IRIS General Presentation

Gonçalo Cadete / INOV

SOTER Final Event

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
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.
IRIS Architecture

- **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

- **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.