Artificial Intelligence Threat Reporting & Incidence report System

IRIS: a Framework for enhancing CERTs and CSIRTs Collaborative Response to Cyberattacks

René Serral (UPC)

Xavier Azemar (Cisco)

Mariano Lamarca (IMI)

Rodrigo Diaz (ATOS)

SCEWC / 15th November 22

Project at a Glance

Consortium

- **6 Public organizations**
- **3 SMEs**
- **4 Large ICT industries**
- **6 Research institutions & Universities**

Call Identifier: 2020-SU-DS-2020

Topic: SU-DS02-2020 Intelligent security and privacy management

EC Funding: 4 918 790.00

Duration: 36 months (Sept 2021-Aug 2024)

Consortium: 19 partners

Coordinator: INOV - Instituto de Engenharia de Sistemas e Computadores, Inovacão, (INOV), Portugal

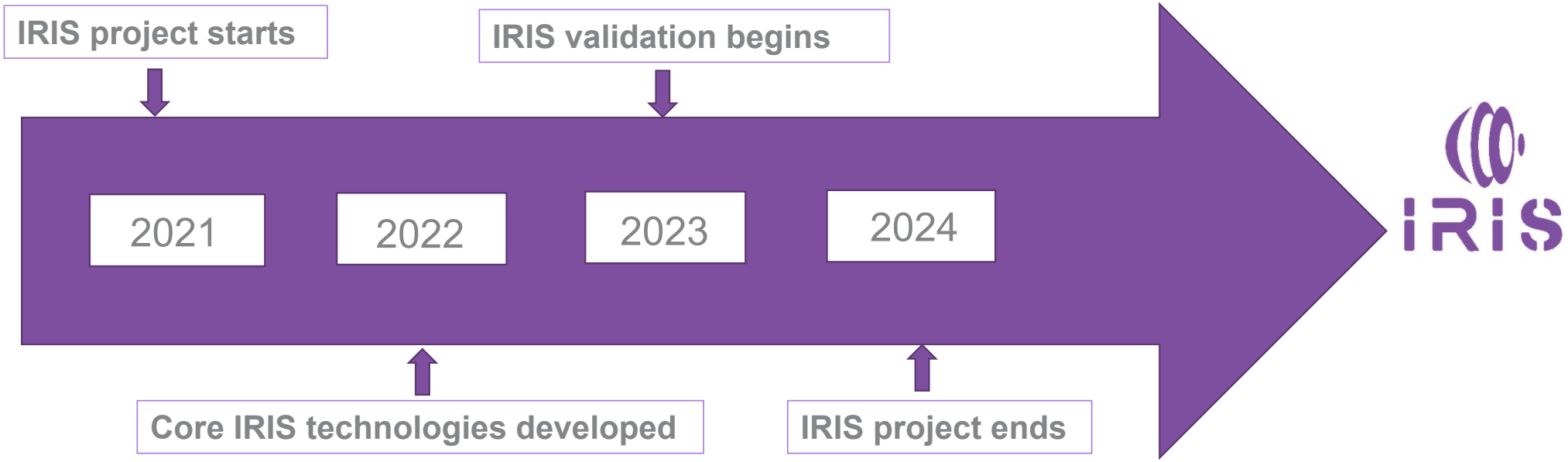
Learn More: www. iris-h2020.eu

Join us: @iris-h2020

IRIS H2020 Project

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 Time Plan



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 Smart Cities

IoT and AI-Enabled platforms

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

The **H2020 IRIS project** aims to deliver a framework that will support European CERT and CSIRT networks **detecting, sharing, responding and recovering from cybersecurity threats and vulnerabilities of IoT and AI-driven ICT systems,** in order to **minimize the impact of cybersecurity and privacy risks.**

The IRIS platform will be made available, **free of charge**, to the European national CERT and CSIRTs, by the end of the project.

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

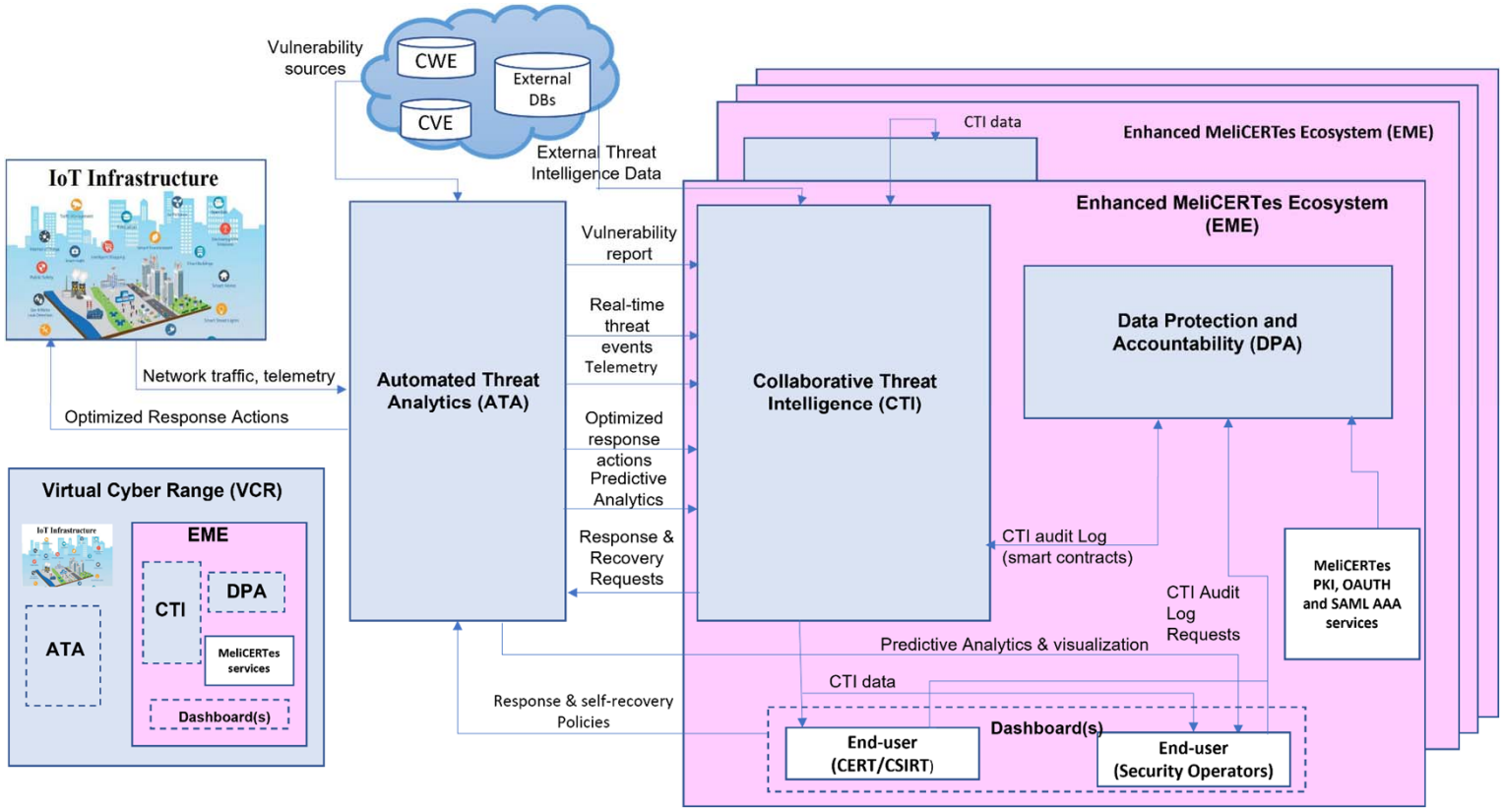
- To **identify** the user, technical and business requirements and **design** the architecture of an AI threat reporting and incident response system
- To **analyze** the relevant ethics principles and legal framework on privacy concerns
- To **develop** a collaborative platform for ICT stakeholders and European CERTs/CSIRTs for the successful operation of IoT and AI-enabled ICT systems
- To **demonstrate** and **validate** the integrated IRIS platform across three realistic pilot demonstrators in three smart cities
- To **ensure** wide communication and scientific dissemination of the IRIS results, efficient exploitation and contribution to relevant standardization bodies

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 Methodology

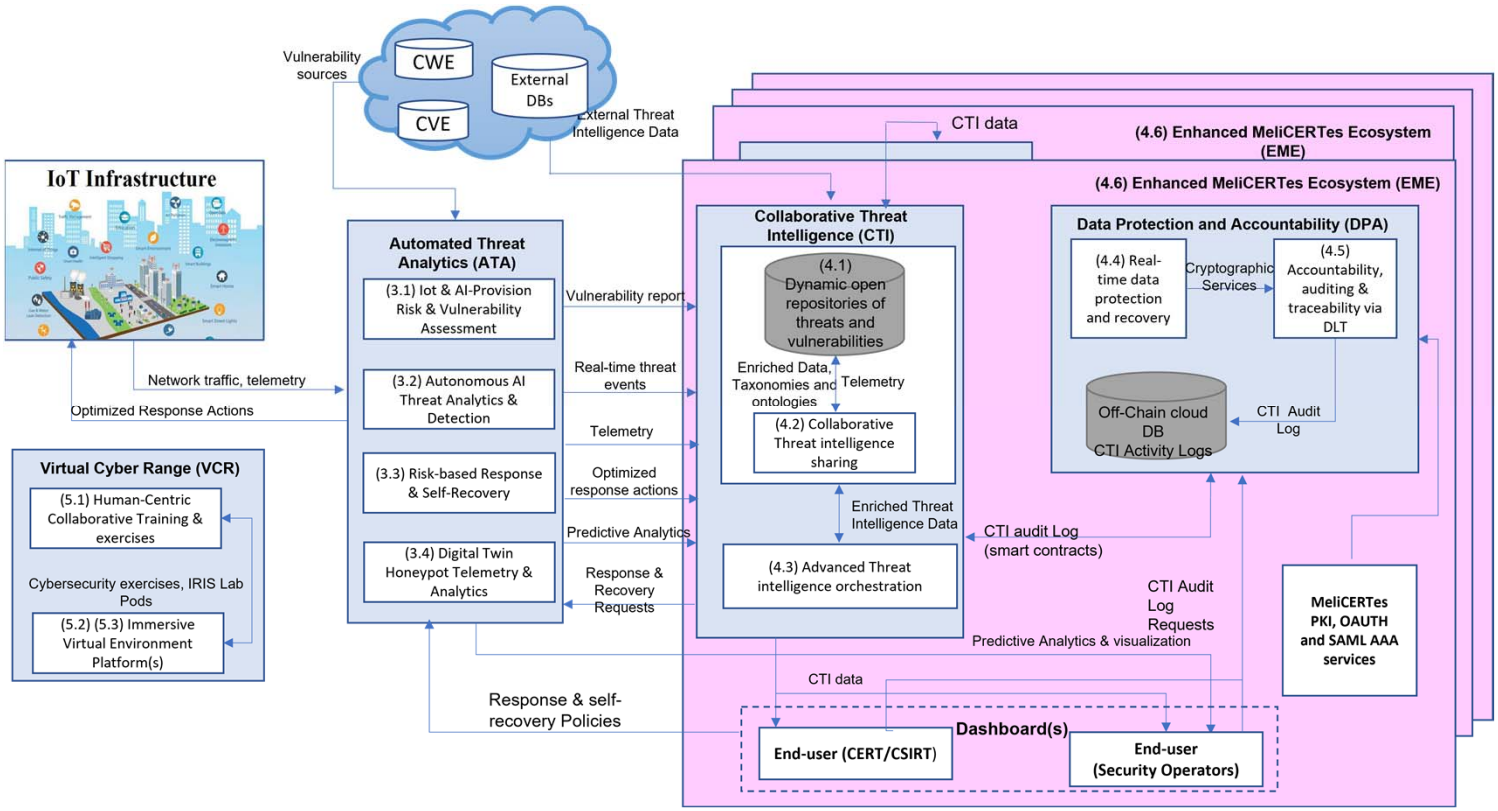
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

IRIS High Level Architecture



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 Task View Architecture

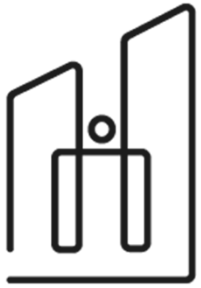


This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

IRIS

Artificial Intelligence Threat Reporting & Incidence report System

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.

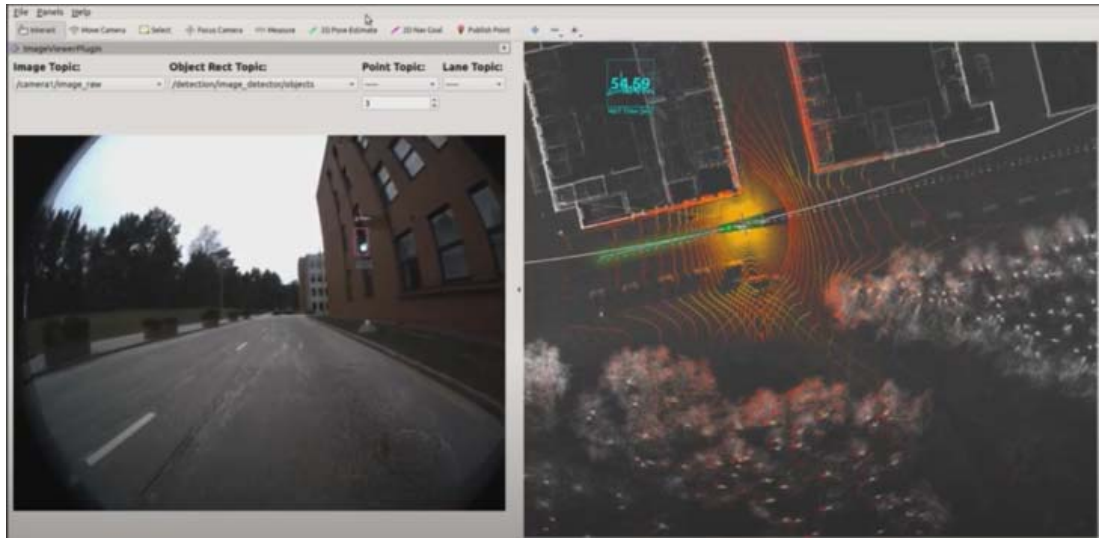
Scenario 1: Telematics and Smart City Data Exchange & Security

- 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



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

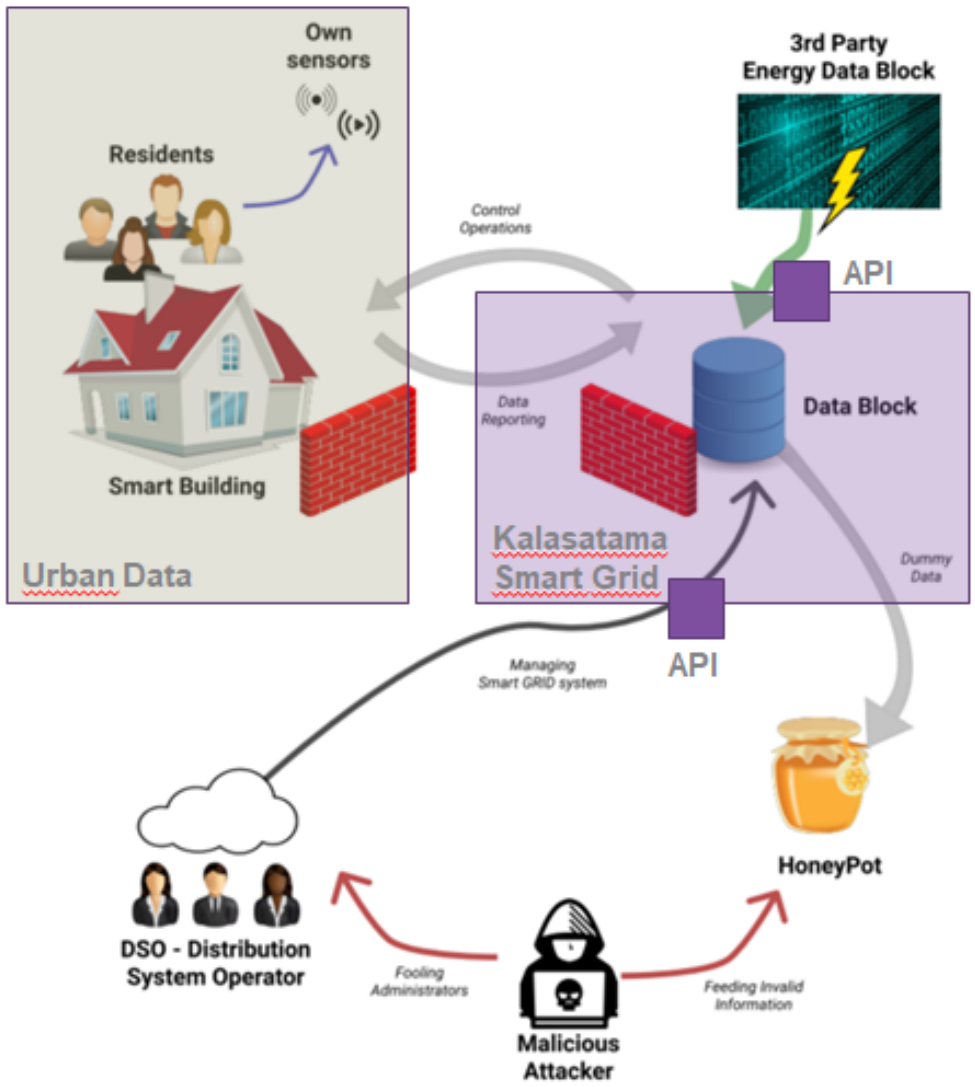
- Availability of telemetric data from the AV to the Urban Operating Platform (UoP)
- False information being fed to disrupt the ML/AI used for autonomous driving

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.

Artificial Intelligence Threat Reporting & Incidence report System

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.

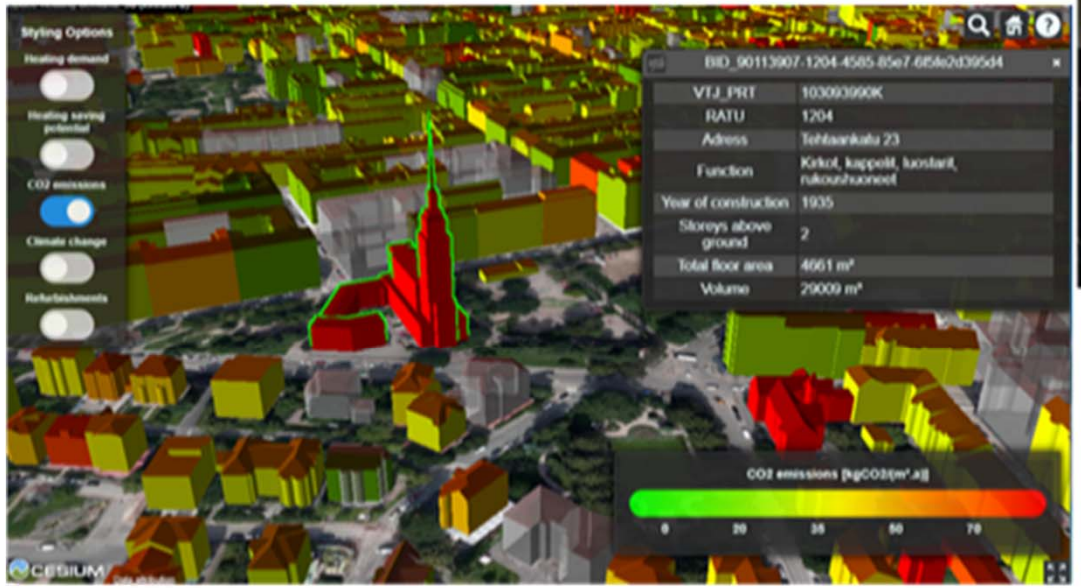
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

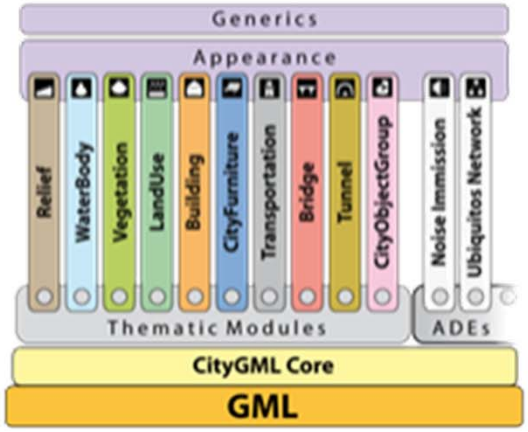
Smart Kalasatama Data Examples

- 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



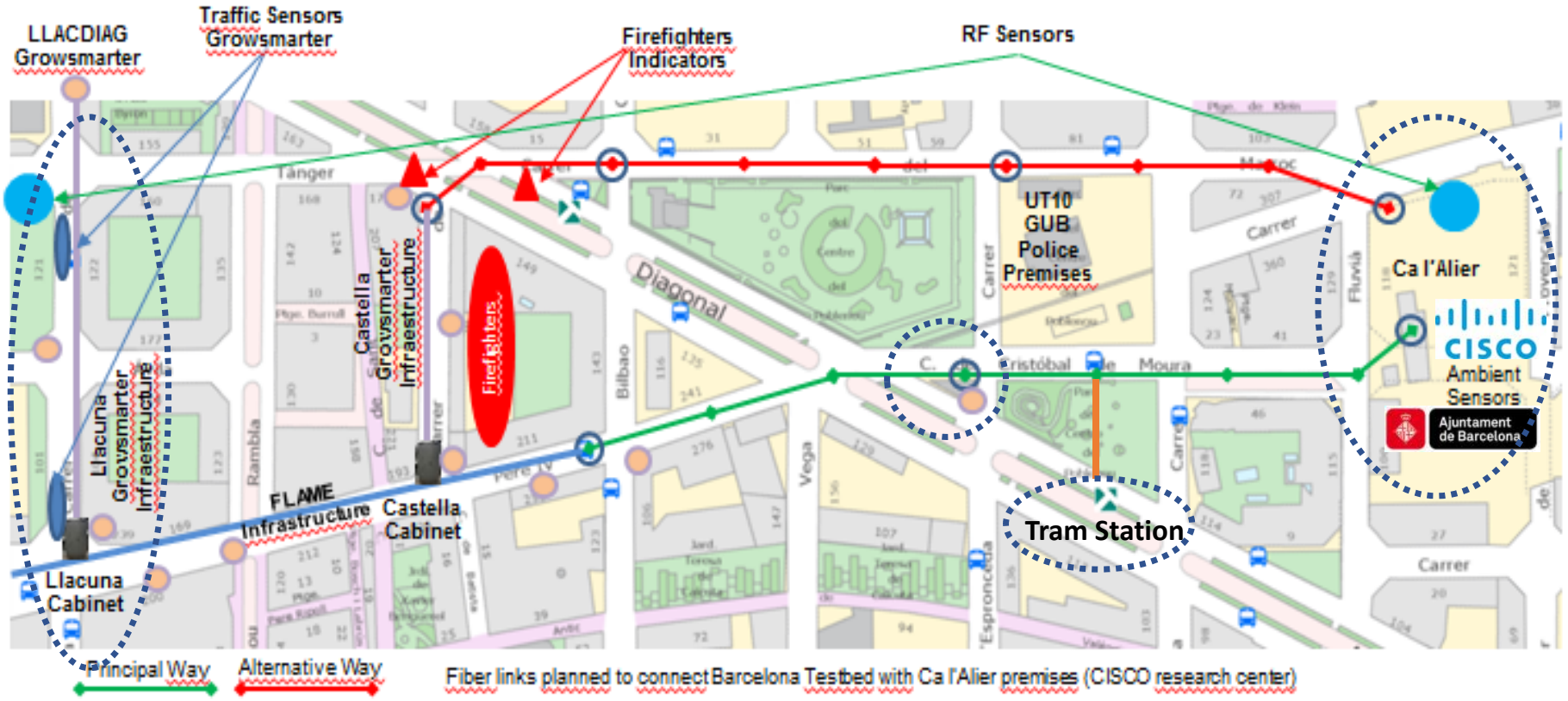


This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

Artificial Intelligence Threat Reporting & Incidence report System

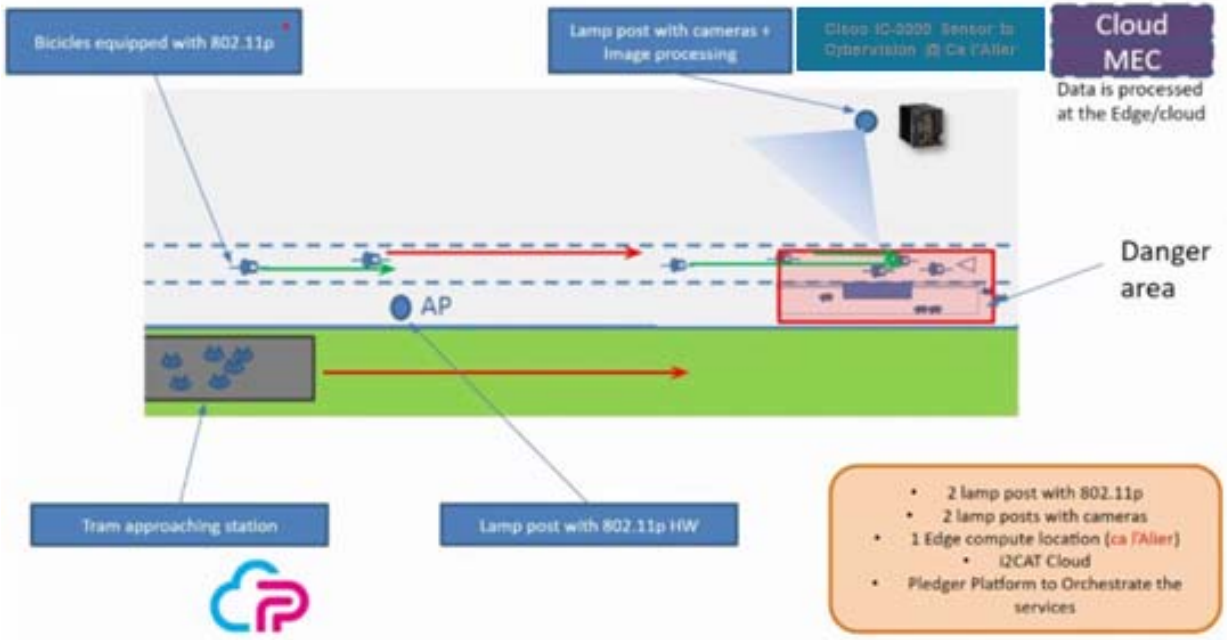
IRIS Barcelona Use Case

Integration of IRIS initiative in 5GBarcelona Testbed



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.



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.

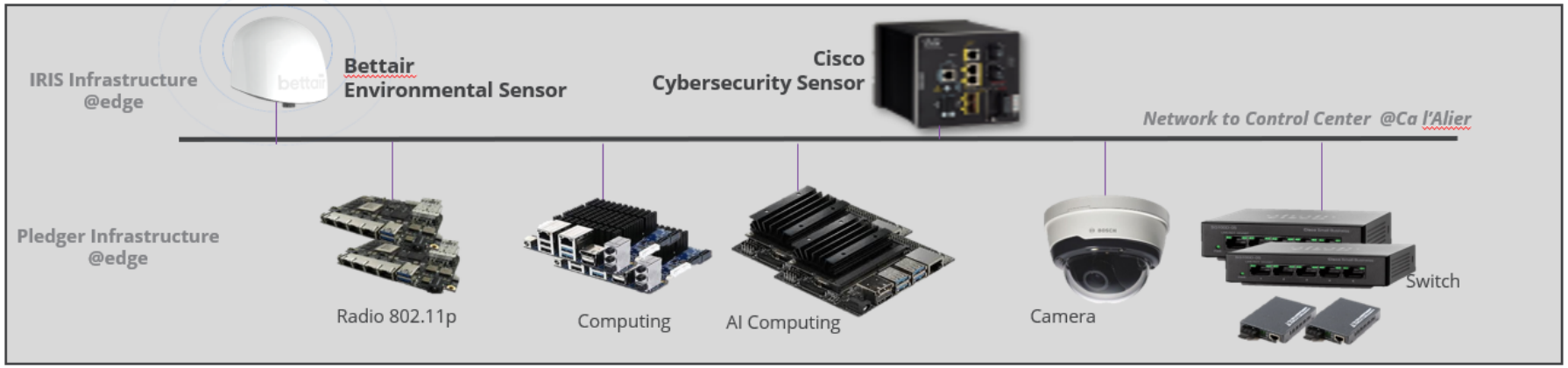
Threat Actor Injects fake data by targeting the different hardware appliances in the scenario with the goal of either denying the service, thus forcefully stopping the Tramway, or faking the presence of a possible pedestrian or bicycle approaching the intersection.

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

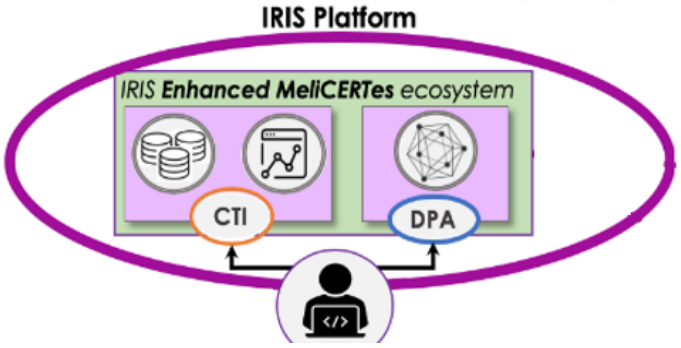


Cybersecurity Sensor and Control Center (CyberVision) → **Automated Threat Analytics (ATA)** → **Cyber-Threat Intelligence (CTI)** → **CERT**

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

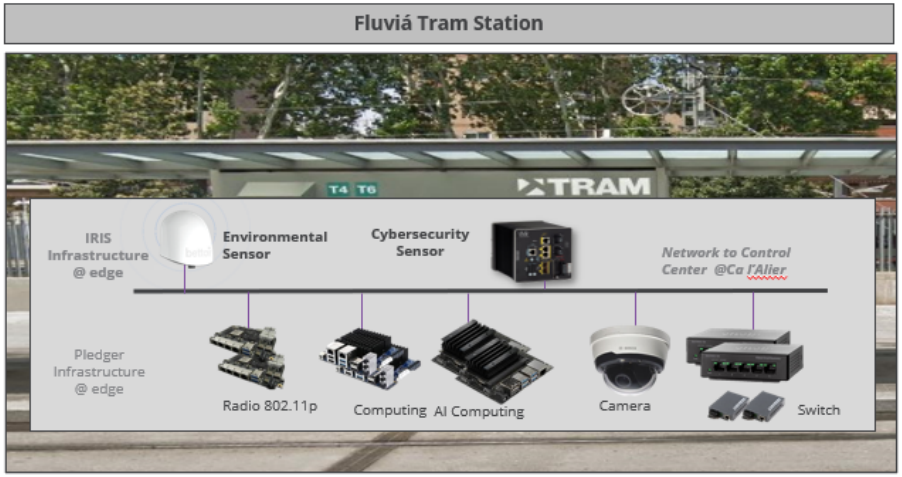


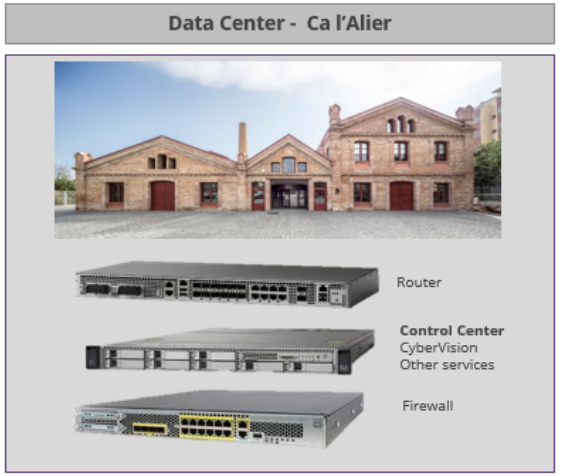

```
events: [
  {id: "63886854-d029-5742-9085-3d66a338fc29", severity: "HIGH", category: "Cisco Cyber Vision Operations",…},
  {
    id: "9be38302-eea8-51d6-973b-e79763ce8f7e",
    severity: "HIGH",
    category: "Inventory Events",
    date: 1645236068000,
    shortMessage: "New component detected"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

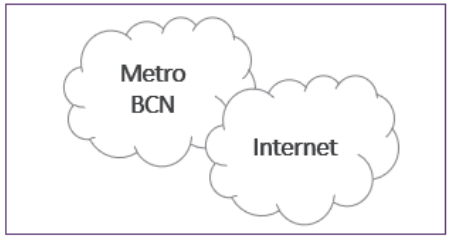

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

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