Artificial Intelligence Threat Reporting & Incidence report system

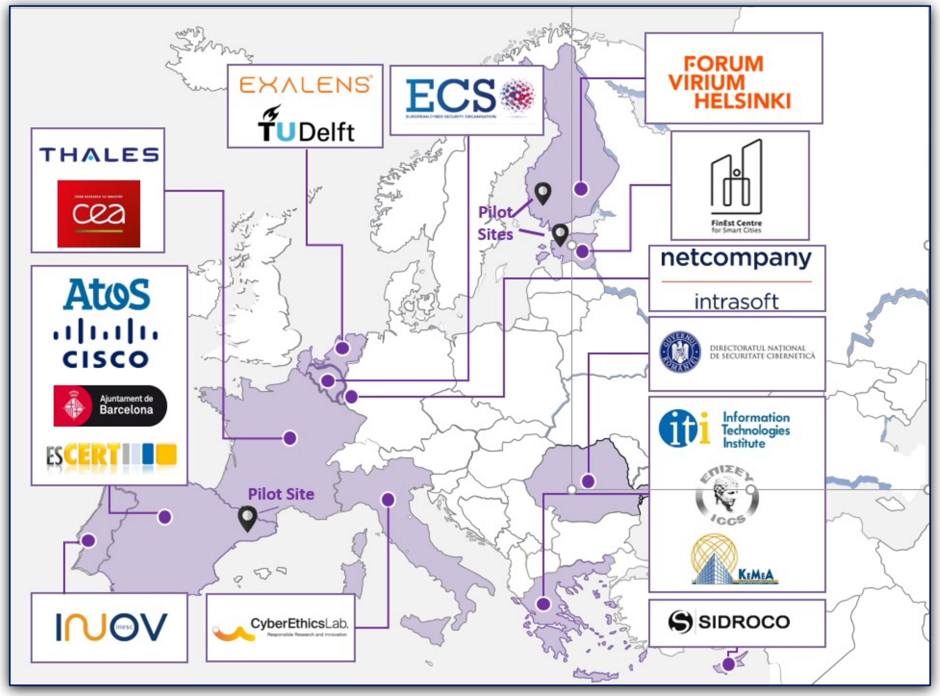
IRIS Short Presentation

Nelson Escravana, INOV

2022-10-28

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

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

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.

IRIS Motivation & Vision

Emerging IoT and AI technologies, whose architecture and behaviour are **not currently well understood** by security practitioners, such as CERTs and CSIRTs.

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

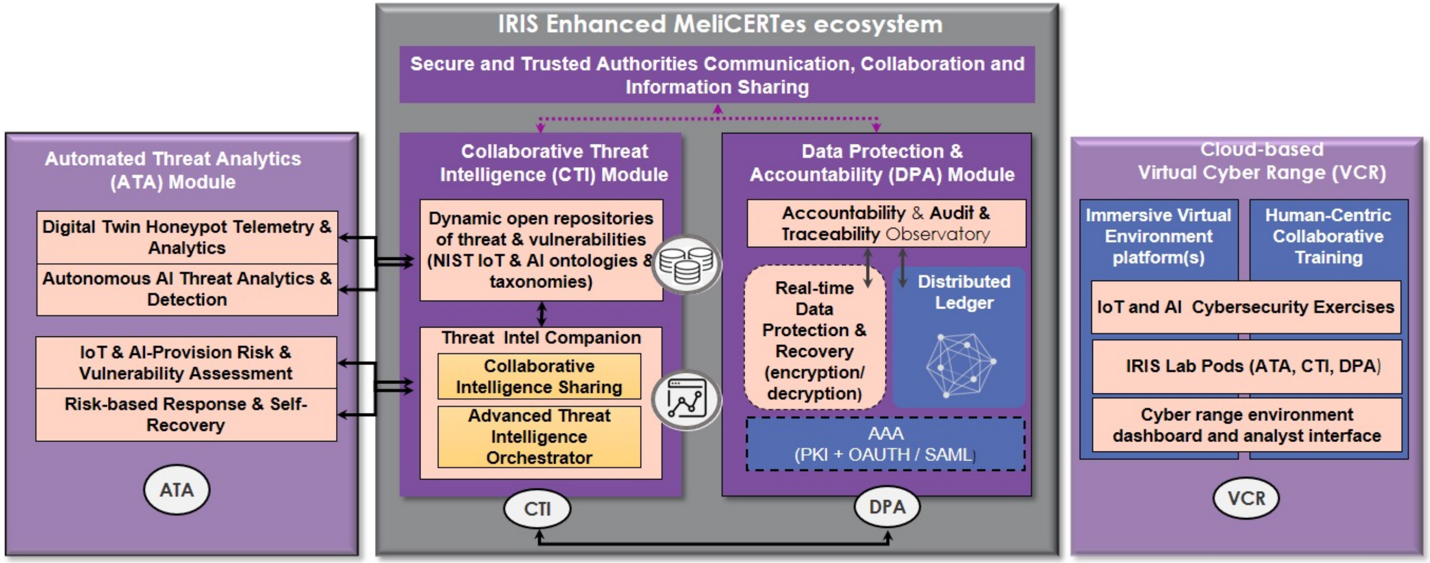
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727. This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

IRIS key 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, **within** the relevant ethics principles and legal framework on privacy concerns.
- ◎ 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.
- ◎ To **design, implement, demonstrate** and **validate** IRIS approach

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;

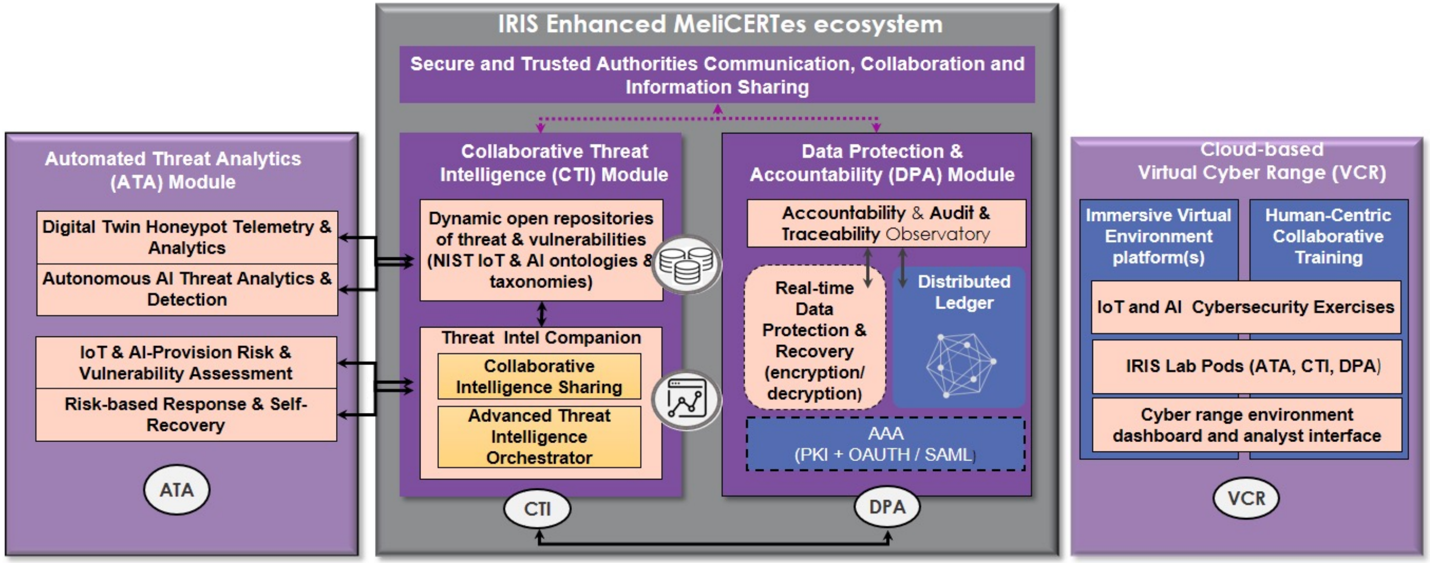
❖ an **Open Threat Intelligence** interface for disseminating taxonomies of IoT and AI threats;

❖ 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

❖ a Data Protection & Accountability (**DPA**) module

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

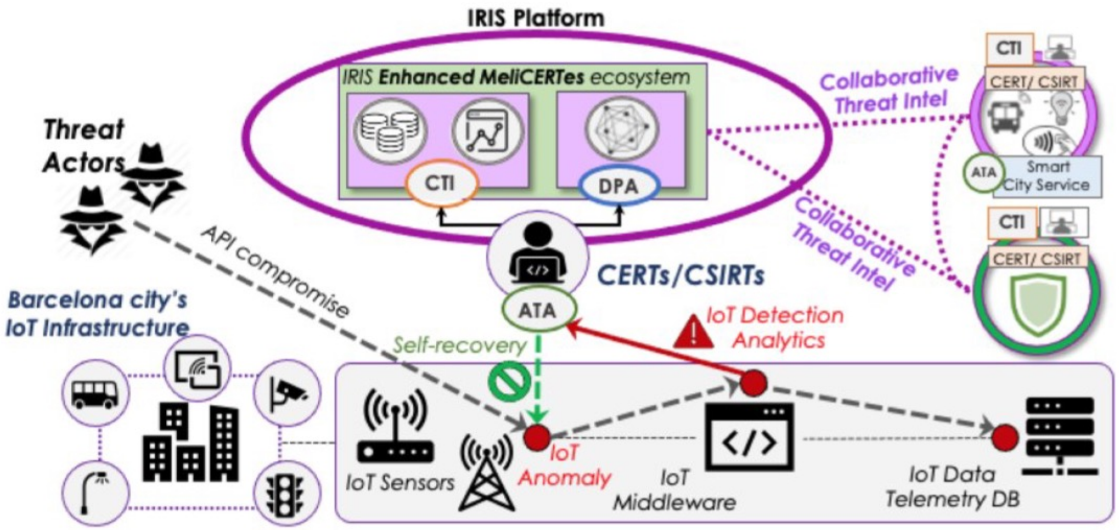


IRIS Enhanced MeliCERTes ecosystem
Secure and Trusted Authorities Communication, Collaboration and Information Sharing
Automated Threat Analytics (ATA) Module
Digital Twin Honeypot Telemetry & Analytics
Autonomous AI Threat Analytics & Detection
IoT & AI-Provision Risk & Vulnerability Assessment
Risk-based 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.

Pilot 1. Barcelona City. Tramway Monitoring



Use Case focused on **ATA** and **CTI** modules

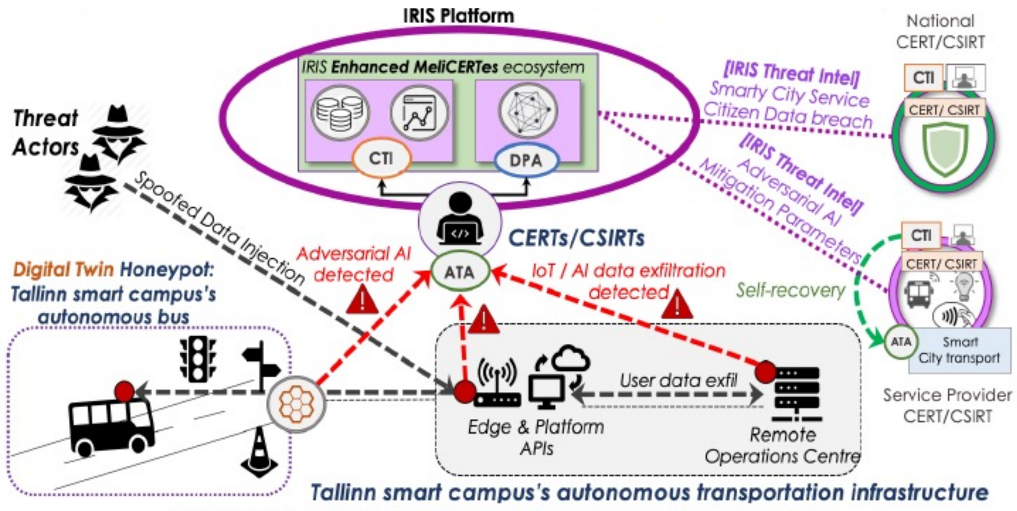
- Attack analysis (T3.1, T3.2)
- Mitigation (T3.3, T4.3)
- Sharing and reporting
- Threat Intelligence

Involved actors

- Human and non-technical actors:
  - o Tramways
  - o Pedestrians
  - o Bike users
- Entities:
  - o Transport Operators
  - o CERTs
- Equipment:
  - o Cyber Vision Sensors
  - o Cyber Vision Center

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.

Pilot 2. Tallinn City. Autonomous Transportation System



IRIS Platform
IRIS Enhanced MeliCERTes ecosystem
CTI
DPA
Threat Actors
Spoofed Data Injection
Digital Twin Honeypot: Tallinn smart campus's autonomous bus
CERTs/CSIRTs
Adversarial AI detected
ATA
IoT / AI data exfiltration detected
[IRIS Threat Intel] Smarty City Service Citizen Data breach
[IRIS Threat Intel] Adversarial AI Mitigation Parameters
National CERT/CSIRT
CTI
CERT/ CSIRT
CTI
CERT/ CSIRT
Self-recovery
ATA
Smart City transport
Service Provider CERT/CSIRT
User data exfil
Edge & Platform APIs
Remote Operations Centre
Tallinn smart campus's autonomous transportation infrastructure

Use Case focused on the **ATA** module

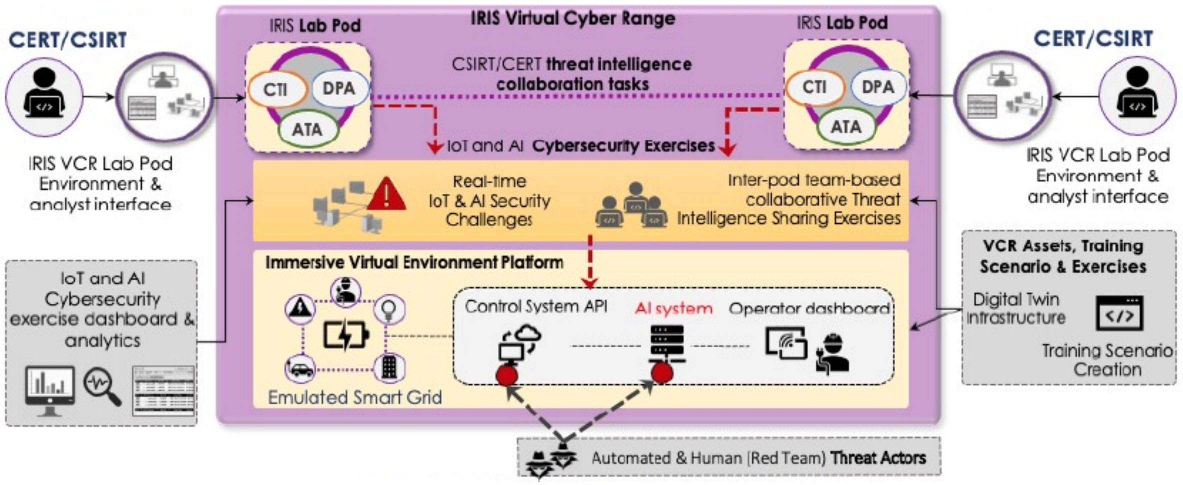
- Attack analysis
- Anomaly detection
- Incident response
- ATA Digital Twin honeypot
- Threat analytics for advanced IoT and AI attacks
- Self-recovery in real time

Involved actors

- Human and non-technical actors:
  - o Autonomous transportation system
  - o Smart City Passengers
  - o Malicious threat actor
- Entities:
  - o Smart City Transport Provider
  - o CERTs
- Equipment:
  - o Digital Twin Honeypot
  - o Urban 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.

Pilot 3. Helsinki City. Smart grid System


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
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

Use Case focused on the **VCR** module

- Attack detection
- Impact mitigation
- Educate CSIRT/CERT on incident response

Involved actors

- Human and non-technical actors:
  - o DSO
  - o Building residents
  - o Malicious threat actor
- Entities:
  - o Smart grid system
  - o CERTs
- Hardware/Software:
  - o Data wallet
  - o Energy equipment

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 and evaluation sessions

  -> **A Stakeholder and Industrial Workshop coming soon**
- Access to the IRIS Community repository, with relevant documentation

Who can join?

- CISOs
- CISO team members
- Your service providers, e.g. SOC Manager

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.

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.