Consortium

INOV inesc

ECS European Cyber Security Organisation

Guvernul României — Directoratul Național de Securitate Cibernetică

INTRASOFT International

THALES — Building a future we can all trust

Atos

CISCO

EXALENS

SIDROCO

CyberEthicsLab. — Responsible Research and Innovation

list — cea tech

iti — Information Technologies Institute

ΕΝΙΣΕΥ ICCS

TU Delft

FinEst Centre for Smart Cities

UPC — Universitat Politècnica de Catalunya BarcelonaTech

KEMEA

Ajuntament de Barcelona

FORUM VIRIUM HELSINKI

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

www.iris-h2020.eu

coordinator@iris-h2020.eu

@iris_h2020

IRIS H2020 Project

IRIS

What is IRIS about?

The Challenge

As existing and emerging smart cities continue to expand their IoT and AI-enabled platforms, this introduces novel and complex dimensions to the threat intelligence landscape 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.

Vision

IRIS will deliver a framework that support European CERT and CSIRT networks detecting, sharing, responding and recovering from cybersecurity threats and vulnerabilities of IoT and AI-driven ICT systems, to minimize the impact of cybersecurity and privacy risks, through a collaborative-first approach and state-of-the-art technology.

Project Facts

Duration: 36 months
(September 2021-August 2024)
EU funding: 4 918 790.00
Pilots: Barcelona/Spain, Tallinn/Estonia, Helsinki/Finland

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

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 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.
- 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 and implement 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 design and implement a virtual cyber range platform for training cybersecurity professionals to fight against adversarial AI and machine learning attack.
- 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.