Press Release

Brussels, 6 October 2021

Artificial Intelligence Threat Reporting & Incidence report system

A new EU project has come to protect ICT systems providing collaborative-first approach and state-of-the-art technology

The European-funded project IRIS, which consists of 19 partners from 12 European countries, officially launched its activities with the organisation of the virtual consortium kick-off meeting held in September 2021.

As existing and emerging smart cities continue to expand their IoT and AI-enabled platforms, novel and complex dimensions to the threat intelligence landscape are introduced. These are 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. This lack of experience, as well as of tools for detecting and reporting IoT and AI attack vectors is further aggravated by potentially greater safety risks caused by such attacks.

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

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.

minimise the impact of cybersecurity and privacy risks. The IRIS platform will be made available, free of charge, to the European CERT and CSIRTs, by the end of the project.

IRIS' concept is proposed as a federated threat intelligence architecture that instates three core technological and human-centric components into the threat intelligence ecosystem:

- **The Collaborative Threat Intelligence** module: it forms the nexus of the IRIS framework and core component of the architecture enhancing the capabilities of the existing MeliCERTes platform by introducing **Analytics Orchestration**, an **Open Threat Intelligence interface** and an intuitive **Threat Intelligence Companion**. All these are supported by a **Data Protection and Accountability** module;
- **The Automated Threat Analytics** module: it collects and supplies key threat and vulnerability assessment telemetry and responds to received intelligence, initiating autonomous response and self-recovery procedures;
- **The Cloud-based Virtual Cyber Range:** it delivers an immersive virtual environment for collaborative CERT/CSIRT training exercises based on real-world environment platforms (and Digital Twin Honeypots), providing representative adversarial IoT & AI threat intelligence scenarios and hands-on training.

The IRIS platform will be demonstrated and validated in three carefully selected pilots resembling real world environments with the engagement of three smart cities (Helsinki, Tallinn and Barcelona) along with the involvement of national CERTs, CSIRTs and cybersecurity authorities.

"*IRIS is uniquely positioned to provide a high impact solution to support the operations of European CERTs and CSIRTs for coordinated response to large-scale cross-border cybersecurity incidents and crises*," mentions Mr Nelson Escravana from INOV, the Project Coordination Team.

"We are looking forward to contributing to IRIS through our ongoing work on standardisation, sector-specific requirements and CISO community-building. With our Working Group 3 on Cyber Resilience of Economy, Infrastructure and Services, we'll be able to engage with key stakeholders to validate policy recommendations and facilitate public-private collaboration on information-sharing and cyber threat intelligence that will strengthen IRIS' collaborative approach centred around CERTs/CSIRTs.", says ECSO Senior Policy Manager Nina Olesen.

The IRIS consortium comprises of public organisations, SMEs with cutting-edge cyber technologies, large industries as service providers, as well as research and academic partners with significant achievements to cybersecurity and privacy technologies.

About ECSO

The European Cyber Security Organisation (ECSO) is a non-for-profit organisation, established in 2016. ECSO unites more than 250 European cybersecurity stakeholders, including large companies, SMEs and startups, research centres, universities, end-users, operators, associations and national administrations. ECSO works with its Members and Partners to develop a competitive European cybersecurity ecosystem providing trusted cybersecurity solutions and advancing Europe's cybersecurity posture and its technological independence.

More information: www.ecs-org.eu.

Contact Details

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

Email: coordinator@iris-h2020.eu

Project at a Glance

Acronym	IRIS
Title	Artificial Intelligence threat Reporting and Incident response System
Funding	This project has received funding from from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727
Duration	36 months (September 2021 – August 2024)
Project Coordinator	INOV - Instituto de Engenharia de Sistemas e Computadores, Inovacão, (INOV), Portugal Email: *coordinator@iris-h2020.eu*
Consortium	• INOV - Instituto de Engenharia de Sistemas e Computadores, Inovacão, (INOV), Portugal • European Cyber Security Organisation (ECSO), Belgium • Centrul National De Raspuns La Incidente De Securitate Cibernetica, (CERT-RO), Romania • Intrasoft International SA (INTRA), Luxembourg • Thales Six Gts France SAS (THALES), France • Atos It Solutions And Services Iberia SL (ATOS), Spain • Cisco Systems Spain S.L (CISCO SPAIN), Spain • Exalens (CLS), Netherlands • Sidroco Holdings Limited (SID), Cyprus • Cyberethics Lab SRLS (CEL), Italy • Commissariat A L Energie Atomique Et Aux Energies Alternatives (CEA), France • Ethniko Kentro Erevnas Kai Technologikis Anaptyxis, (CERTH), Greece

	• Institute Of Communication And Computer Systems (ICCS), Greece • Technische Universiteit Delft (TU Delft), Netherlands • Tallinna Tehnikaülikool (TalTech), Estonia • Universitat Politecnica De Catalunya (UPC), Spain • Kentro Meleton Asfaleias (KEMEA), Greece • Institut Municipal D'informatica De Barcelona (IMI BCN), Spain • Forum Virium Helsinki OY (FVH), Finland
Social Media	• Twitter: @iris_h2020 • LinkedIn: IRIS H2020 Project
Website	www.iris-h2020.eu/