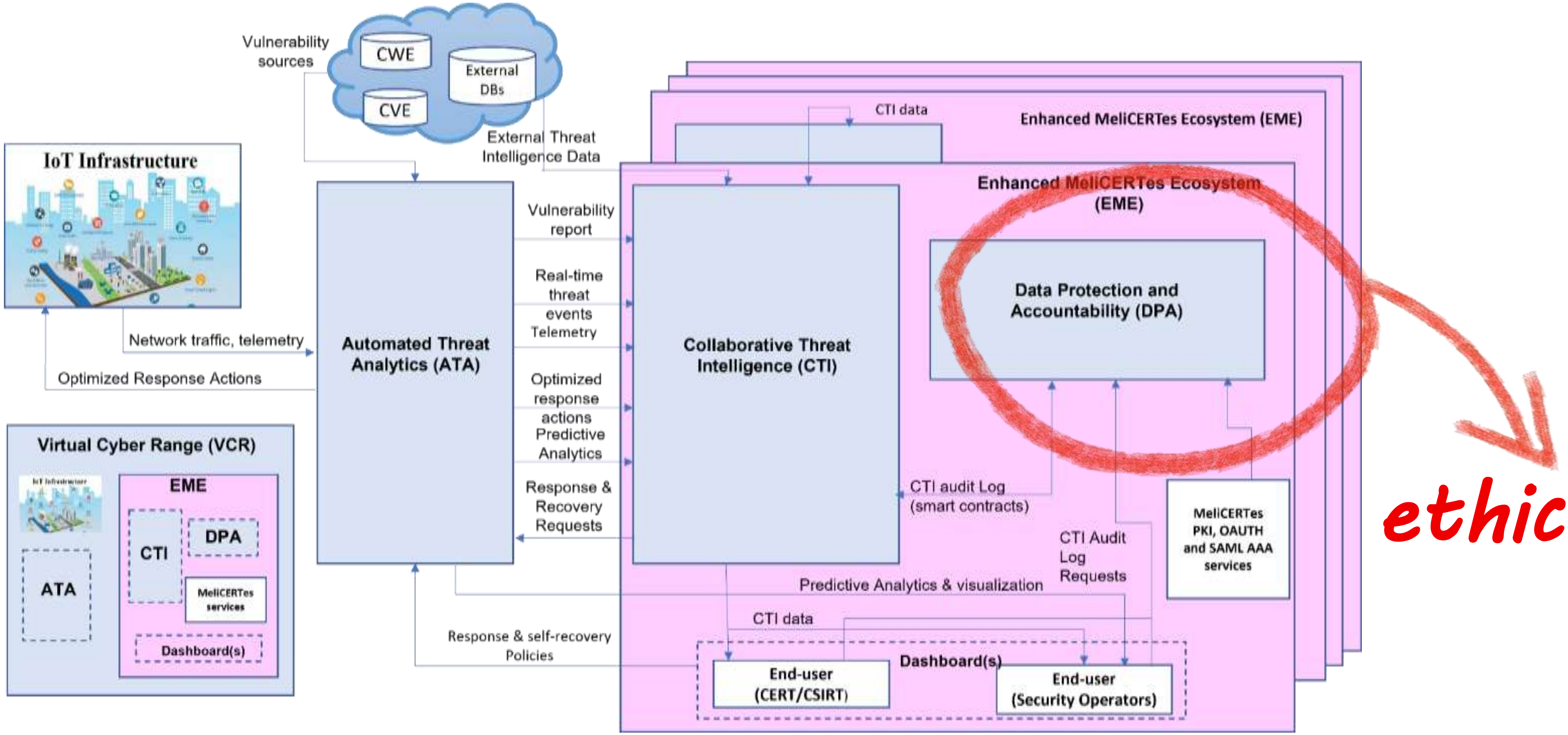
IRIS High Level Architecture


Vulnerability sources
CWE
CVE
External DBs
External Threat Intelligence Data
IoT Infrastructure
Network traffic, telemetry
Optimized Response Actions
Automated Threat Analytics (ATA)
Vulnerability report
Real-time threat events, Telemetry
Optimized response actions
Predictive Analytics
Response & Recovery Requests
CTI data
Enhanced MeliCERTes Ecosystem (EME)
Enhanced MeliCERTes Ecosystem (EME)
Collaborative Threat Intelligence (CTI)
Data Protection and Accountability (DPA)
CTI audit Log (smart contracts)
CTI Audit Log Requests
MeliCERTes PKI, OAUTH and SAML AAA services
Predictive Analytics & visualization
CTI data
Dashboard(s)
End-user (CERT/CSIRT)
End-user (Security Operators)
Response & self-recovery Policies
Virtual Cyber Range (VCR)
IoT Infrastructure
EME
CTI
DPA
ATA
MeliCERTes services
Dashboard(s)

intelligence

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors’ view and European Commission is not responsible for any use that may be made of the information it contains.

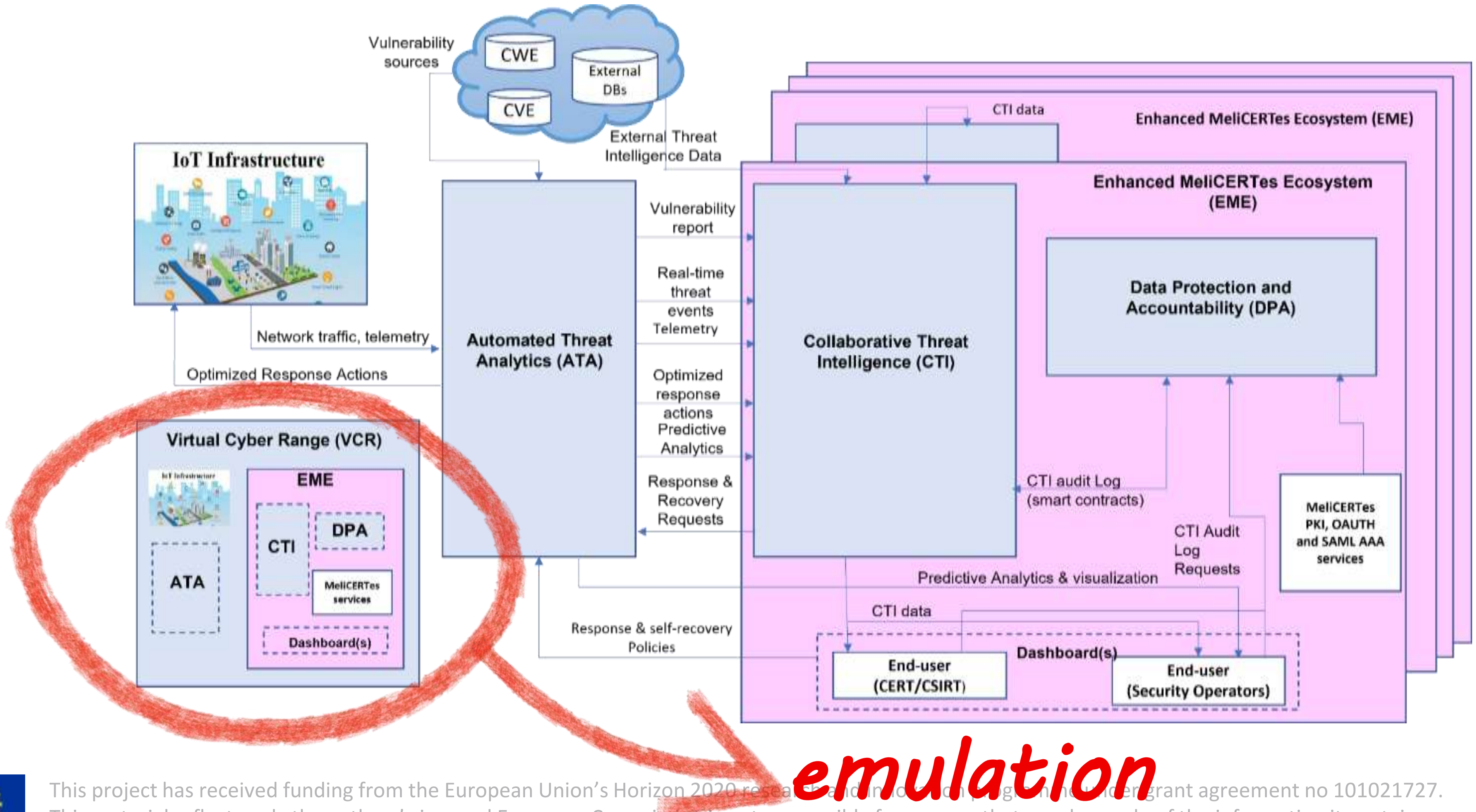
IRIS High Level Architecture


Vulnerability sources
CWE
CVE
External DBs
External Threat Intelligence Data
IoT Infrastructure
Network traffic, telemetry
Optimized Response Actions
Automated Threat Analytics (ATA)
Vulnerability report
Real-time threat events
Telemetry
Optimized response actions
Predictive Analytics
Response & Recovery Requests
Response & self-recovery Policies
Virtual Cyber Range (VCR)
IoT Infrastructure
EME
CTI
DPA
ATA
MeliCERTes services
Dashboard(s)
CTI data
Enhanced MeliCERTes Ecosystem (EME)
Enhanced MeliCERTes Ecosystem (EME)
Collaborative Threat Intelligence (CTI)
Data Protection and Accountability (DPA)
CTI audit Log (smart contracts)
CTI Audit Log Requests
MeliCERTes PKI, OAUTH and SAML AAA services
Predictive Analytics & visualization
CTI data
Dashboard(s)
End-user (CERT/CSIRT)
End-user (Security Operators)

ethics

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

IRIS High Level Architecture

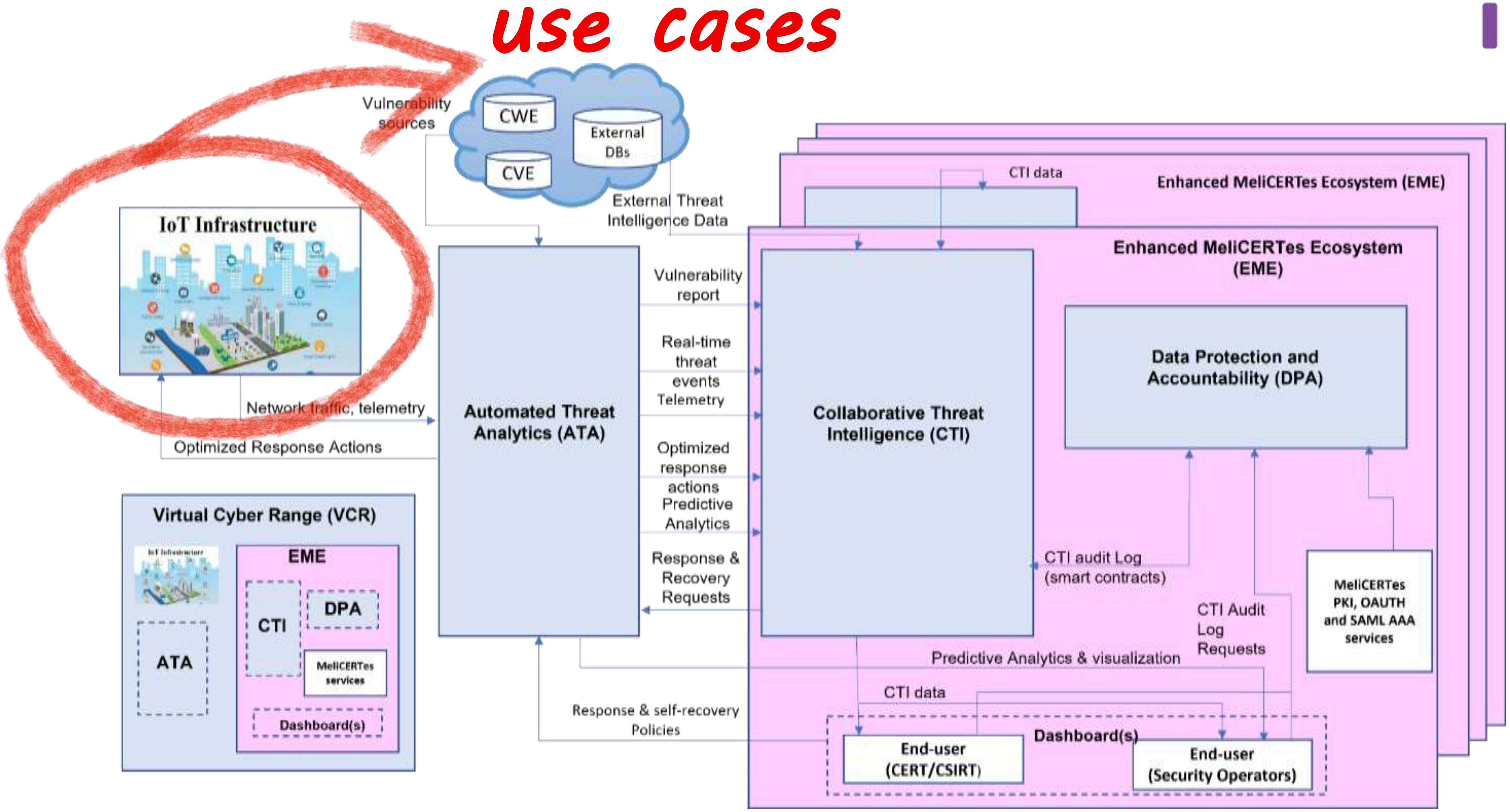


Vulnerability sources
CWE
External DBs
CVE
External Threat Intelligence Data
IoT Infrastructure
Network traffic, telemetry
Optimized Response Actions
Automated Threat Analytics (ATA)
Vulnerability report
Real-time threat events
Telemetry
Optimized response actions
Predictive Analytics
Response & Recovery Requests
CTI data
Enhanced MeliCERTes Ecosystem (EME)
Enhanced MeliCERTes Ecosystem (EME)
Collaborative Threat Intelligence (CTI)
Data Protection and Accountability (DPA)
CTI audit Log (smart contracts)
CTI Audit Log Requests
MeliCERTes PKI, OAUTH and SAML AAA services
Predictive Analytics & visualization
CTI data
Response & self-recovery Policies
Dashboard(s)
End-user (CERT/CSIRT)
End-user (Security Operators)
Virtual Cyber Range (VCR)
IoT Infrastructure
EME
CTI
DPA
ATA
MeliCERTes services
Dashboard(s)
emulation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

IRIS High Level Architecture

use cases



Vulnerability sources

CWE

External DBs

CVE

External Threat Intelligence Data

IoT Infrastructure

Network traffic, telemetry

Optimized Response Actions

Automated Threat Analytics (ATA)

Vulnerability report

Real-time threat events Telemetry

Optimized response actions Predictive Analytics

Response & Recovery Requests

Response & self-recovery Policies

Virtual Cyber Range (VCR)

IoT Infrastructure

ATA

EME

CTI

DPA

MeliCERTes services

Dashboard(s)

CTI data

Enhanced MeliCERTes Ecosystem (EME)

Enhanced MeliCERTes Ecosystem (EME)

Collaborative Threat Intelligence (CTI)

Data Protection and Accountability (DPA)

CTI audit Log (smart contracts)

CTI Audit Log Requests

MeliCERTes PKI, OAUTH and SAML AAA services

Predictive Analytics & visualization

CTI data

Dashboard(s)

End-user (CERT/CSIRT)

End-user (Security Operators)

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors’ view and European Commission is not responsible for any use that may be made of the information it contains.

Tallinn Pilot Use Case

FinEst Centre
for Smart Cities

AI Enabled Infrastructure - Transportation

- Autonomous Vehicle Shuttles for Public Transportation
- Vehicle-to-Everything (V2X) Communication
- Teleoperation/Remote Control Operations Center
- Autonomous Vehicle Telemetry and Smart City Data fused into Urban Operating Platform (UoP)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

Scenario 1: Telematics and Smart City Data Exchange & Security

- The Autonomous Vehicle (AV) Shuttle fleet will navigate around the smart campus environment
- Urban Operating Platform (UoP) gathers AV Shuttle telemetry
- UoP stores
  - ✓ Location of the vehicles
  - ✓ Navigation
  - ✓ Odometry
  - ✓ …

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

Scenario 2: Trustworthiness of Machine Vision Telemetry

- The Autonomous Vehicle (AV) approaches a traffic-light controlled intersection or roadway
- The machine vision of the AV focusses on the traffic light
- The AV object-detection module detects the traffic light color
- Depending on the traffic light the AV will pass-through or stop

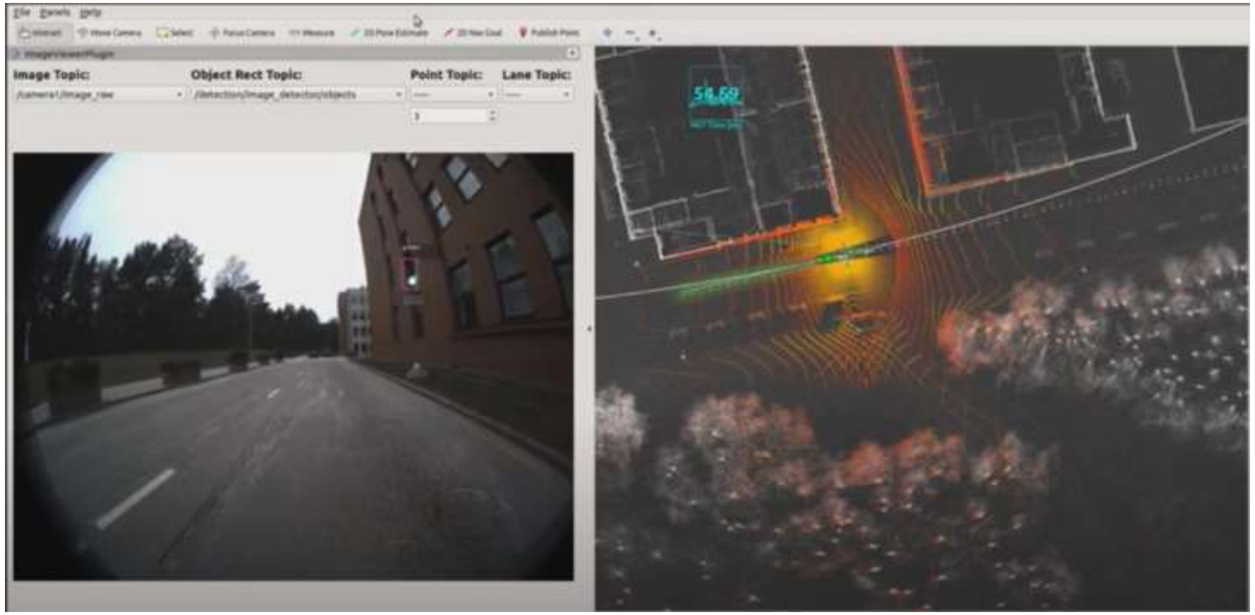


Image Topic: /camera1/image_raw

Object Rect Topic: /detection/image_detector/objects

Point Topic: ----

Lane Topic: ----

3

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors’ view and European Commission is not responsible for any use that may be made of the information it contains.

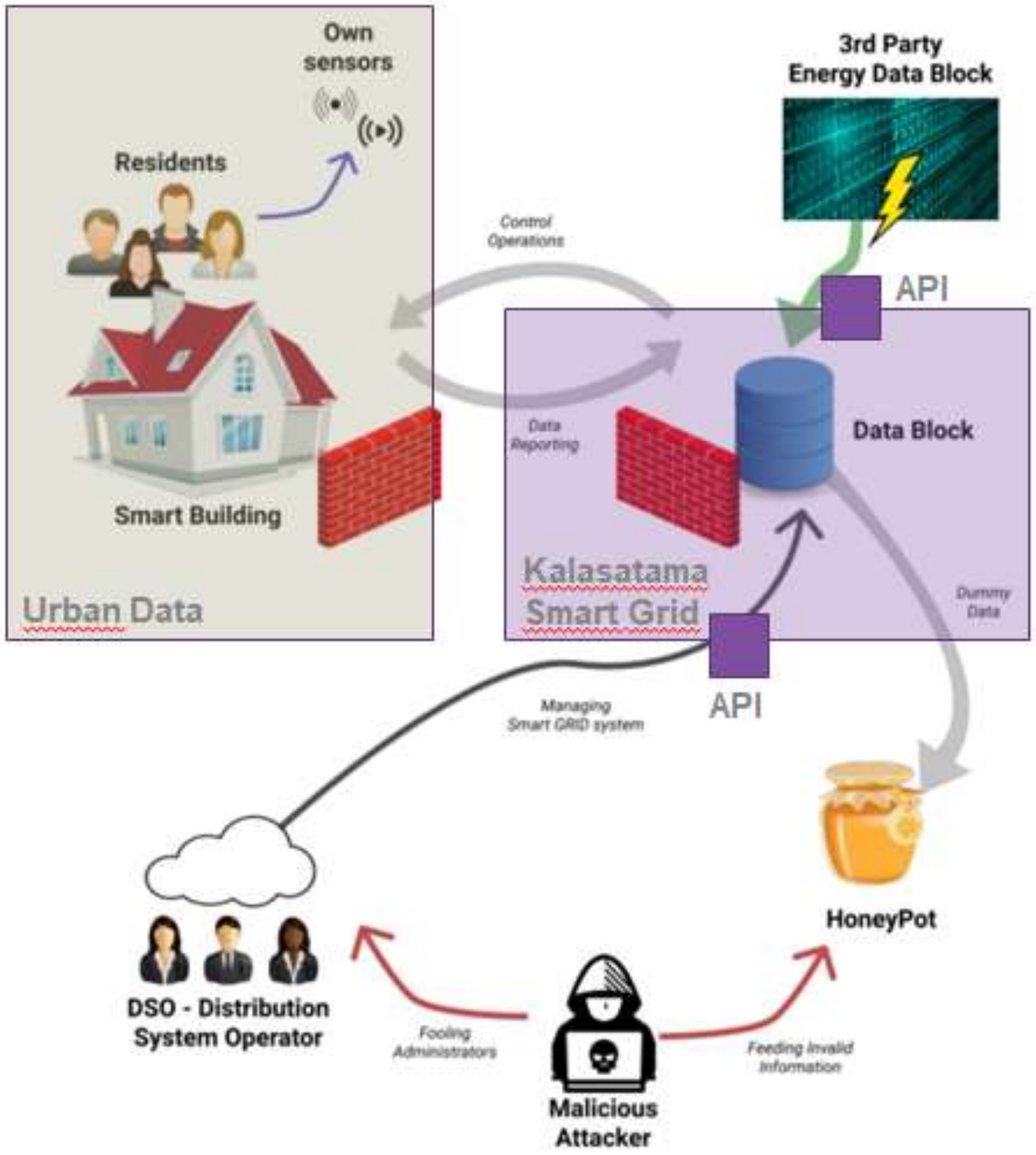
Tallinn Pilot Cyber Threat Scenarios

- Availability of telemetric data from the AV to the Urban Operating Platform (UoP)
- False information being fed to disrupt the ML/AI used for autonomous driving

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

Helsinki Pilot Use-Case

FORUM
VIRIUM
HELSINKI



Components

Kalasatama smart grid

Kalasatama smart grid APIs

Kalasatama smart district **Digital Twin**

Provision of **load control**

Urban Data Platform (IoT)

Smart grid APIs from the city of Tallinn.

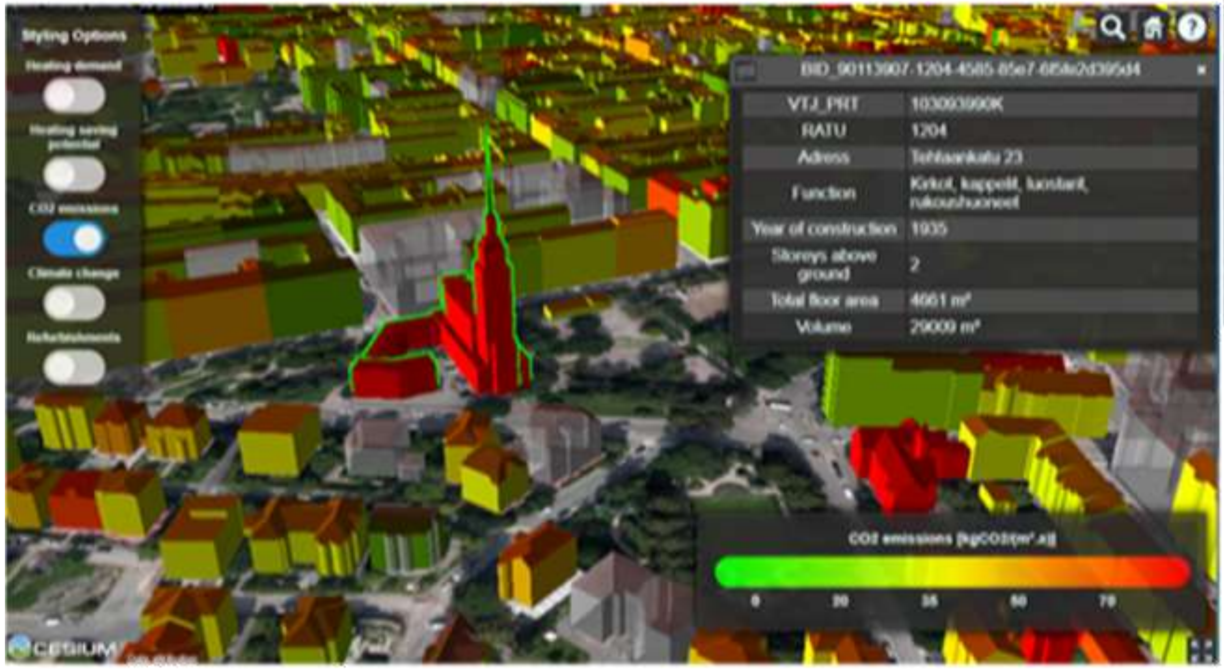
This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors’ view and European Commission is not responsible for any use that may be made of the information it contains.

Smart Kalasatama Data Examples

- Solar Energy Potential
  - ✓ Amount of solar radiation in buildings
- Heating Demand Prediction
  - ✓ Heating energy demand prediction until 2050
- Geoenergy Potential
  - ✓ 150m / 300m / 1000m deep well potentials, groundwater areas, ...
- Energy Data of Buildings
  - ✓ Municipal register information (e.g., heating method of buildings, usage, ...)
  - ✓ Repairs and alterations
  - ✓ Protected buildings
  - ✓ Calculated energy consumption of buildings by age group

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

Digital Twin



Styling Options

Heating demand ○

Heating saving potential ○

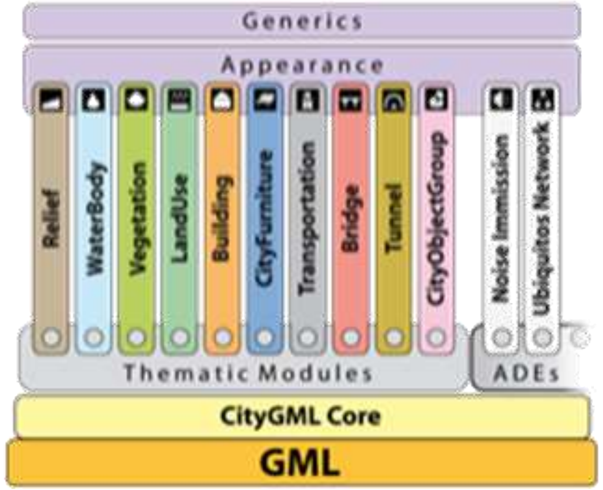
CO2 emissions ●

Climate change ○

Refurbishments ○

BID_90113907-1204-4585-85e7-6f54e2d395d4

VTJ_PRT	103093990K
RATU	1204
Adress	Tehtaankatu 23
Function	Kirkot, kappelit, luostarit, rukoushuoneet
Year of construction	1935
Storeys above ground	2
Total floor area	4061 m²
Volume	29009 m³



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

IRIS Barcelona Use Case

Ajuntament de Barcelona

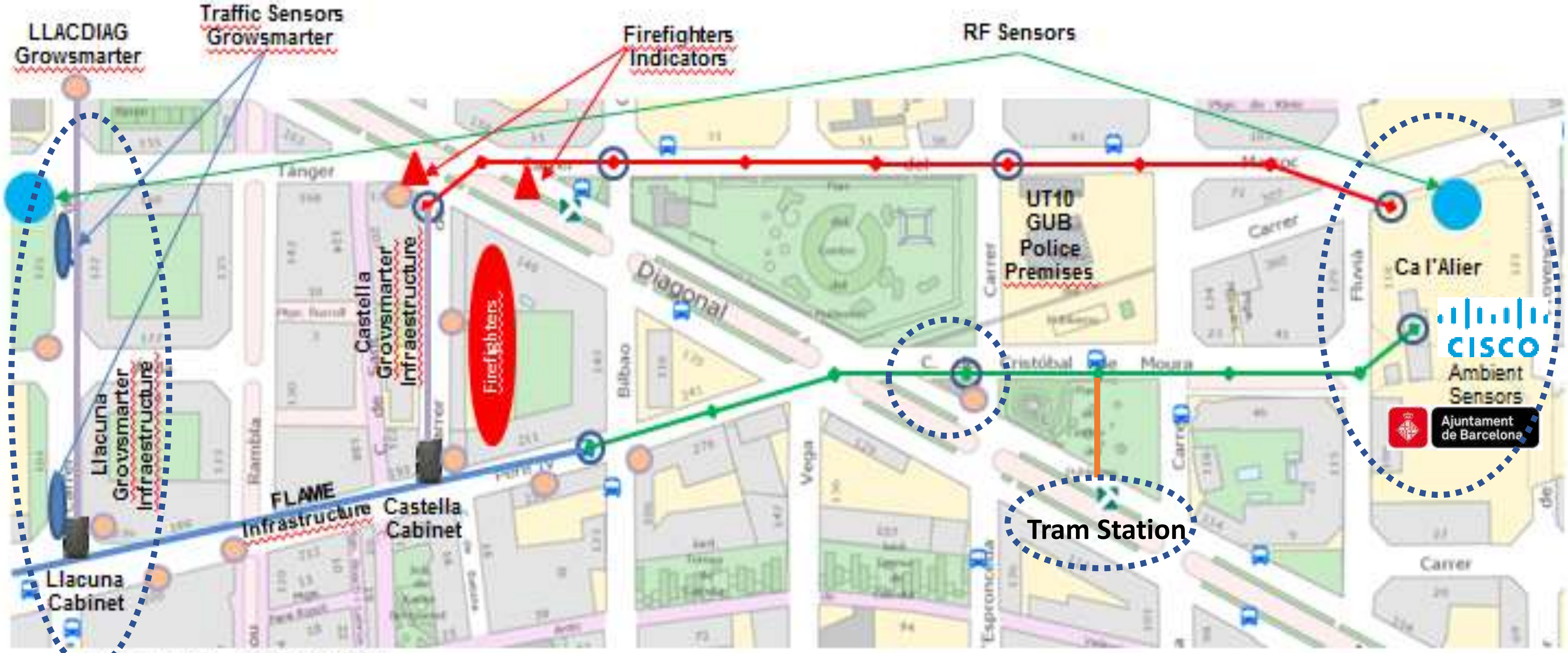
Atos

cisco

ESCERT 25 Años

UPC inLab FIB talent & tech

Integration of IRIS initiative in 5GBarcelona Testbed



Principal Way

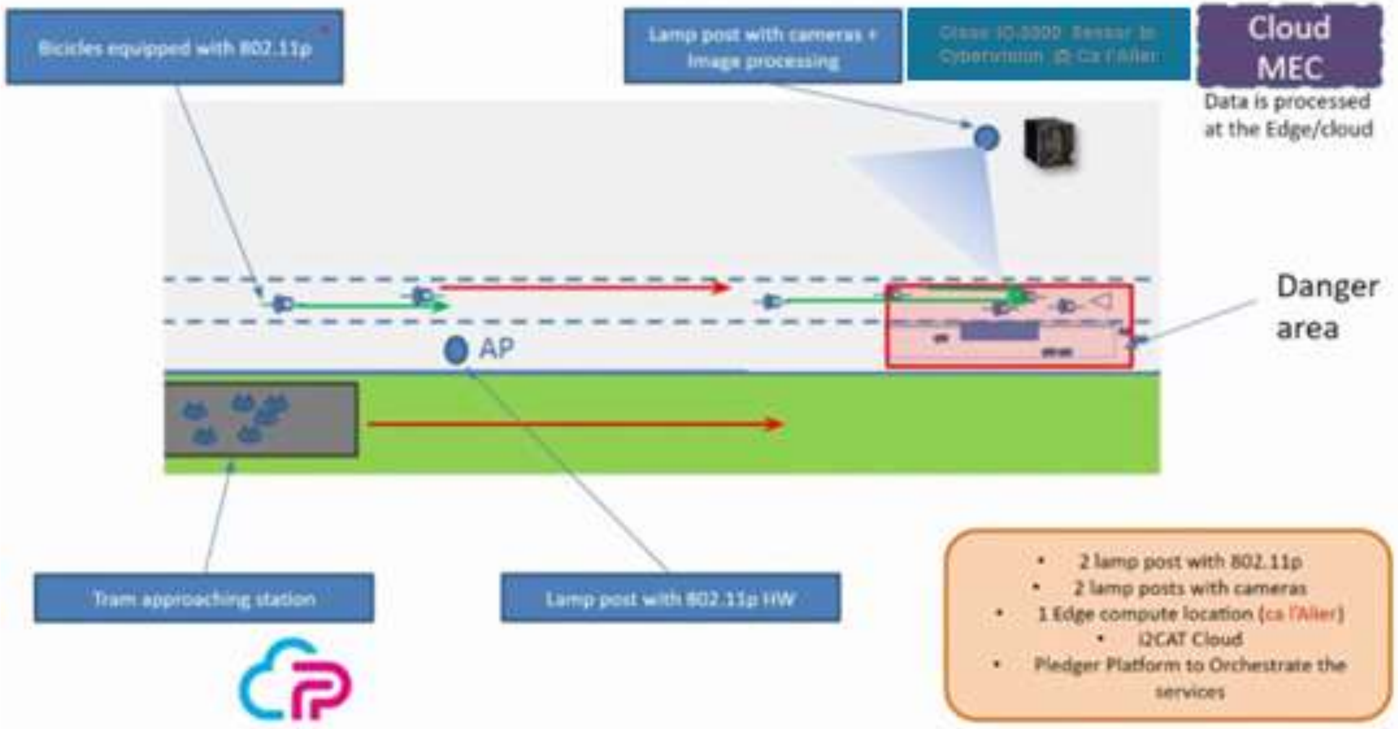
Alternative Way

Fiber links planned to connect Barcelona Testbed with Ca l'Alier premises (CISCO research center)

● Access Nodes from projects: Growsmarter, FLAME, 5GCITY & Barcelona WIFI with potential to reuse in IRIS

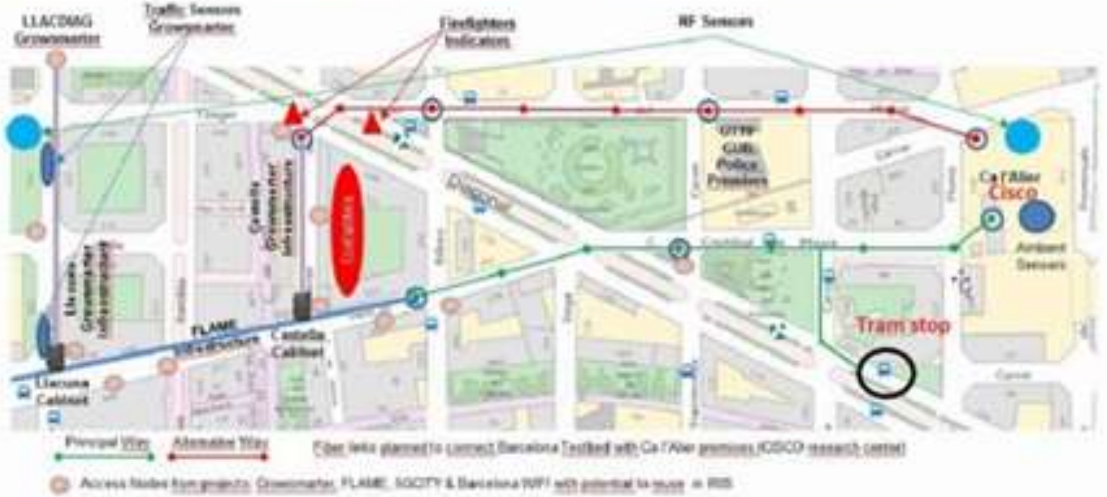
Smart Cities Service: Vulnerable Road Users (VRUs) Protection

- VRUs (Bicicles/E-Scooters + pedestrians) are exposed to dangerous situations, when people exiting the tram at a station cross the bicycle lane to get to the pedestrian lane.
- With 802.11p to detect bicycles and image processing to detect the tram, possible risky situations are detected and notifications are sent out to warn the different actors.



Bicicles equipped with 802.11p
Lamp post with cameras + Image processing
Cisco IO-3000 Sensor to Cybervision @ Ca l'Alier
Cloud MEC
Data is processed at the Edge/cloud
AP
Danger area
Tram approaching station
Lamp post with 802.11p HW

- 2 lamp post with 802.11p
- 2 lamp posts with cameras
- 1 Edge compute location (ca l'Alier)
- i2CAT Cloud
- Pledger Platform to Orchestrate the services



LLACUNAG Growsmarter
Traffic Sensors Growsmarter
Firefighters Indicators
RF Sensors
OTTP GUB Police Providers
Ca l'Alier
Cisco
Ambient Sensors
Castella Growsmarter Infrastructure
Llacuna Growsmarter Infrastructure
FLAME Infrastructure
Castella Cabinet
Llacuna Cabinet
Tram stop
Principal Way
Alternative Way
Fiber links planned to connect Barcelona Testbed with Ca l'Alier premises (CISCO research center)
Access Nodes from projects: Growsmarter, FLAME, 5GCITY & Barcelona WiFi with potential to reuse in IRIS

Cybersecurity Challenges

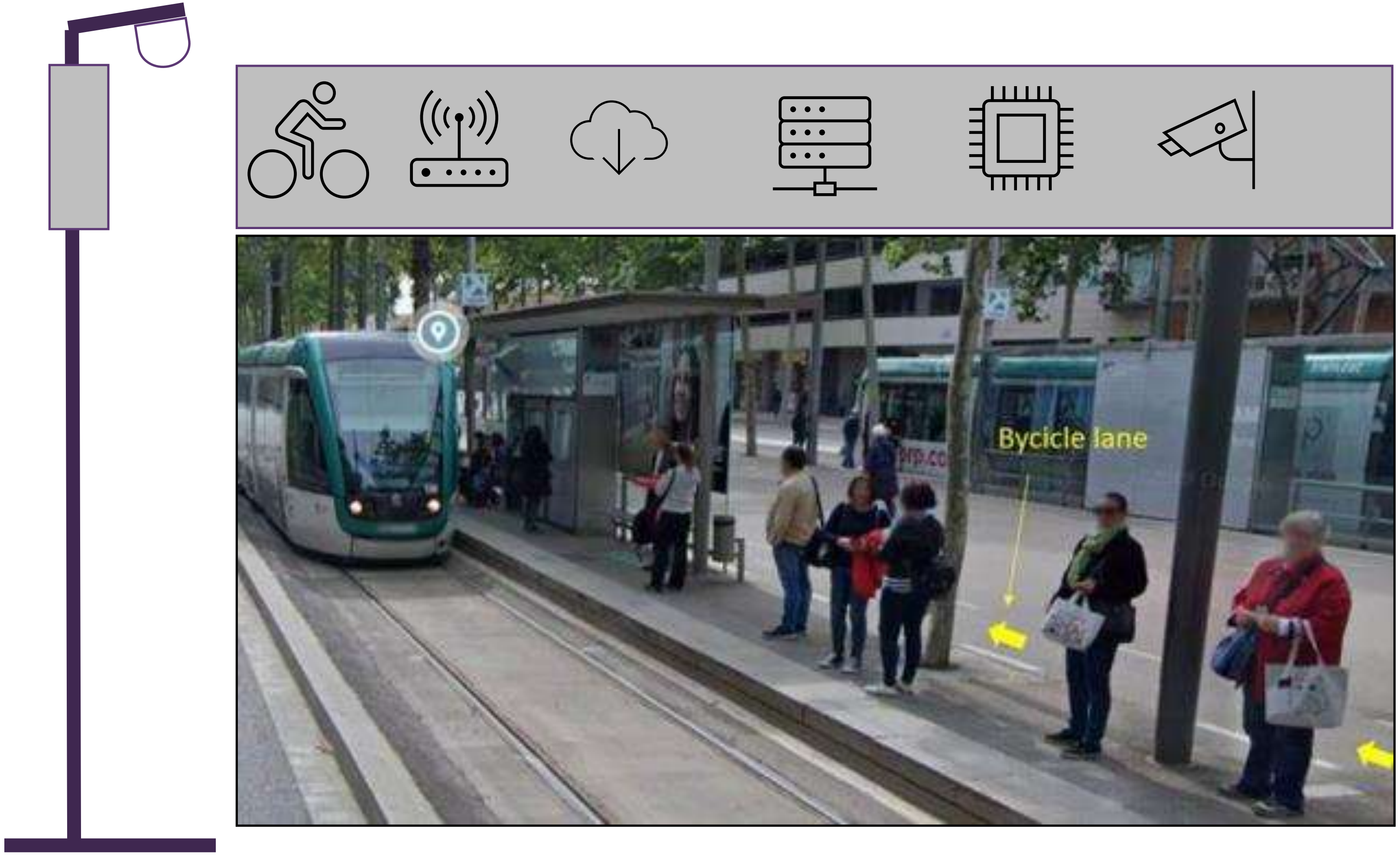
- Ensuring availability of IoT and IA infrastructure for the safety of tram users.

- Lack of experience as well as of tools, for detecting and reporting IoT & AI attack vectors.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors’ view and European Commission is not responsible for any use that may be made of the information it contains.

AI & IoT Infrastructure

Leveraging Infrastructure of Horizon 2020 Project Pledger



IoT & AI attack vectors

- 801.11p Wireless devices
- Networking equipment routers and switches
- Edge computing
- Cameras
- AI computer vision

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

Cyber Threat Scenarios

On-Street cameras generate information about the intersection status. This information is used by Tramway operators to control (allow/disallow) the Tramway. This information is shared through an API.

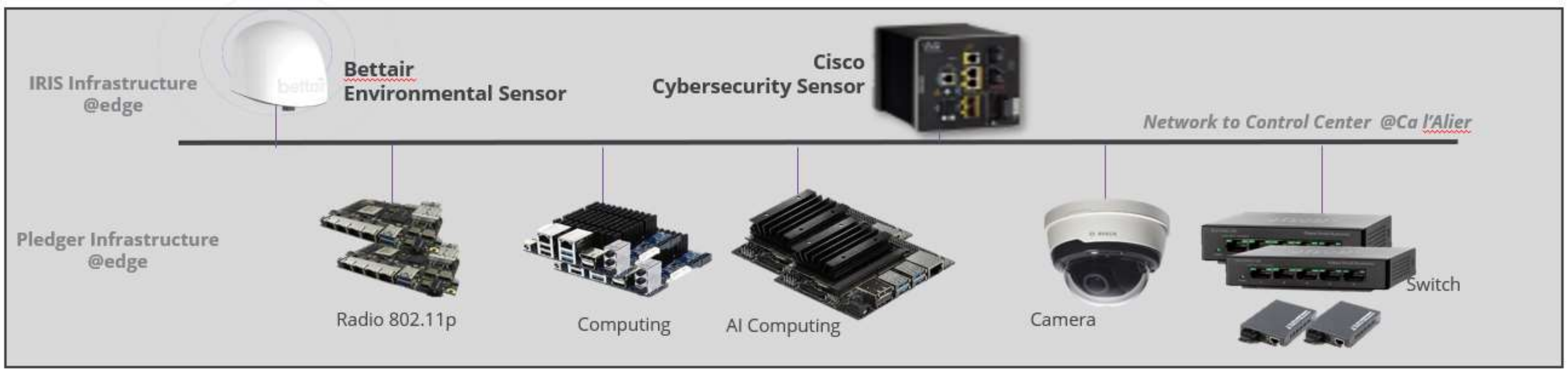
Threat Actor Injects fake data by targeting the different hardware appliances in the scenario with the goal of either denying the service, thus forcefully stopping the Tramway, or faking the presence of a possible pedestrian or bicycle approaching the intersection.

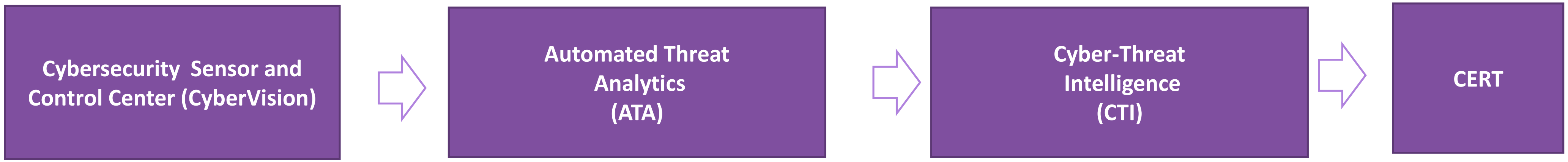
IRIS ATA module is able identify actionable and accurate cyber threats against the availability of the supporting infrastructure.
Also, IRIS will assist CERT investigation and incident response through the **CTI module**, Sharing the information about the attacks and security breaches.

CERT and Tramway operators are notified by IRIS Platform.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors’ view and European Commission is not responsible for any use that may be made of the information it contains.

AI & IoT Infrastructure + cybersecurity and environmental sensors



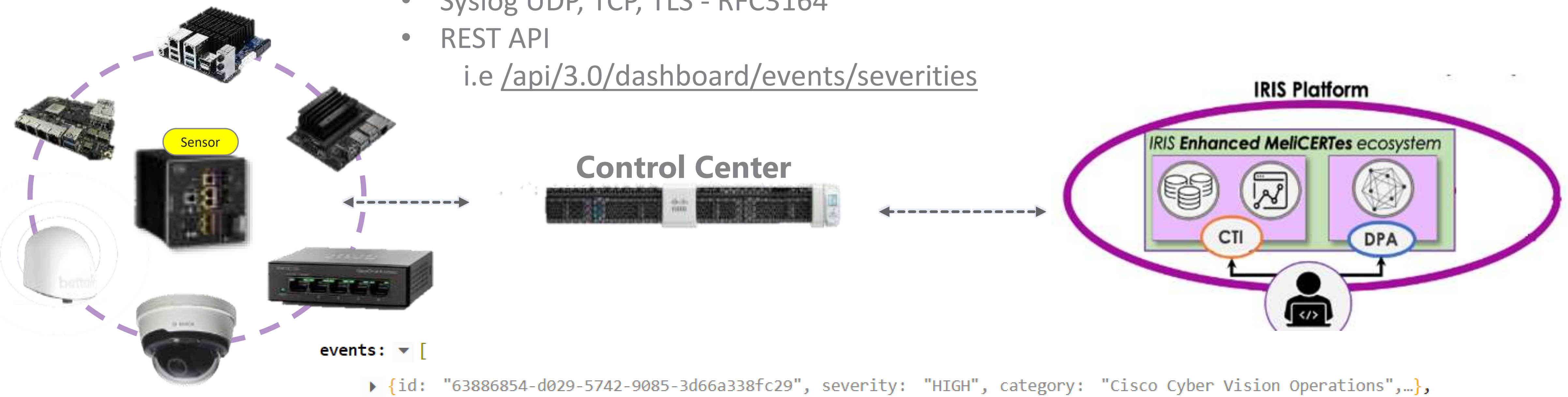

Cybersecurity Sensor and Control Center (CyberVision)
Automated Threat Analytics (ATA)
Cyber-Threat Intelligence (CTI)
CERT

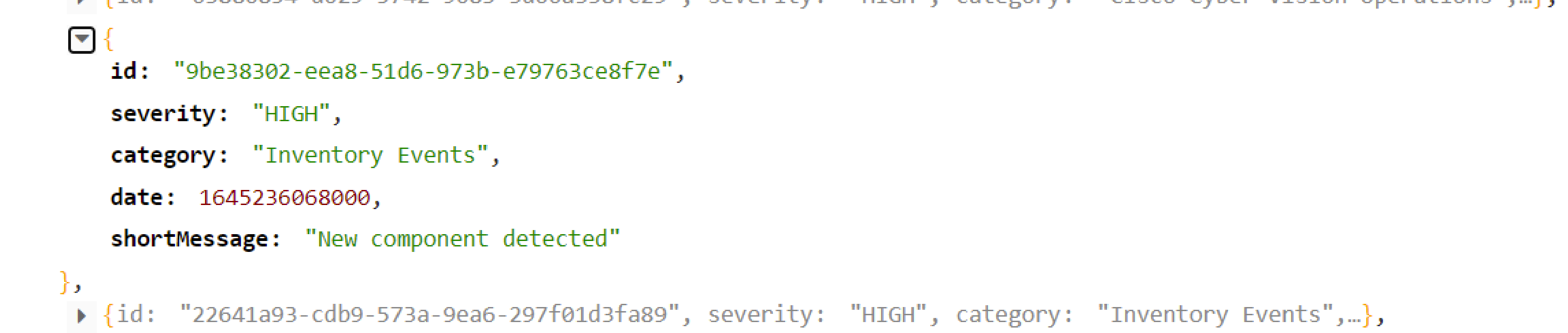
Cybersecurity Sensor uses DPI technology to extract meaningful information (data & metadata) for the network devices using 100% passive sensor. Information is sent to **CyberVision Control Center** and reported to **IRIS Automated Threat Analytics (ATA)** module that extends existing intrusion detection tools to identify specific IoT and AI attack vectors, then shared through **IRIS Collaborative Secure and Trusted Cyber-Threat Intelligence (CTI)**

Connecting to IRIS Autonomous Threat Analytics (ATA) and Cyber-Threat Intelligence Sharing (CTI)

- Syslog UDP, TCP, TLS - RFC3164
- REST API

  i.e /api/3.0/dashboard/events/severities



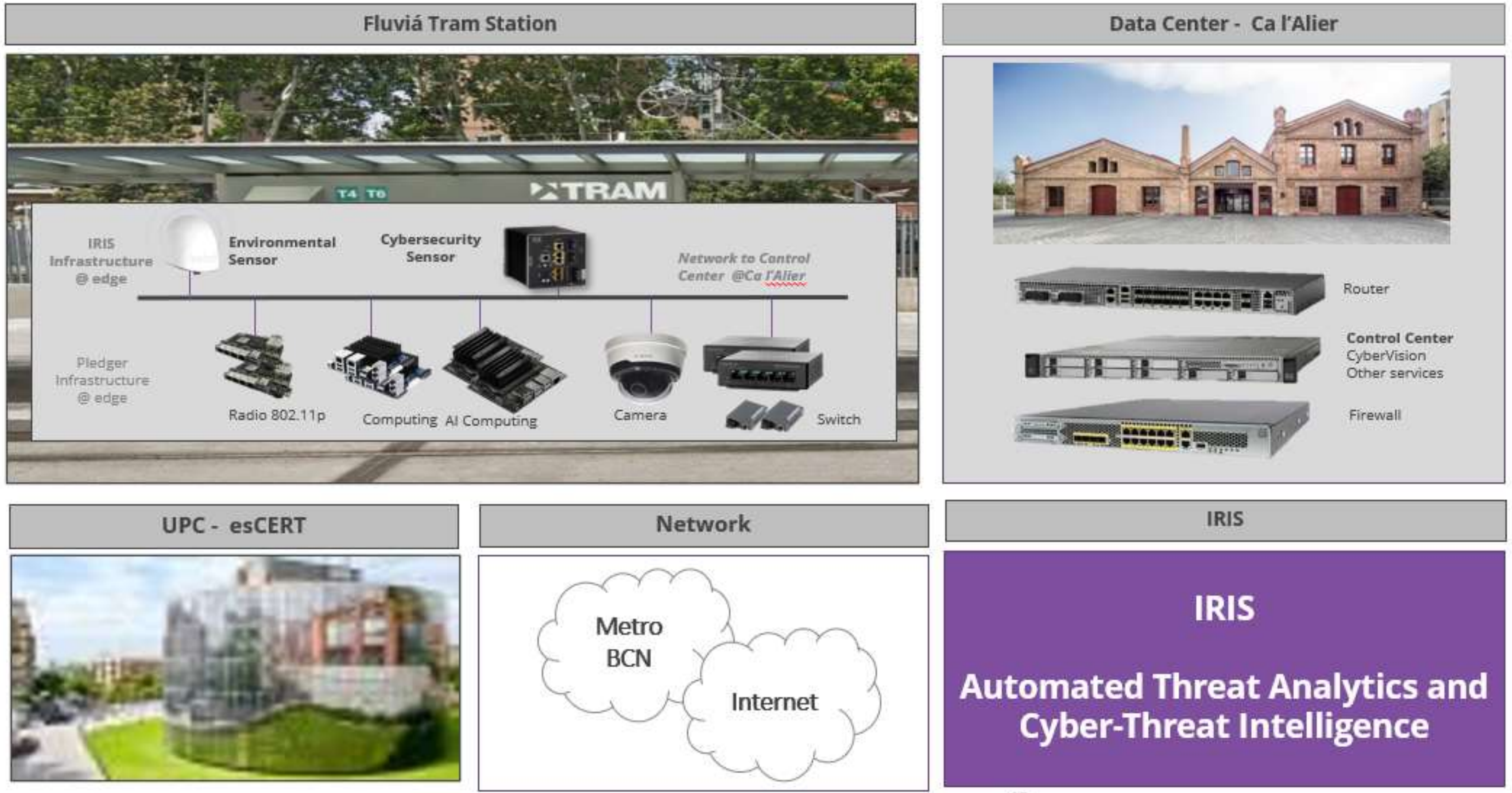


```
events: ▼ [
  ▶ {id: "63886854-d029-5742-9085-3d66a338fc29", severity: "HIGH", category: "Cisco Cyber Vision Operations",…},
  ▼ {
     id: "9be38302-eea8-51d6-973b-e79763ce8f7e",
     severity: "HIGH",
     category: "Inventory Events",
     date: 1645236068000,
     shortMessage: "New component detected"
  },
  ▶ {id: "22641a93-cdb9-573a-9ea6-297f01d3fa89", severity: "HIGH", category: "Inventory Events",…},
```

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

Barcelona Pilot – IRIS Platform Validation

- Identification of attacks
- Information sharing to IRIS platform of incidents
- Enable Cyber Incident Response from CERTS



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

Thank you for your attention!
Any questions?

iris-h2020.eu

IRIS H2020 Project

iris_h2020