Artificial Intelligence Threat Reporting & Incidence report system

IRIS General Presentation

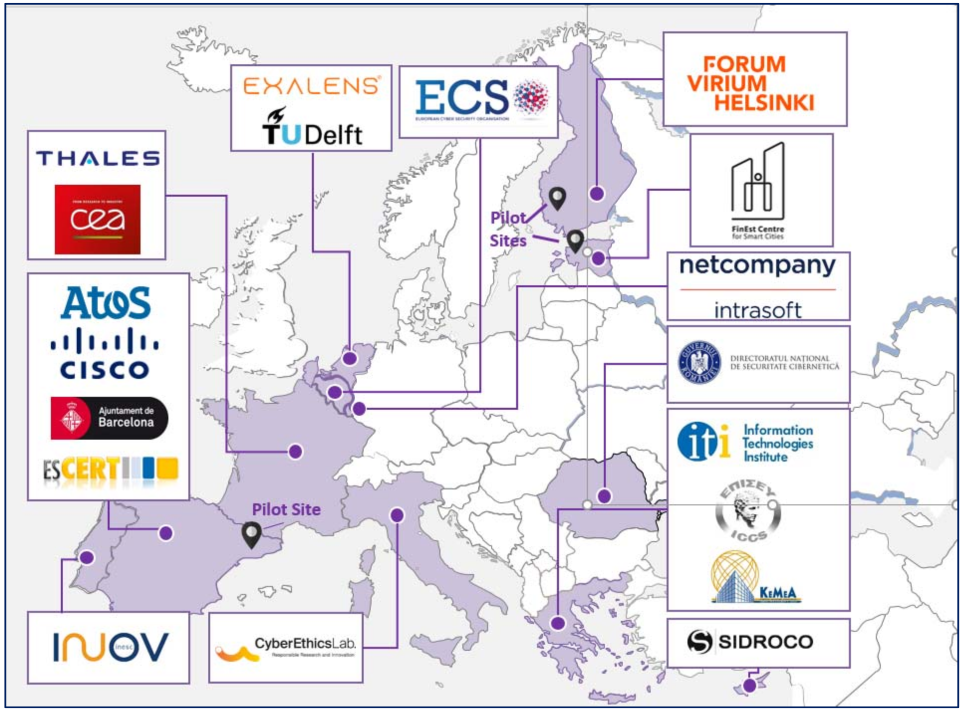
Pantelis Kanellopoulos, ICCS

ELECTRON International Event

- 6th December 2022 -

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.

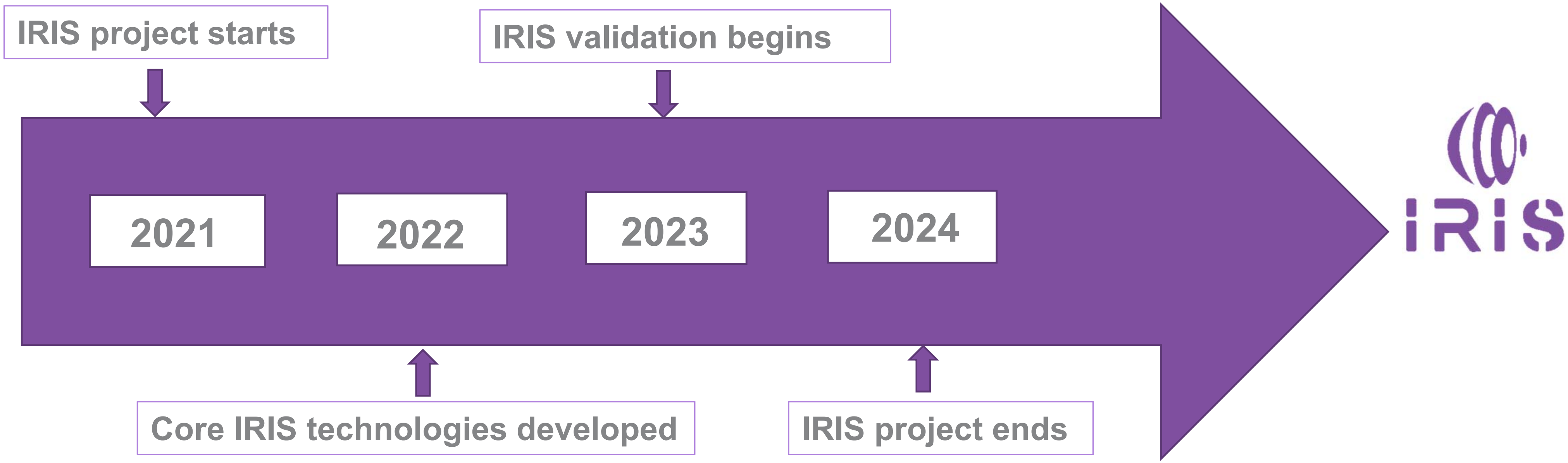
IRIS Vision

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.

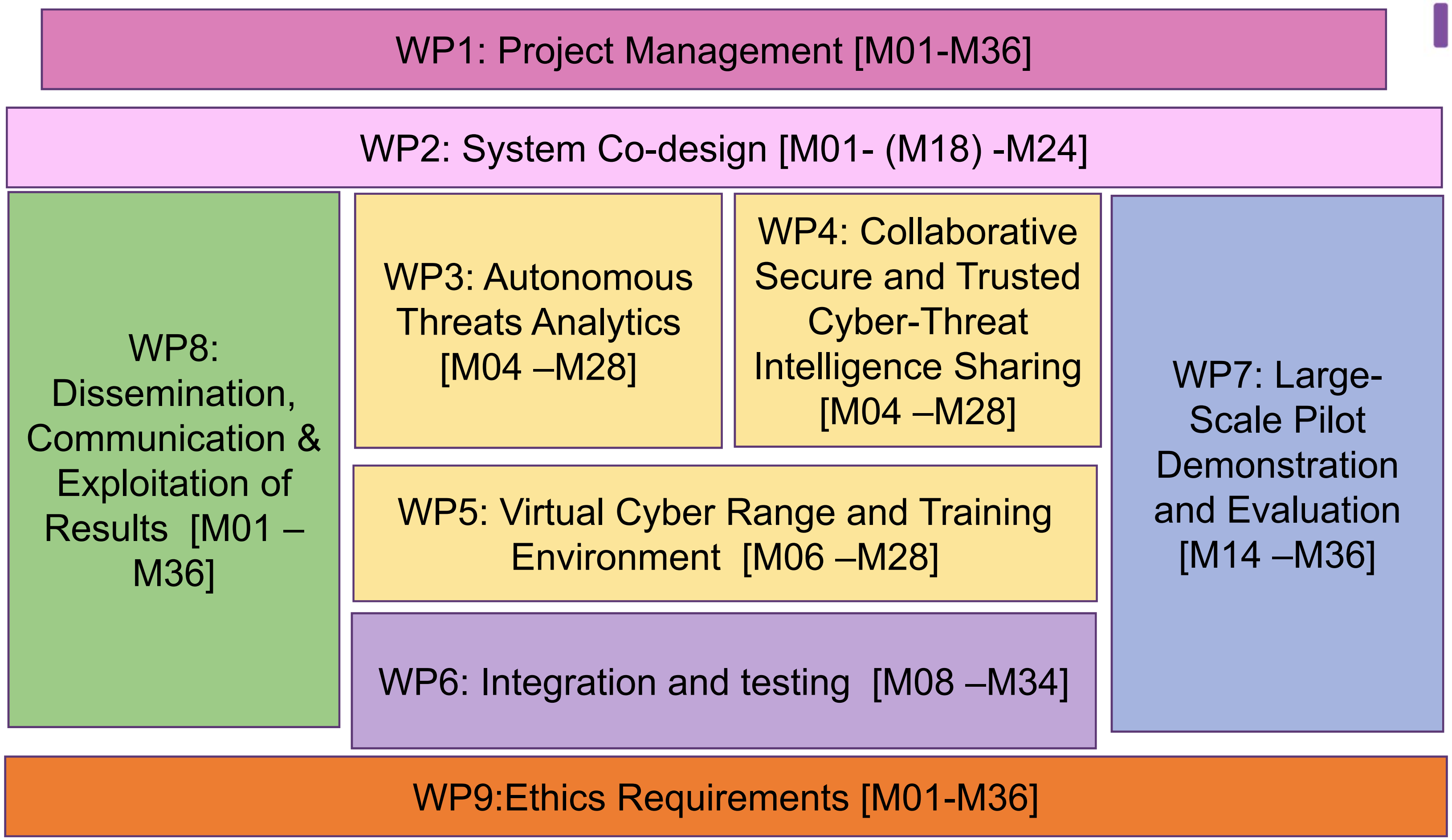
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

IRIS 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 Work Packages



WP1: Project Management [M01-M36]

WP2: System Co-design [M01- (M18) -M24]

WP8: Dissemination, Communication & Exploitation of Results [M01 –M36]

WP3: Autonomous Threats Analytics [M04 –M28]

WP4: Collaborative Secure and Trusted Cyber-Threat Intelligence Sharing [M04 –M28]

WP5: Virtual Cyber Range and Training Environment [M06 –M28]

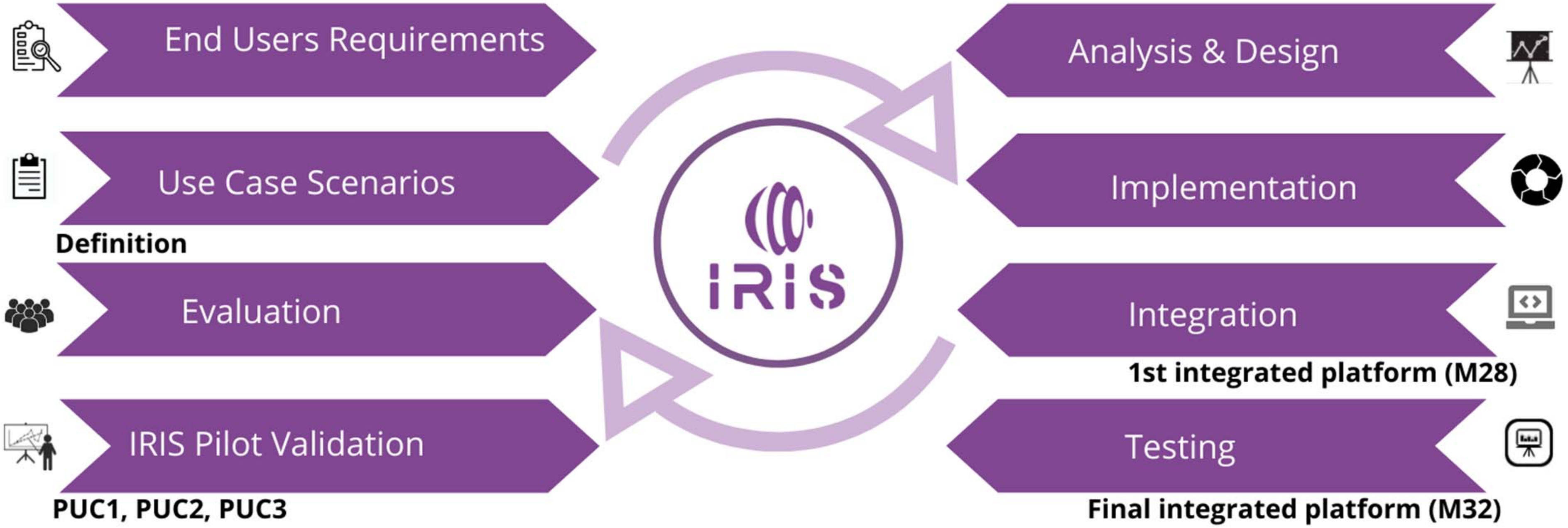
WP6: Integration and testing [M08 –M34]

WP7: Large-Scale Pilot Demonstration and Evaluation [M14 –M36]

WP9:Ethics Requirements [M01-M36]

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 Objectives

- To **identify** the user, technical and business requirements and **design** the architecture of an AI threat reporting and incident response system to support the operations of CERTs/CSIRTs towards minimizing the impact caused by cybersecurity and privacy risks in IoT platforms and AI-provisions
- To **analyse** the relevant ethics principles and legal framework on privacy concerns, as well as to understand relevant stakeholders' behaviour to identify the main legal, ethics and social enablers for the IRIS solution
- To **develop** a collaborative threat intelligence and information sharing toolkit that allows ICT stakeholders and European CERTs/CSIRTs to create and seamlessly share context-rich information about cyber threats targeting IoT and AI-driven 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

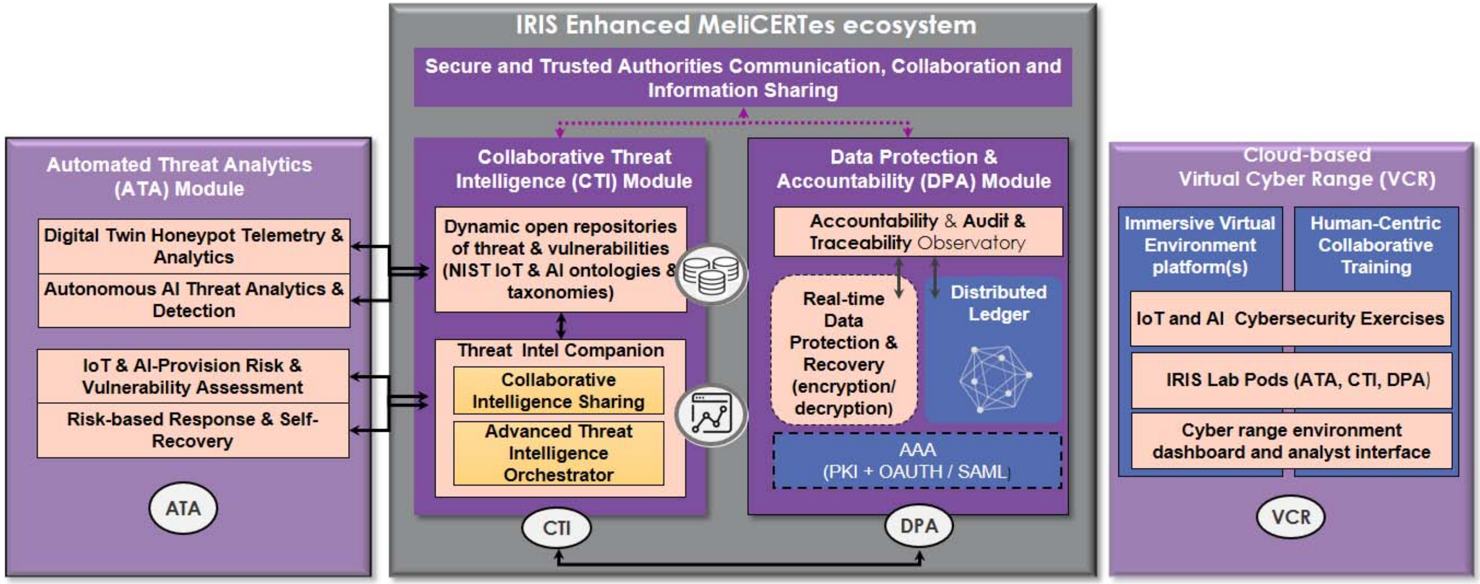
◎ To **design and implement**:

- ➢ an automated threat analytics framework capable of detecting and responding to cyber threats targeting IoT and AI-driven ICT systems, while exhibiting advanced recovery capabilities
- ➢ a virtual cyber range platform for training cybersecurity professionals to fight against adversarial AI and machine learning attack
- ➢ a data protection and accountability module to establish trust and enable the protection of data necessary 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 to the research, academic, and CERT/CSIRT community, efficient exploitation and business planning of the IRIS concepts and solutions to the market, and contribution of specific project results to relevant standardisation 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.

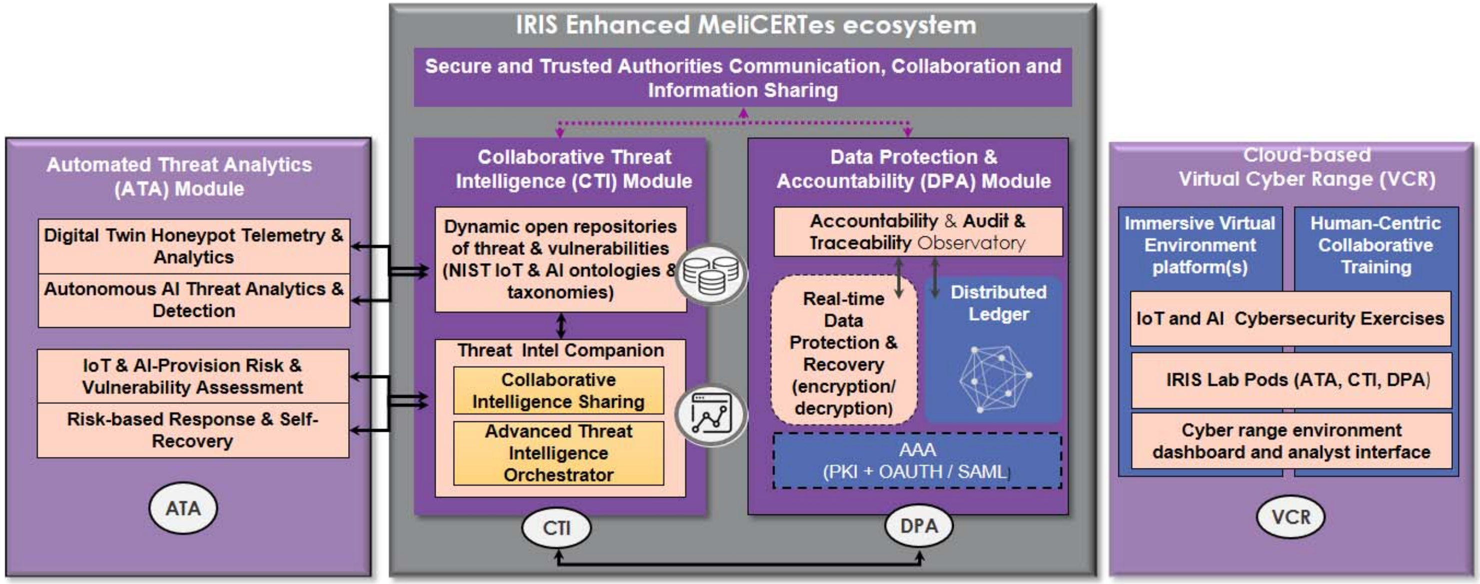
IRIS Architecture


IRIS Enhanced MeliCERTes ecosystem
Secure and Trusted Authorities Communication, Collaboration and Information Sharing
Automated Threat Analytics (ATA) Module
Digital Twin Honeypot Telemetry & Analytics
Autonomous AI Threat Analytics & Detection
IoT & AI-Provision Risk & Vulnerability Assessment
Risk-based Response & Self-Recovery
ATA
Collaborative Threat Intelligence (CTI) Module
Dynamic open repositories of threat & vulnerabilities (NIST IoT & AI ontologies & taxonomies)
Threat Intel Companion
Collaborative Intelligence Sharing
Advanced Threat Intelligence Orchestrator
CTI
Data Protection & Accountability (DPA) Module
Accountability & Audit & Traceability Observatory
Real-time Data Protection & Recovery (encryption/ decryption)
Distributed Ledger
AAA
(PKI + OAUTH / SAML)
DPA
Cloud-based Virtual Cyber Range (VCR)
Immersive Virtual Environment platform(s)
Human-Centric Collaborative Training
IoT and AI Cybersecurity Exercises
IRIS Lab Pods (ATA, CTI, DPA)
Cyber range environment dashboard and analyst interface
VCR

- ❑ **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

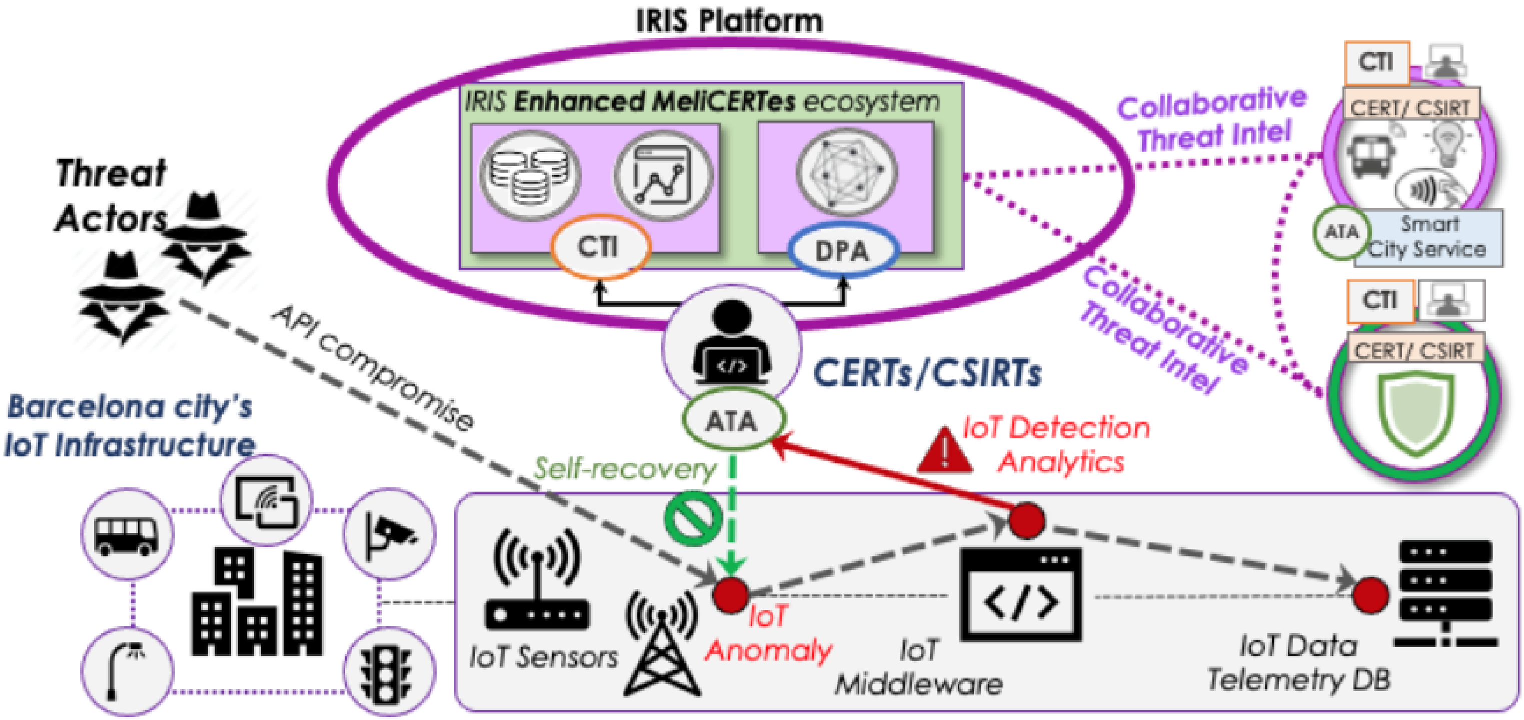

IRIS Enhanced MeliCERTes ecosystem
Secure and Trusted Authorities Communication, Collaboration and Information Sharing
Automated Threat Analytics (ATA) Module
Digital Twin Honeypot Telemetry & Analytics
Autonomous AI Threat Analytics & Detection
IoT & AI-Provision Risk & Vulnerability Assessment
Risk-based Response & Self-Recovery
ATA
Collaborative Threat Intelligence (CTI) Module
Dynamic open repositories of threat & vulnerabilities (NIST IoT & AI ontologies & taxonomies)
Threat Intel Companion
Collaborative Intelligence Sharing
Advanced Threat Intelligence Orchestrator
CTI
Data Protection & Accountability (DPA) Module
Accountability & Audit & Traceability Observatory
Real-time Data Protection & Recovery (encryption/ decryption)
Distributed Ledger
AAA
(PKI + OAUTH / SAML)
DPA
Cloud-based Virtual Cyber Range (VCR)
Immersive Virtual Environment platform(s)
Human-Centric Collaborative Training
IoT and AI Cybersecurity Exercises
IRIS Lab Pods (ATA, CTI, DPA)
Cyber range environment dashboard and analyst interface
VCR

- ❑ **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.

IRIS Pilots: **Pilot Use Case 1**

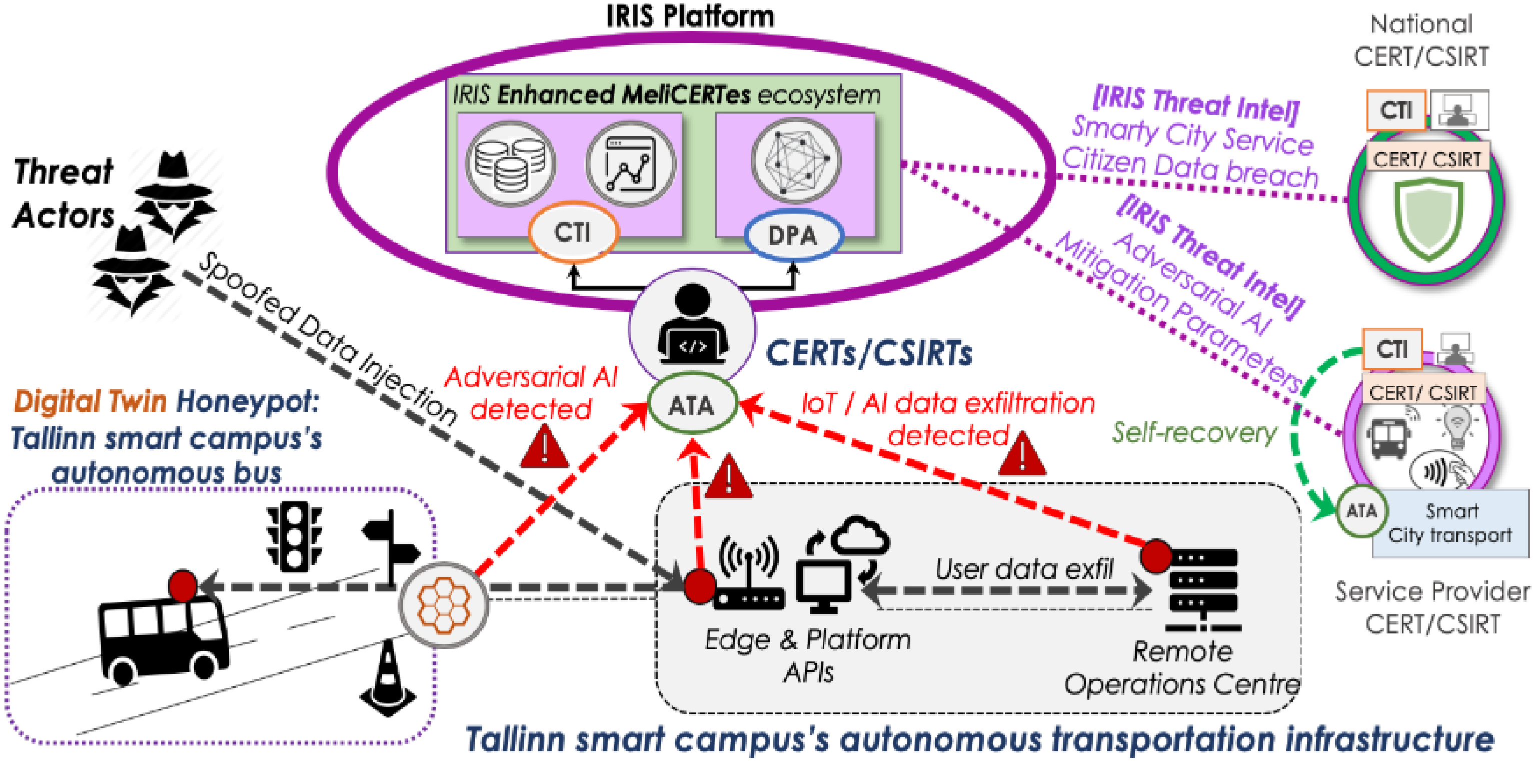
Securing the smart city's IoT and control systems against confidentiality and integrity breaches (Barcelona, Spain)



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 Pilots: **Pilot Use Case 2**

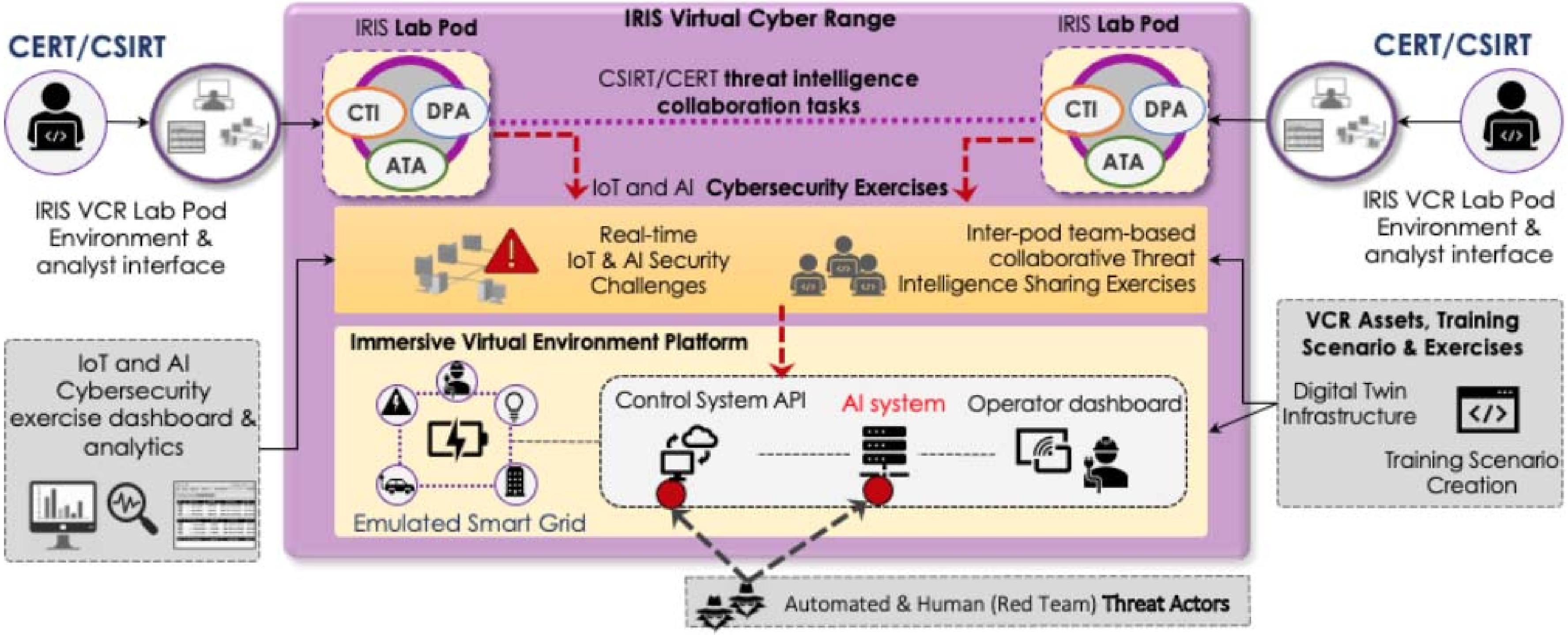
Securing AI-enabled infrastructure of autonomous transport systems in a smart city (Tallinn, Estonia)



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.

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)


CERT/CSIRT
IRIS VCR Lab Pod Environment & analyst interface
IoT and AI Cybersecurity exercise dashboard & analytics
IRIS Lab Pod
IRIS Virtual Cyber Range
IRIS Lab Pod
CTI
DPA
ATA
CSIRT/CERT threat intelligence collaboration tasks
CTI
DPA
ATA
IoT and AI Cybersecurity Exercises
Real-time IoT & AI Security Challenges
Inter-pod team-based collaborative Threat Intelligence Sharing Exercises
Immersive Virtual Environment Platform
Emulated Smart Grid
Control System API
AI system
Operator dashboard
Automated & Human (Red Team) Threat Actors
CERT/CSIRT
IRIS VCR Lab Pod Environment & analyst interface
VCR Assets, Training Scenario & Exercises
Digital Twin Infrastructure
Training Scenario Creation

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.

Join IRIS Stakeholder Community

❑ Why joining the IRIS Community?

- ✓ Insights into challenges and solutions on **how to share threat information**, **how to conduct effective** threat response, **how to improve threat reporting** to CERTs/CSIRTs
- ✓ Invitation to participate in **focus groups, evaluation sessions and other project events** such as the upcoming **IRIS 1st Stakeholder and Industrial Workshop** that the project will
- ✓ Access to the **IRIS Community repository**, with relevant documentation

❑ Who can join? ,

- ✓ CERT / CSIST professionals
- ✓ CISOs, cybersecurity managers, and other cybersecurity professionals
- ✓ Cybersecurity service providers (SOC, tools, services, information sharing)

❑ How to join?

Just **send an email** to with **name/email/role of candidates**, to iris-community@iris-h2020.eu

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.

Upcoming project event:
IRIS 1st Stakeholders and Industrial Workshop

The **1st Stakeholders and Industrial Workshop** will present the **most mature results** of the project to **industrial stakeholders.**

🔊**Topic: Threat reporting – What's the IRIS offer?**

□ **Date: End February 2023** *(date & Agenda will be announced soon)*

💻 **Format: Online**

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!

Pantelis Kanellopoulos, ICCS

ELECTRON International Event

- 6th December 2022 -

iris-h2020.eu

IRIS H2020 Project

iris_h2020

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.