Artificial Intelligence Threat Reporting & Incidence report system

Nelson Escravana

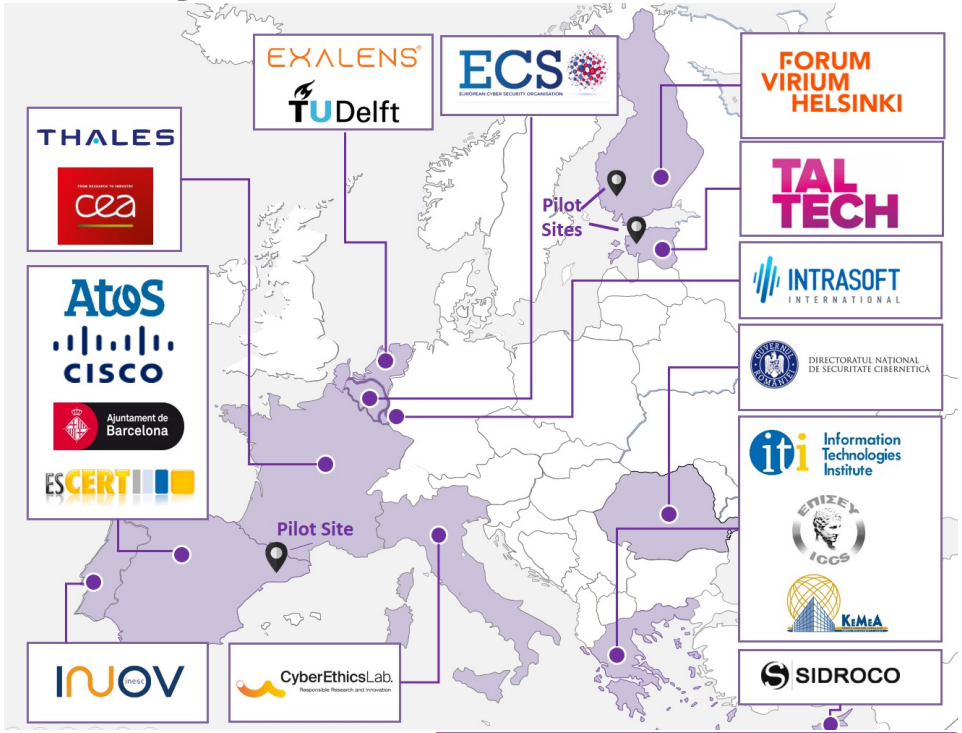
IRIS - Sistema de Relatórios de Ameaças e Resposta a Incidentes de Inteligência Artificial

Nelson Escravana

Rede Nacional CSIRTS .PT

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.

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 Motivation

As existing and emerging **smart cities** continue to **expand their IoT and AI-enabled platforms**, **novel and complex dimensions to the threat intelligence landscape are introduced**. These, are linked with identifying, responding and sharing data related to attack vectors, based on emerging IoT and AI technologies, whose architecture and behaviour are **not currently well understood** by security practitioners, such as CERTs and CSIRTs.

This lack of experience as well as of **tools, for detecting and reporting IoT & AI attack vectors** is further aggravated by potentially greater safety risks caused by such attacks.

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.**

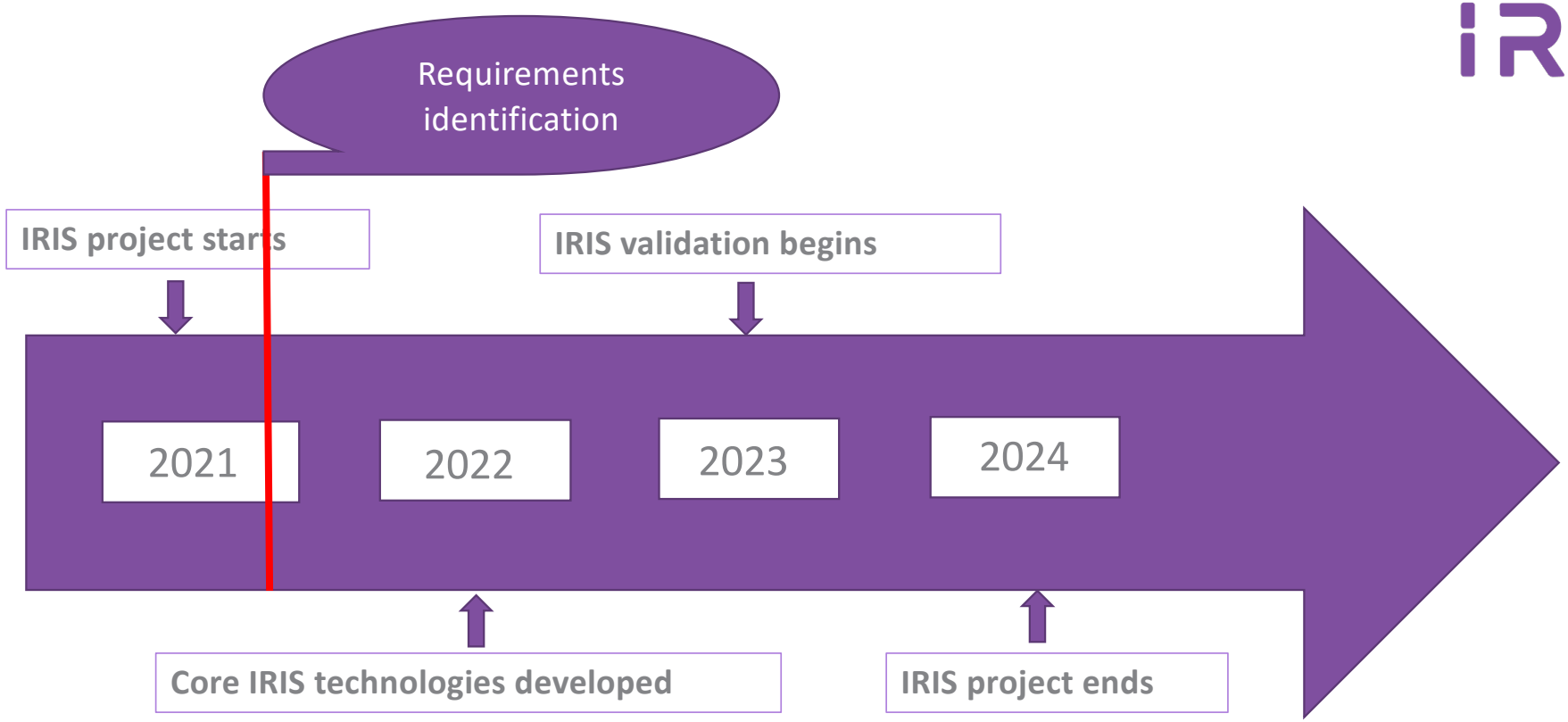
The IRIS platform will be made available, **free of charge**, to the European national CERT and CSIRTs, by the end of the project.

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 Methodology

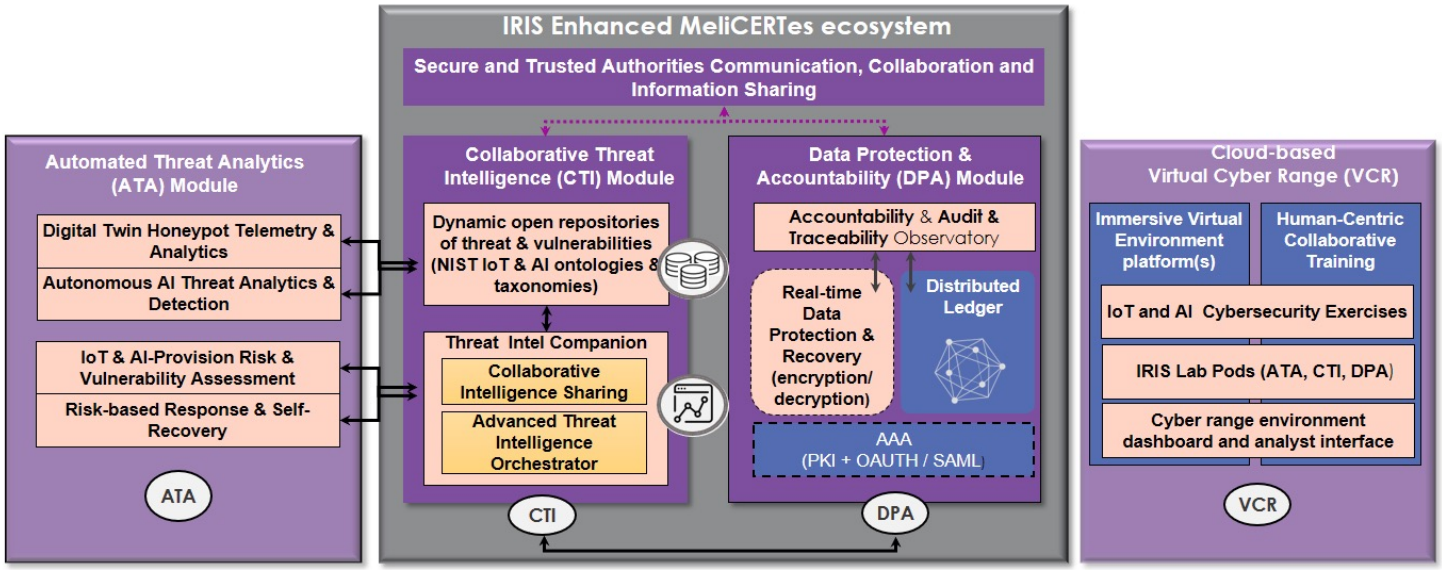
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727. This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

IRIS 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.

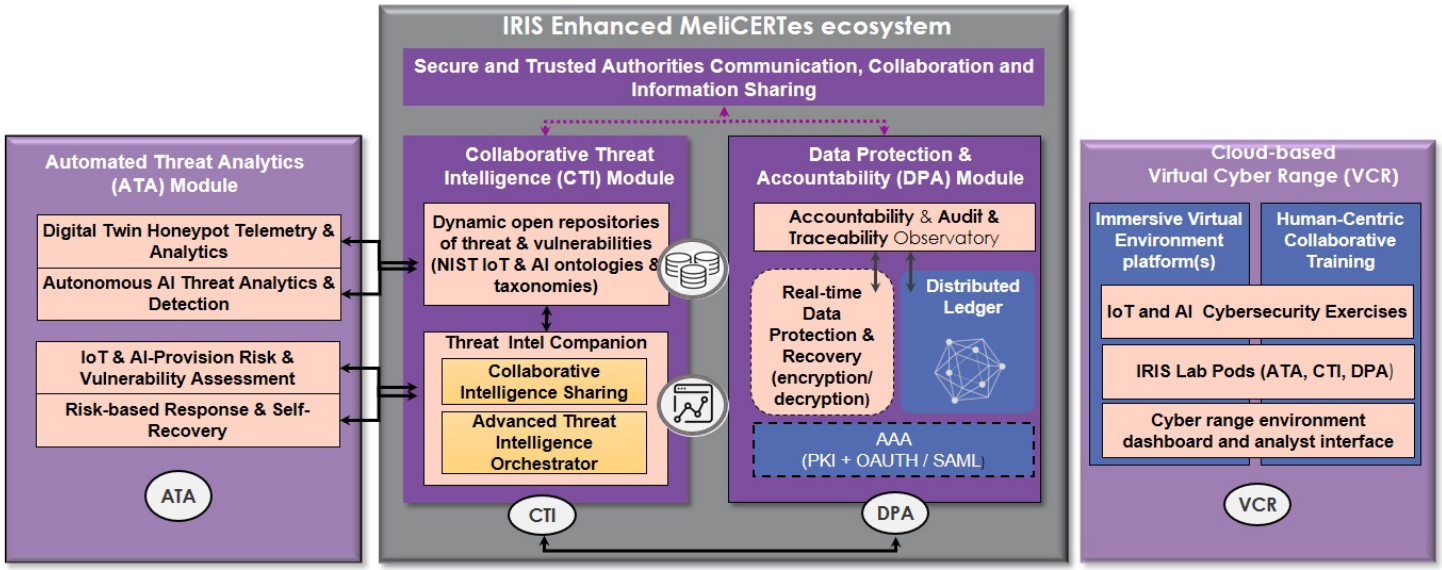
IRIS Architecture



- **Collaborative Threat Intelligence (CTI)** that introduces Analytics Orchestration for supervising coordination between incident response and recovery;
- an **Open Threat Intelligence** interface for disseminating taxonomies of IoT and AI threats;
- an intuitive **Threat Intelligence Companion** that serves as a key human-in-the-loop interface for collaborative incident response and threat intelligence sharing between CERTs/CSIRTs at both the municipal and national level.

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 Architecture



- **Automated Threat Analytics (ATA)** that extends existing intrusion detection tools with a novel threat detection engine for identifying specific IoT and AI attack vectors and includes digital twin honeypots for collecting attack telemetry against end-user systems reliant on these technologies.
- **Virtual Cyber Range (VCR)** for collaborative CERT/CSIRT training exercises based on real-world environment platforms, providing representative adversarial IoT & AI threat intelligence scenarios and hands-on training.

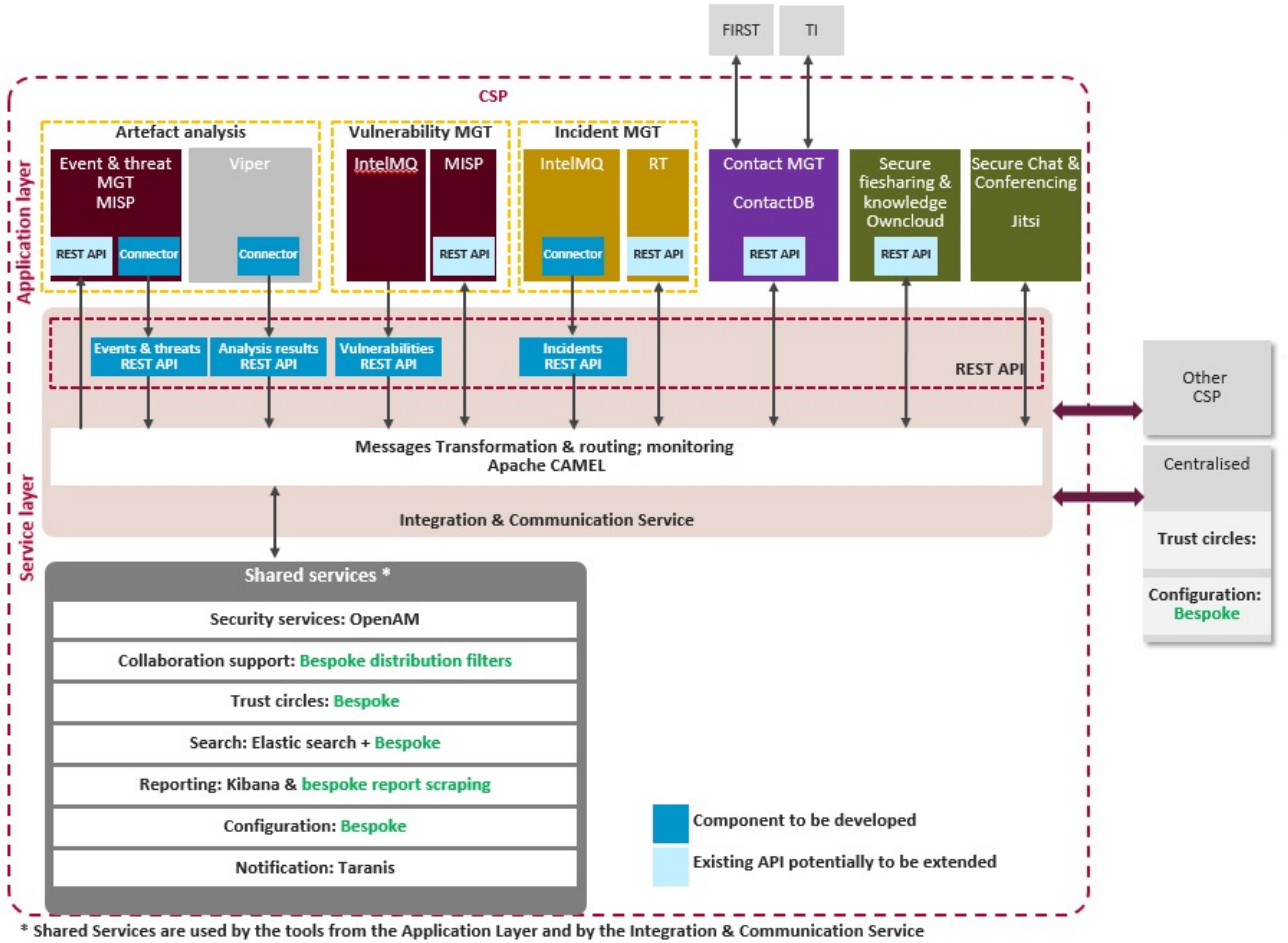
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727. This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

MeliCERTes

- MeliCERTes CSP I tender project:
  - ✓ Tender coordinated by Capgemini and other sub-contractors, including INTRASOFT
  - ✓ Enabling trusted online communication, collaboration and information sharing among CERTs and CSIRTs
  - ✓ https://github.com/melicertes/csp → Open source
  - ✓ MeliCERTes facilitated building of a network for establishing confidence and trust among national CSIRTs and for promoting swift and effective operational cooperation.
  - ✓ CSIRTs participate in MeliCERTes within verified Trust Circles for sharing and collaborating on computer security incidents.
  - ✓ MeliCERTes CSP is an open source modular platform, adopted by ENISA, offering a complete security incident management solution.

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.

MeliCERTes



* Shared Services are used by the tools from the Application Layer and by the Integration & Communication Service

MeliCERTes CSP I is **a modular platform** that offers a **security incident management solution** but also **allows CSIRTs to share information and collaborate with each other within verified Trust Circles**.

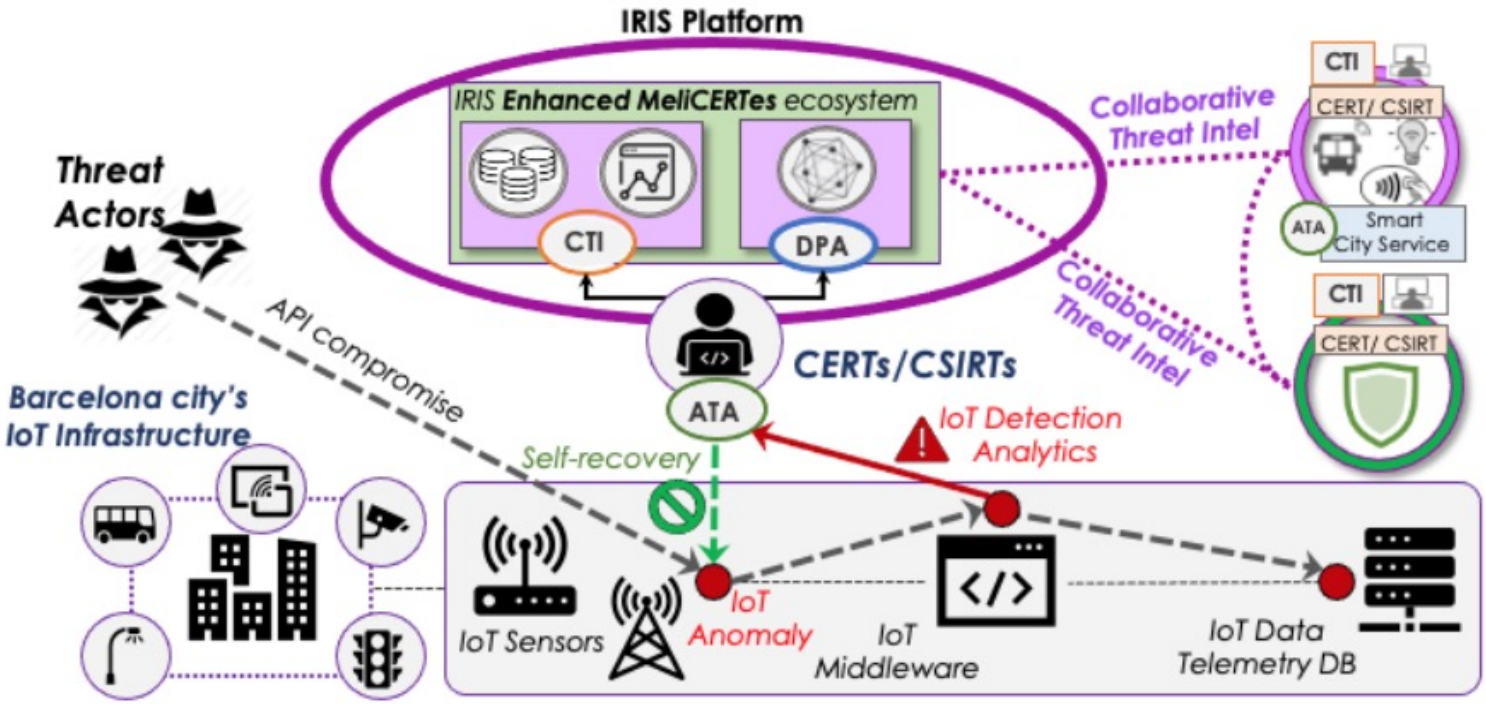
Includes open-source projects:

- **IntelMQ** harvests and manages security vulnerability events from multiple sources.
- **MISP** organises harvested information as events, main module for vulnerability management and information exchange among CSIRTs.
- **Viper** receives events from MISP for critical malware analysis. Analysis results updated back into MISP.
- **OwnCloud** used to securely exchange module files within Trust Circles.
- **Jitsi** is for establishing real-time communications channels for quick response and collaboration.

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.

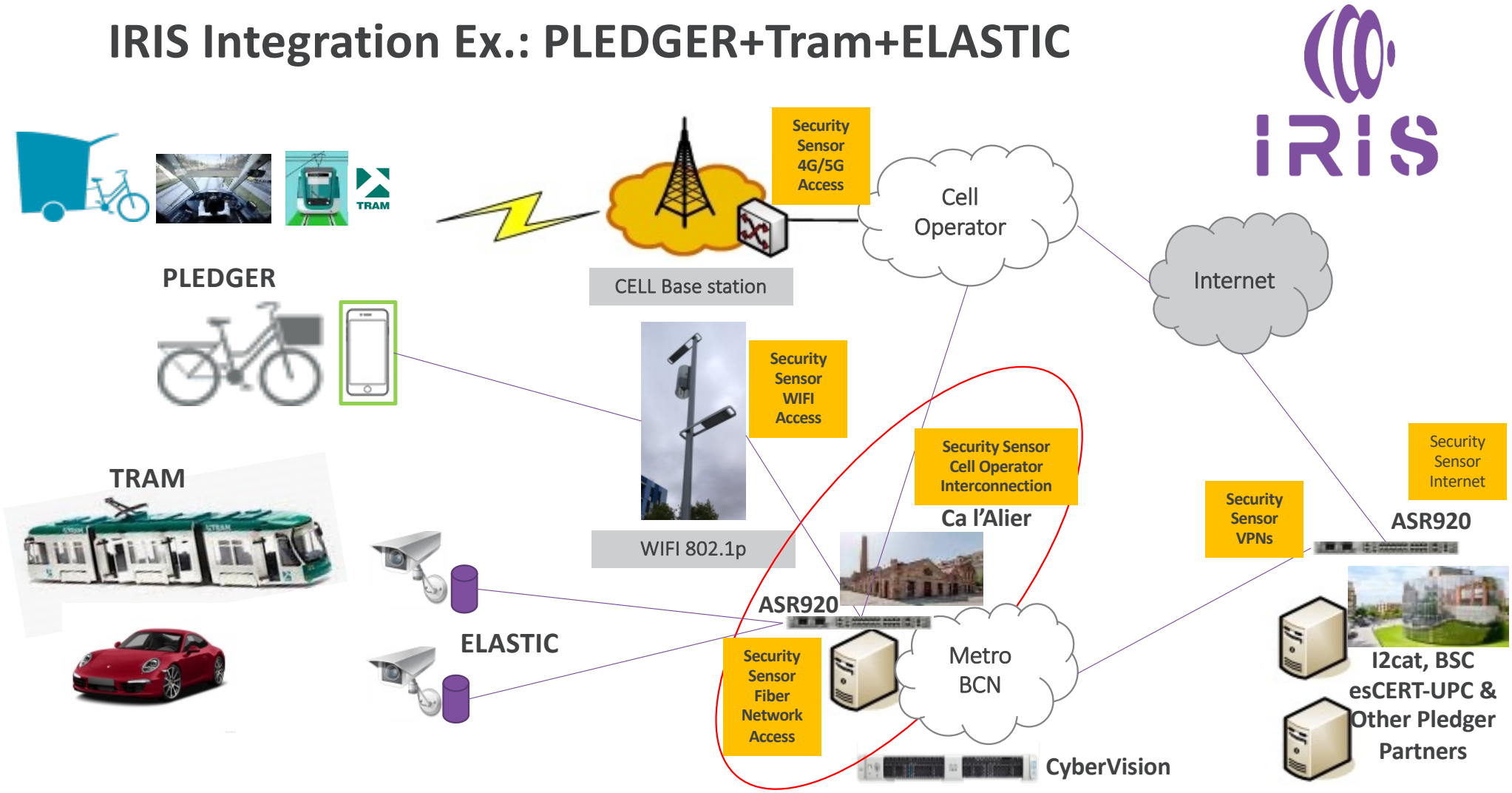
IRIS Pilots: **Pilot Use Case 1**

Securing the smart city's IoT and control systems against confidentiality and integrity breaches (Barcelona, Spain)



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 Integration Ex.: PLEDGER+Tram+ELASTIC



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.

Key capabilities

VISBILITY

- Asset inventory
- Identify relationships between assets
- Generate inventory reports

Benefits
Store all data collected within the CyberVision center database, export or link to other systems (CMDB).

OPERATIONAL INSIGHTS

- History of events & asset modifications
- Highlight changes to asset configurations
- View key events on the control system
- Generate Controller reports

Benefits
Provide situational awareness and empower OT staff to reduce attack surface.

ANOMALY DETECTION

- Automated baselines for asset behaviors
- User created baselines
- Alerts on deviations

Benefits
Identify malicious behaviors.

VULNERABILITY

- Threat Intelligence database
- Identify asset vulnerabilities
- Generate vulnerability reports

Benefits
Provide situational awareness and empower OT staff to reduce attack surface.

INTRUSION DETECTION

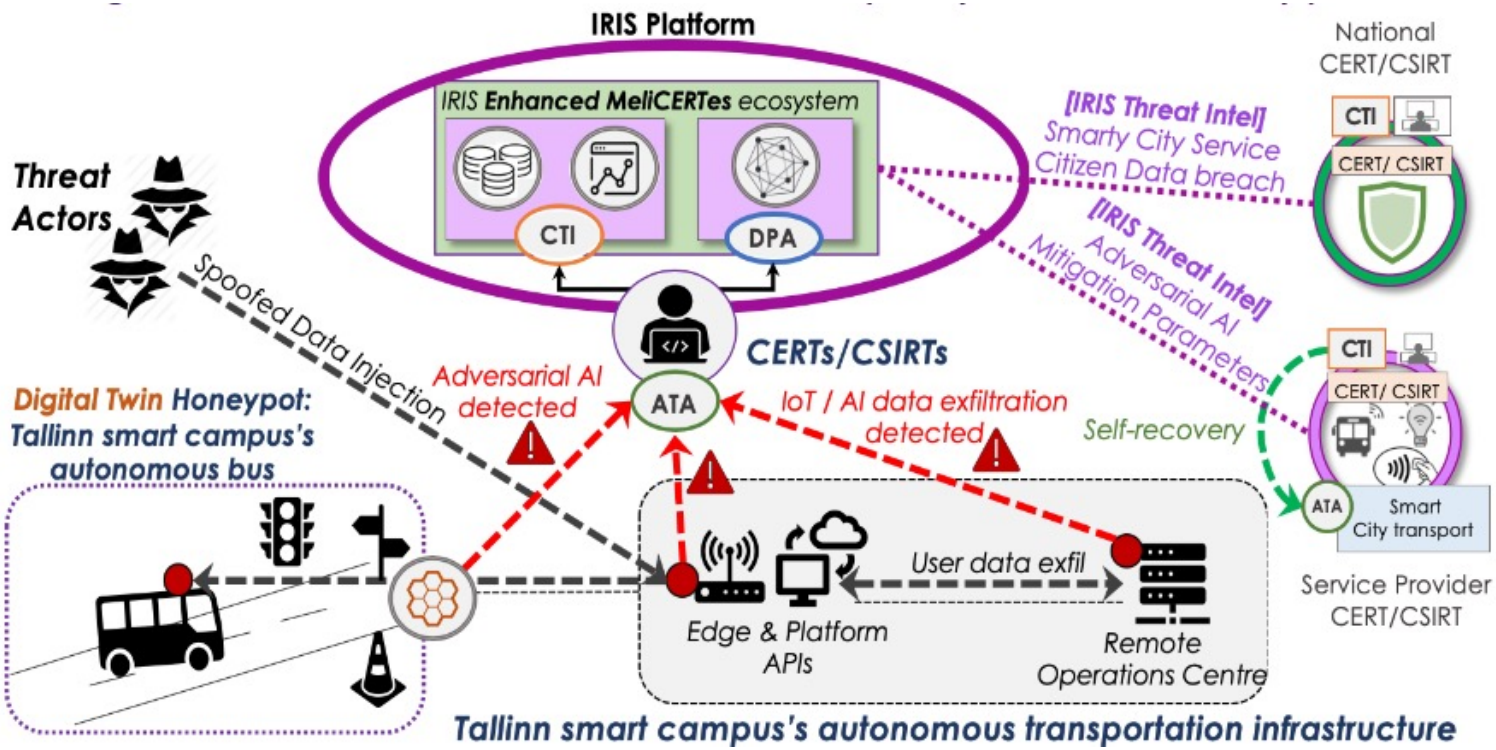
- Snort based Intrusion Detection
- Signatures curated for industrial networks

Benefits
- ❑ Enable and streamline incident response.
- ❑ Accelerate remediation & recovery.

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 Pilots: **Pilot Use Case 2**

Securing AI-enabled infrastructure of autonomous transport systems in a smart city (Tallinn, Estonia)



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 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.

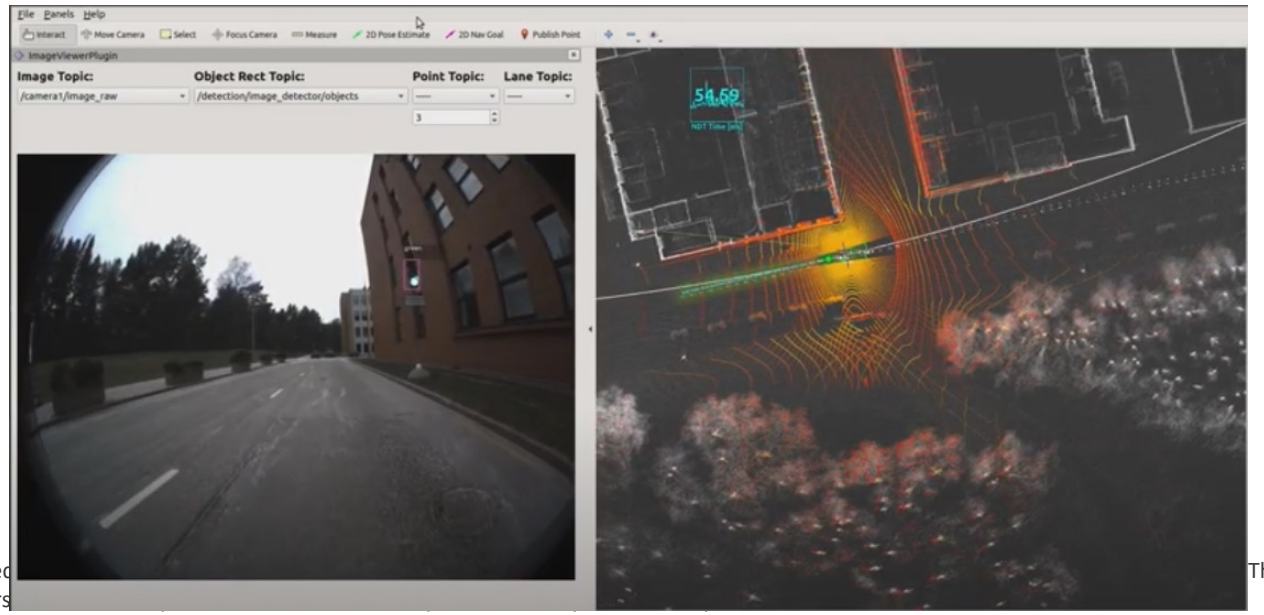
Tallinn Pilot Cyber Threat Scenarios

1) Availability of telemetric data from the AV to the Urban Operating Platform (UoP)
2) 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.

Example

The Autonomous Vehicle (AV) approaches a traffic-light controlled intersection or roadway. The machine vision of the AV focusses on the traffic light and the AV object-detection module detects the traffic light color and makes a driving decision to pass-through or stop.



This project has received
reflects only the authors

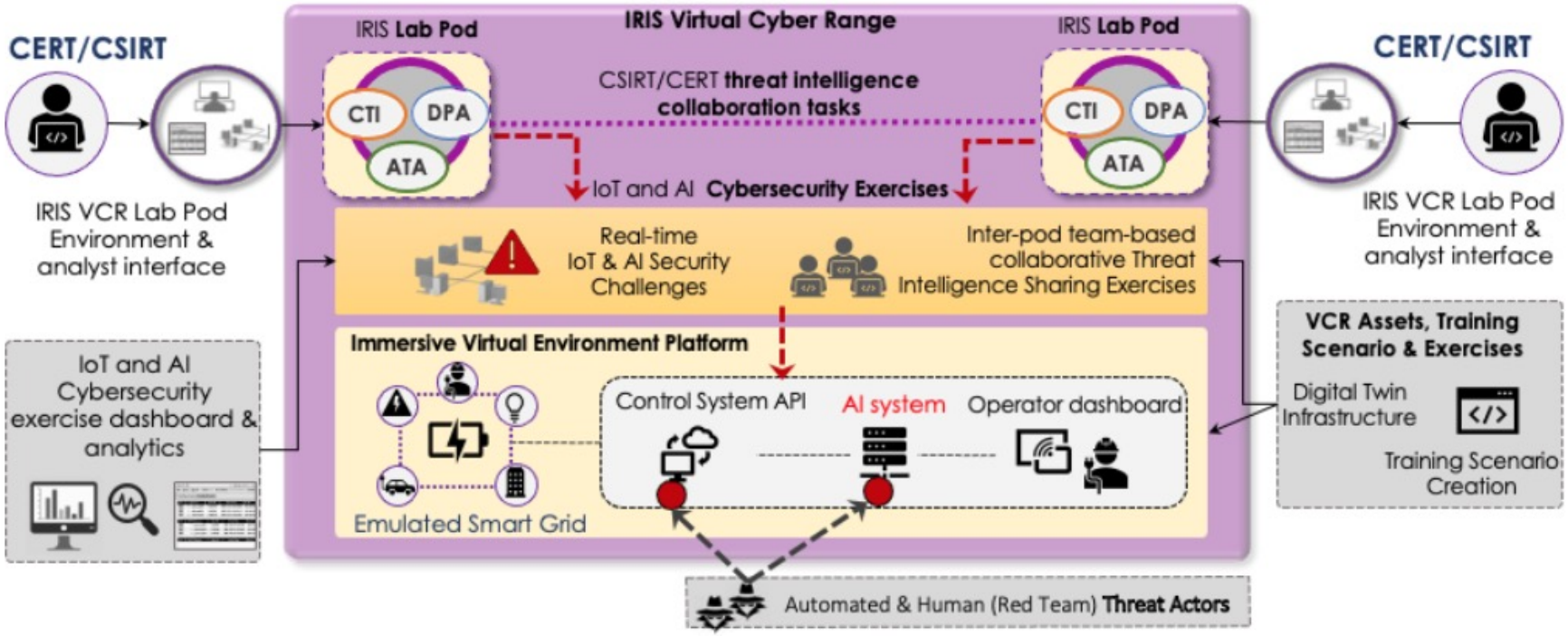
Key capabilities

- Threat Identification
- Self-Healing
- Information Sharing
- Enable Cyber Incident Response from CERTS/CSIRTS

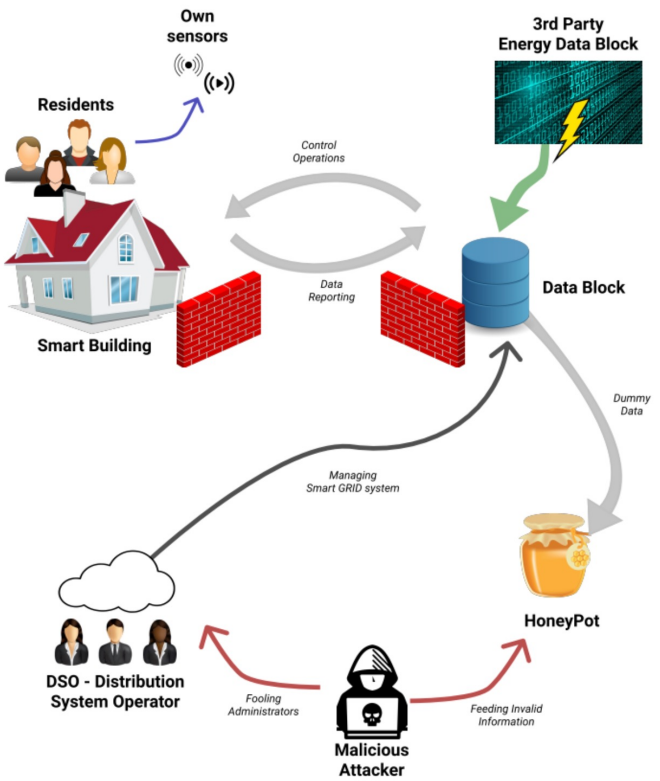
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727. This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

IRIS Pilots: **Pilot Use Case 3**

Effective incident response and threat intelligence collaboration for critical cross-border smart grid threats (Helsinki, Finland and Tallinn, Estonia)



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.



Stakeholders to consider

- **DSO (Distribution system operator)** – Acting as a party who directly reports the energy demand, controlling the building load. E.g., malform the data in the load system, confusing the DSOs and the load control.
- **Building Residents -** Having data wallets of personal data as a React application, allowing users to map own sensors in the system. E.g., security of personal data.
- **CERTs/CSIRTs –** Feedback on handling and forecasting security incidents, complex attacks and propagated vulnerabilities in IoT and AI-driven ICT systems.

Cross-Border Smart Grids – Helsinki - Talin Pilot

- Helsinki city **Smart grid** - enabling real time smart metering, electric vehicles network and new storage solutions for electricity.
- Provision of **load control functions** that the distribution system operator (DSO) can use in situations where the production has reached its peak.
- **Urban Data Platform**, a smart city data platform based on Apache Kafka, Apache Spark, Microsoft Azure-
- **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.

Cybersecurity Challenge

- Effective incident response and threat intelligence collaboration for critical **cross-border** smart grid threats
- Focus on protecting the customer facing components of the smart grid against threats to control functions defined for the demand control.

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.

Nelson Escravana

2021-12-10

iris-h2020.eu

IRIS H2020 Project

iris_h2020

Nelson Escravana

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.