IRIS

@iris_h2020 | IRIS H2020 Project | @IRIS_H2020 | IRIS H2020 Project

coordinator@iris-h2020.eu | www.iris-h2020.eu

IRIS Vision

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.

Project Facts

Duration: 36 months (September 2021-August 2024)
EU funding: 4 918 790.00

Pilots:
#1 **Barcelona**, Spain
#2 **Tallinn**, Estonia
#3 **Helsinki**, Finland and **Tallinn**, Estonia

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

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727.

Pilot Use Cases

Pilot Use Case #1

Securing the smart city's IoT and control systems against confidentiality & integrity breaches

Focus: Securing the IoT and control system infrastructure deployed in a tramway station against confidentiality and integrity breaches.

Place: Barcelona, Spain

Expected outcomes:

- Safer environment where tramways, pedestrians and bikes may coexist safely
- Less safety issues and accidents stemming from man-made cyber-attacks

End Users: CERTs/CSIRTs, transport operators

Pilot Use Case #2

Securing AI-enabled infrastructure of autonomous transport systems in a smart city

Focus: Protection of the AI-enabled infrastructure of the autonomous transport system (AV shuttle and the Remote Operation Centre) available in Tallinn against potential orchestrated attacks.

Place: Tallinn, Estonia

Expected outcomes:

- Minimization of the impact of the attack by identifying the threat, self-recovering from it and sharing the corresponding intelligence with other related system operators and platforms
- Assisting system operators to identify if specially crafted data, designed to confuse AI-based decision making, (e.g., spoofed/fuzzed) are received from onboard vehicle sensors, or injected directly to APIs

End Users: CERTs/CSIRTs, CI security operators

Pilot Use Case #3

Effective incident response and threat intelligence collaboration for critical cross-border smart grid threats

Focus: Education of CERTs/CSIRTs on effective incident response and threat intelligence collaboration in cross-border cyber-attacks.

Place: Tallinn, Estonia and Helsinki, Finland

Expected outcomes:

- Safer services and more protected components of the smart grid to the building residents
- Better decision-making for the energy operators
- Secure energy infrastructure

End Users: CERTs/CSIRTs, Energy infrastructure stakeholders

Consortium

INOV (inesc) · ECS European Cyber Security Organisation · Universitatea Politehnica București · Directoratul Național de Securitate Cibernetică · Atos · Thales Building a future we can all trust · netcompany intrasoft · Cisco · list CEA tech · Exalens · Επίσεη ICCS · Sidroco · CyberEthicsLab. Responsible Research and Innovation · TU Delft · UPC Universitat Politècnica de Catalunya BarcelonaTech · FinEst Centre for Smart Cities · iti Information Technologies Institute · KEMEA · Ajuntament de Barcelona · Forum Virium Helsinki