Artificial Intelligence Threat Reporting & Incidence report system

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

A collaborative CERT/CSIRT platform to combat cyber-threats in **IoT and AI-driven systems**

Nelson Escravana (INOV)

16-17/10/2023

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** systems, **novel and complex threats are introduced**.

Architecture and behaviour of emerging IoT and AI technologies are **not currently well understood** by security practitioners, such as CERTs and CSIRTs.

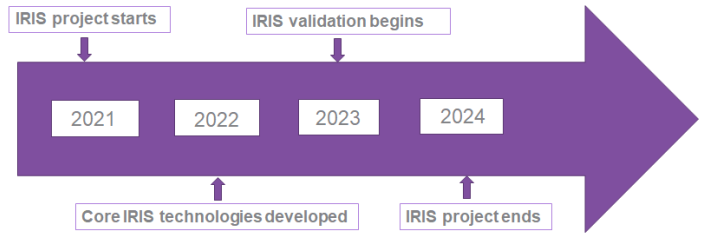
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727. This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

IRIS 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 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.

Project at a Glance



Call Identifier: 2020-SU-DS-2020

Topic: SU-DS02-2020 Intelligent security and privacy management (IA)

EC Funding: 4 918 790.00 EUR

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

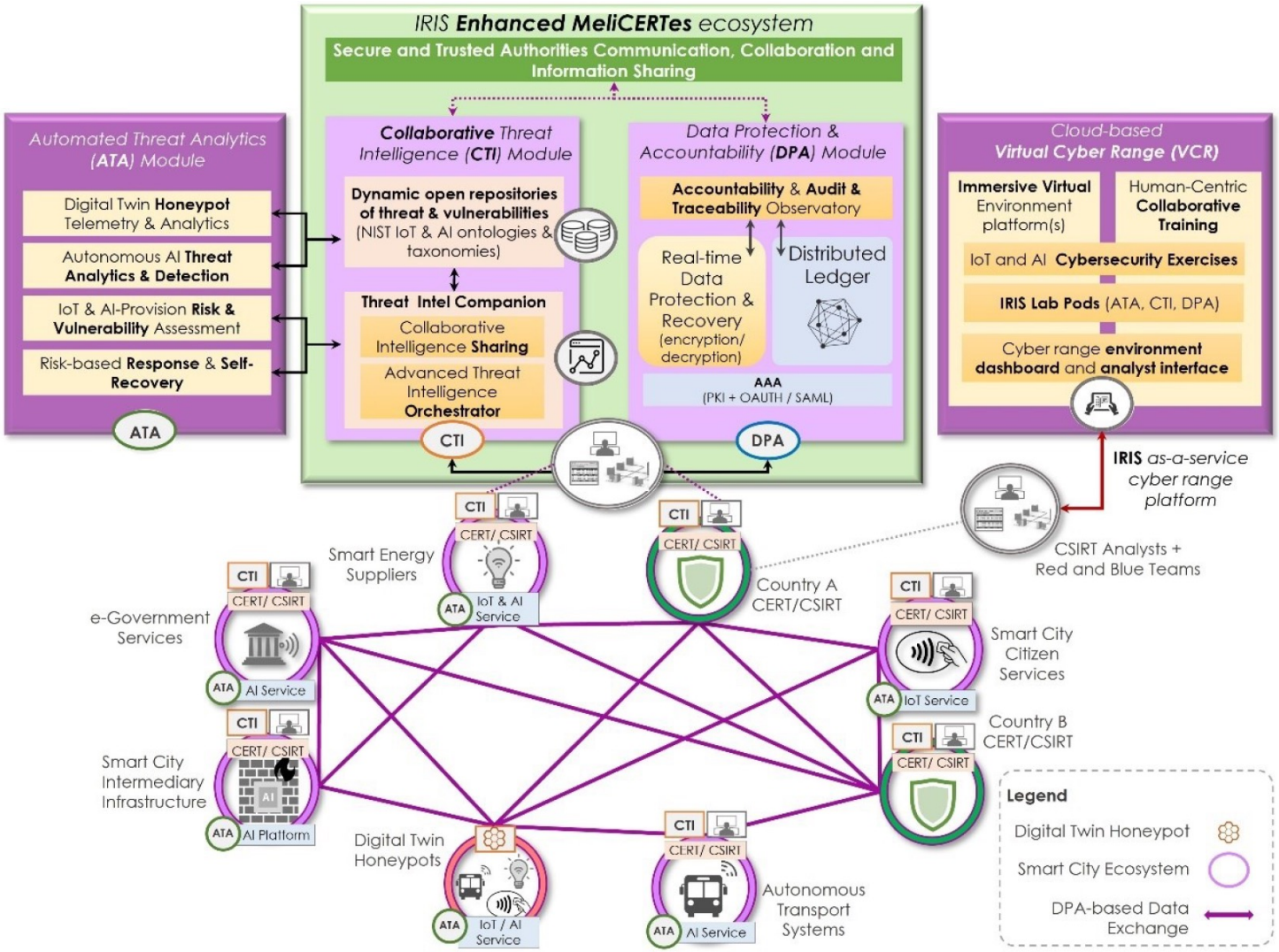
Join us: Diris-h2020

IRIS H2020 Project

Consortium

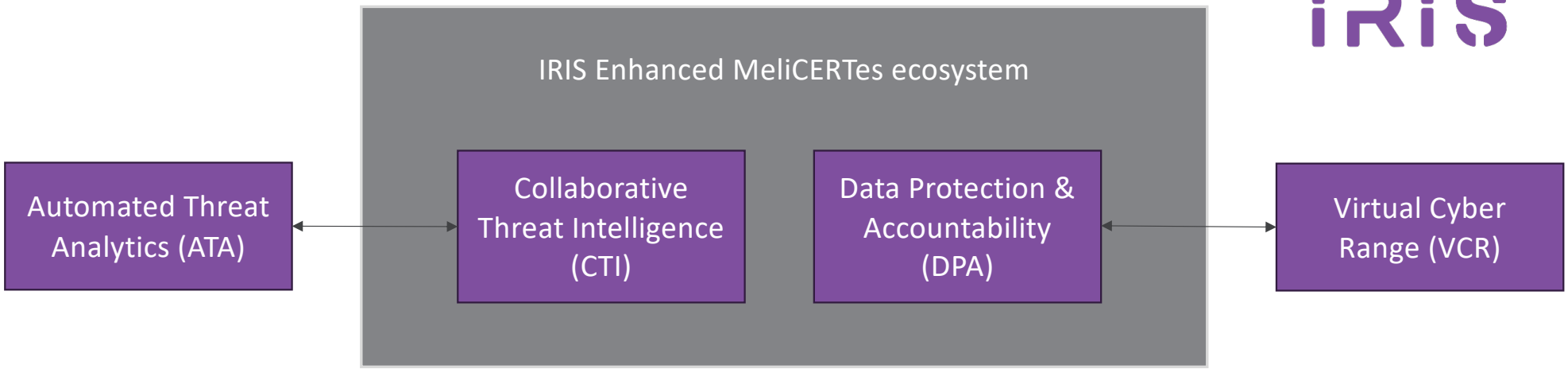
- **6 Public organizations**
- **3 SMEs**
- **4 Large ICT industries**
- **6 Research institutions & Universities**

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.



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 Tools	Description
BINSEC and Vulnerability Discovery Manager	Detection and analysis of vulnerabilities
Response & Recovery	Optimized response recommendations and actions
Nightwatch	IoT threat telemetry
SIVI	Detection and analysis of real-time threats
SiHoneyPots	Analysis and telemetry

IRIS Tools	Description
Threat Intel Sharing & Storage	Threat and Vulnerability repository and data sharing tool
Threat Intel Orchestrator	Orchestration
EME	Data Visualization
DPA	Auditing and accountability

IRIS Tools	Description
VCR	IRIS emulated infrastructure and education platform for CERT/CSIRT teams
CyberTraP	Cybersecurity training exercises

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.

PUC #1 Barcelona **Securing the smart city's IoT and control systems against confidentiality & integrity breaches**

Test and validate IRIS platform in the city of Barcelona:

- **Leverage existing systems, IoT devices** (e.g., lampposts, parking, traffic, ambient sensors, RF sensors) and **wireless access points** (SmallCells, LTE, Wi-Fi) with virtualization capabilities.
- Ensure that the IRIS platform will be able to **successfully detect possible malicious traffic** to the IoT systems and their data telemetry, which may lead to their compromise.
- Test and validate IRIS ability to **report efficiently and effectively** the impact of possible breaches in the IoT and control 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.

PUC #2 Tallinn **Securing AI-enabled infrastructure of autonomous transport systems in a smart city**

Test and validate IRIS platform in the city of Tallinn:

- PUC2 relies on the **fully autonomous buses system** for public transportation in the city of Tallinn.
- The autonomy relies on the **absence of human driver** and the **constant monitoring** of the buses by a central remote operation center
- Validate IRIS platform capabilities to **identify, self-recover and share 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.

PUC #3 Helsinki + Tallinn **Effective incident response and threat intelligence collaboration for critical cross-border smart grid threats**

Test and validate IRIS platform in the cities of Tallinn and Helsinki:

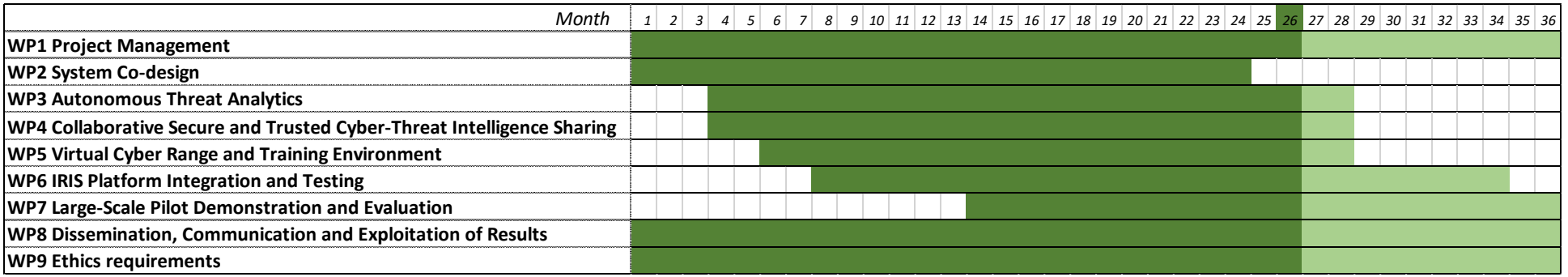
1. PUC3 involves **cross-border threats in the smart grid energy sector**, using two smart grid APIs, from Kalasatama/Helsinki and from the city of Tallinn
2. The objective is to train CERT/CSIRT to **coordinate threat mitigation** to network connected components of the smart grid
3. Validate the capabilities of IRIS platform in mitigating cyber threats **that target cross border attacks** against energy smart grids and assess the **virtual cyber range capabilities of the IRIS platform** to help train CERT/CSIRT personnel and energy grid cyber security stakeholders

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.

Current status

- Finished:
  - Requirements and Architecture
- Currently:
  - Finalizing development and integration of all components
  - Preparing the pilots for the 3 PUCs (2024 1Q)
- Next:
  - Refine technologies
  - Second round of pilots (2024 2Q)

We are here



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!

Nelson Escravana

(INOV – Project Coordinator)

coordinator@iris-h2020.eu

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.