iRiS

artificial Intelligence threat Reporting and Incident response System

As existing and emerging smart cities continue to expand their IoT and AI-enabled platforms, this introduces novel and complex challenges to the threat intelligence landscape linked with identifying, responding and sharing data related to attack vectors, targetting emerging IoT and AI technologies.
IRIS is a Horizon 2020 project that integrates and demonstrates a single platform addressed to CERTs/CSIRTs and Critical Infrastructure Operators for assessing, detecting, responding to and sharing information regarding threats & vulnerabilities of IoT and AI-driven ICT systems within smart cities. To achieve this, IRIS brings together experts in cybersecurity, IoT, AI explainability, automated threat detection, response, and recovery.

IRIS helps European CERTs/CSIRTs and Critical Infrastructure Operators minimise the impact of cybersecurity and privacy risks as well as threats introduced by cyber-physical vulnerabilities in IoT platforms and adversarial attacks on AI-provisions and their learning/decision-making algorithms.
The IRIS platform has been demonstrated and validated in 3 highly realistic environments with the engagement of 3 smart cities (in Helsinki, Tallinn and Barcelona) along with the involvement of national CERTs/CSIRTs, and cybersecurity authorities.

The project duration extended from September 2021 to August 2024. Its resulting offerings to the Cyberesecurity market are four Service Bundles that can be used either individually or together according to the needs of the target end user :

- the Automated Threat Analytics
- the Enhanced MeliCERTes ecosystem
- the Virtual Cyber Range
- the Add-on Services

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.

IRIS

Automated Threat Analytics Service Bundle

The Automated Threat Analytics (ATA) Service Bundle is a novel cybersecurity solution designed to protect IoT and AI systems. This integrated service offers advanced vulnerability management, binary analysis, intrusion detection, and honeypot capabilities tailored specifically for the complexities of smart city environments and critical infrastructures.

ATA Service Bundle can be used to enhance their cybersecurity by evaluating and managing IoT/AI system risks. It facilitates threat intelligence sharing with standardized formats, enriches knowledge bases like MISP, and monitors for abnormal behavior using machine learning. Additionally, Digital Twin Honeypots enable proactive threat analysis and prediction, ensuring an adaptive security framework.

Target:

- Smart city operators (local governments, utility providers, transportation authorities)
- National and regional cybersecurity authorities (CERTs/CSIRTs)
- Businesses of all sizes across various industries utilizing IoT/AI technologies
- Critical Service/Infrastructure operators

Benefits:

- Proactively address emerging threats with tailored IoT/AI security measures
- Reduce the burden on security teams through automation and orchestration
- Facilitates compliance with cybersecurity regulations that focus on risk management and incident response

Partners and contact people:

IRIS

Atos

Susana Gonzalez Zarzosa: susana.gzarzosa@eviden.com
Rodrigo Diaz: rodrigo.diaz@eviden.com

EXALENS®

Irene Karapistoli: irene.karapistoli@exalens.com

CyberEthicsLab.
Responsible Research and Innovation

Lorena Volpini: l.volpini@cyberethicslab.com

list
cea tech

Michael Marcozzi: michael.marcozzi@cea.fr
Sebastien Bardin: sebastien.bardin@cea.fr
Jesus-Javier Gilquijano: Jesus-Javier.GILQUIJANO@cea.fr

IRIS

Enhanced MeliCERTes Ecosystem (EME) Service Bundle

The IRIS-Enhanced MeliCERTes ecosystem (EME) is a distributed SIEM, CTI sharing and collaboration platform enabling secure and trusted interaction among CI operators and CERTs/CSIRTs allowing them to timely be informed, assess the situation at hand and collaborate in case of a detected threat from within a customizable per type of user web frontend.

EME serves as a single hub for cybersecurity stakeholders to coordinate their efforts, share critical information, and optimize their incident response capabilities in the face of evolving cyber threats concerning primarily IoT and AI-driven platforms.The EME's information sharing, visual analytics, secure communication and collaboration features allow national CSIRTs, cybersecurity authorities, and critical infrastructure operators to be timely and fully informed, assess the situation and work together in real-time during critical incidents to effectively respond and minimize their impact. Its integrated CTI Sharing and Storage tool facilitates the development of standardized threat taxonomies, enhancing collective cyber resilience.

Target:

- National/Regional Computer Security Incident Response Teams (CSIRTs) or CERTs (Computer Emergency Response Teams)
- Cybersecurity authorities and agencies (e.g., ENISA, NCCs, EU-CERT, Europol)
- Critical infrastructure operators (focusing on smart cities) / Operators of Essential Services (OESs)
- Security Operations Centers (SOCs)

Benefits:

- Facilitates timely, interoperable sharing of incident data and cyber threat intelligence (CTI) among all relevant stakeholders

IRIS

Enhanced MeliCERTes Ecosystem (EME) Service Bundle

- **Improved incident response times by streamlining communication and information sharing**
- **Interoperable, integrates with existing cybersecurity tools and systems, leveraging previous investments**
- **User-friendly interface reduces the need to switch between multiple systems**
- **Helps organizations comply with relevant EC cybersecurity regulations and reporting requirements, such as the NIS Directive**

Partners and contact people:

netcompany

intrasoft

Sofia Tsekeridou: sofia.tsekeridou@netcompany.com

ΕΠΙΣΕΥ ICCS

Dr Angelos Amiditis: a.amditis@iccs.gr
Elefttherios Ouzounoglou: eleftherios.ouzounoglou@iccs.gr
Lazaros Karagiannidis: lazaros.karagiannidis@iccs.gr
Giovana Bilali: giovana.bilali@iccs.gr

iti Information Technologies Institute

Eleni Darra: e.darra@iti.gr
Dimitrios Kavallieros: dim.kavallieros@iti.gr
Theodora Tsikrika: theodora.tsikrika@iti.gr
Stefanos Vrochidis: stefanos@iti.gr

Virtual Cyber-Range Service Bundle

The Virtual Cyber Range (VCR) Service Bundle is a platform for immersive and realistic cybersecurity training simulations. It creates engaging, scenario-based exercises that enhance the effectiveness of cybersecurity training for both end-users and professionals. The VCR features highly realistic simulations of targeted attacks, enabling hands-on, practical training that complements theoretical knowledge. The VCR is designed to train CERT/CSIRT analysts and cybersecurity professionals, empowering organizations to develop a skilled, resilient workforce capable of defending against evolving cyber threats.

The VCR enables organizations to engage in hands-on training with immersive scenarios that simulate targeted cyber-attacks and security breaches.

Target:

- Critical infrastructure operators (e.g., energy, transportation, telecom)
- Government agencies (e.g., CERTs, CSIRTs)
- Cybersecurity service providers

Benefits:

- Realistic and immersive simulations improve learning outcomes
- Rapid development and deployment of new training scenarios

Partners and contact people:

THALES
Building a future we can all trust

Lorens Barraud: lorens.barraud@thalesgroup.com
Bruno Vidalenc: bruno.vidalenc@thalesgroup.com

KEMEA

Nikos Kapsalis: n.kapsalis@kemea-research.gr
Sotirios Spantideas: s.spantideas@kemea-research.gr

Add-on Services Service Bundle (Data Protection and Accountability (DPA) module)

The Add-on Services Bundle provides a decentralized, secure solution for logging and auditing critical decisions and changes during collaborative incident response workflows. Unlike traditional centralized logging services, DPA uses advanced self-encryption and secret key sharing technologies to ensure that logs are immutable, traceable, and managed by the collaborating parties themselves. This enhances accountability and trust in incident response processes by offering a transparent logging mechanism.

Add-on Services (DPA) can be used to enhance the integrity and transparency of their incident response processes. By securely logging and auditing critical decisions and changes in an immutable manner, organizations can ensure a reliable record of their actions.

Target:

- EU CERTs/CSIRT Teams
- National Authorities
- Organizations engaged in collaborative incident response workflows

Benefits:

- Provides a clear, immutable record of actions and decisions
- Ensures that all parties involved in incident response can access and verify logs independently

Partners and contact people:

INOV inesc

Goncalo Cadete: goncalo.cadete@inov.pt

TU Delft

Roland Kromes: R.G.Kromes@tudelft.nl

IRIS Components

SiVi

SiVi is a versatile tool with a dual functionality. Firstly, it operates as an intrusion detection system leveraging state-of-the-art machine learning algorithms. Secondly, it features an innovative user-friendly dashboard, offering end users a highly interpretable representation of complex security data. SiVi is part of the AI threat analytics and detection engine of the IRIS Automated Threat Analytics (ATA) module.

SiHoneypots

SiHoneypots is a specialized tool designed to deploy Honeypots associated with modern embedded devices, sensors, and industrial hardware. This tool effectively "traps" malicious actors, capturing pertinent information related to the deployed attacks. SiHoneypots actively supports the acquisition of threat intelligence and facilitates sharing through established message formats. SiHoneypots are part of the AI threat analytics and detection engine of the IRIS Automated Threat Analytics (ATA) module.

Charalampos Eleftheriadis: celeftheriadis@sidroco.com
Zisis Batsos: zbatzos@sidroco.com
Harris Saoulidis: hsaoulidis@sidroco.com

Nightwatch

Nightwatch is an AI-based threat detection tool which enables the identification of threats targeting IoT and AI-provisioned systems through activity readings and endpoint behaviour heuristics. Nightwatch is part of the AI threat analytics and detection engine of the IRIS Automated Threat Analytics (ATA) module.

Risk Based Response and Self Recovery (RRR) module

The RRR module is part of the IRIS ATA module. It uses threat telemetry to generate incident response procedures by employing statistical analysis, optimisation techniques, and machine learning approaches, all within the context of selected response and self-recovery actions.

Irene Karapistoli: irene.karapistoli@exalens.com

IRIS Components

BINSEC

BINSEC is a platform for featuring binary-level security-oriented program analysis. The tool is developed mainly in OCaml. It is open source (LGPL license), and builds upon off the shelf automated constraint solvers, such as Boolector or Z3 ("SMT solvers"), as external components. The interface of the tool is currently file-based.

Jesus-Javier Gilquijano: Jesus-Javier.GILQUIJANO@cea.fr

MAI-GUARD (Artificial Intelligence-based Global Unified Anomaly Detection and Response)

MAI-GUARD is an advanced security tool for embedded industrial systems, which uses embedded AI to quickly detect anomalies and cyber-attacks in machine data, provide automated response to protect the system, and reduce downtime caused by machine failures. In the context of the IRIS project, the primary objective of the MAI-GUARD tool is to detect adversarial example attacks aimed at deceiving the automated vision system of the autonomous AV Shuttle (PUC2). The intent of these attacks is to cause misclassification of critical objects such as other vehicles and traffic lights.

Michael Marcozzi: michael.marcozzi@cea.fr
Sebastien Bardin: sebastien.bardin@cea.fr

Vulnerability Discovery Manager (VDM)

VDM is the tool included in the IoT and AI-Provision Risk and Vulnerability Assessment Module for the dynamic identification, analysis and reporting of known vulnerabilities in the target infrastructure.

Susana Gonzalez Zarzosa: susana.gzarzosa@eviden.com
Rodrigo Diaz: rodrigo.diaz@eviden.com

IRIS Components

Advanced Threat Intelligence Orchestrator (ATIO)

Advanced Threat Intelligence Orchestrator (ATIO) is a full stack solution, that acts like a middleware system, due to, its central location in the architecture, all data is transferred via it. Therefore, ATIO links ATA, EME (which includes CTI and DPA), and Infrastructure. Four backend services and two frontend services compose ATIO. Also, an OPEN-API framework circles it in order to make the component data interoperable.

Dr Angelos Amiditis: a.amditis@iccs.gr
Giovana Bilali: giovana.bilali@iccs.gr

Data Protection and Accountability Module (DPA)

The DPA module provides secure, immutable and traceable logging and auditing functions, to enforce accountability in collaborative network environments, promoting a network of trust.

Goncalo Cadete: goncalo.cadete@inov.pt
Katai Liang: kaitai.liang@tudelft.nl

IRIS CyberTraP Capture the Flag (CTF) tool

The CyberTraP tool will be used as a scoring engine for the IRIS training exercises by the trainees. In addition, the CyberTraP tool can be used to possibly host additional CTF training exercises/scenarios.

Nikos Kapsalis: n.kapsalis@kemea-research.gr
Sotiris Spantideas: s.spantideas@kemea-research.gr

IRIS Components

CTI Sharing & Storage

CTI Sharing and Storage tool has been designed and implemented focusing on the CTI gathering, analysis and enrichment by employing dynamic taxonomies and ontologies of threats, attacks and vulnerabilities according to the contents of the generated CTI. This aims to assist not only researchers and practitioners but also CERTs/CSIRTs and several other stakeholders in developing a common lexicon about threats, attacks and vulnerabilities, collectively increasing their cyber resilience by sharing threat information with the end goal of setting standards and best practices for managing the cybersecurity of ICT systems against attackers.

Eleni Darra: e.darra@iti.gr
Dimitris Kavalieros: dim.kavallieros@iti.gr
Theodora Tsikrika: theodora.tsikrika@iti.gr
Stefanos Vrochidis: stefanos@iti.gr

iti Information Technologies Institute

IRIS-Enhanced MeliCERTes Ecosystem (EME)

The IRIS-Enhanced MeliCERTes ecosystem (EME) in IRIS is a distributed SIEM, CTI sharing and collaboration platform enabling secure and trusted interaction among CI operators and CERTs/CSIRTs allowing them to timely be informed, assess the situation at hand and collaborate in case of a detected threat from within a customizable per type of user frontend.

Sofia Tsekeridou: sofia.tsekeridou@netcompany.com
Dimitris Skias: dimitris.skias@netcompany.com
Kostas Chisiridis: konstantinos.chisiridis@netcompany.com

netcompany
intrasoft

Watch the demo videos on our YouTube channel:
IRIS H2020 Project

IRIS

Consortium

INOV inesc

ECS
EUROPEAN CYBER SECURITY ORGANISATION

GUVERNUL ROMÂNIEI
DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

netcompany
intrasoft

THALES
Building a future we can all trust

Atos

cisco

EXALENS®

SIDROCO

CyberEthicsLab.
Responsible Research and Innovation

list
cea tech

iti
Information
Technologies
Institute

ΕΠΙΣΕΥ
ICCS

TUDelft

FinEst Centre
for Smart Cities

UPC
UNIVERSITAT POLITÈCNICA
DE CATALUNYA
BARCELONATECH

KEMEA
ΚΕΝΤΡΟ ΜΕΛΕΤΩΝ ΑΣΦΑΛΕΙΑΣ
CENTER FOR SECURITY STUDIES

Ajuntament de
Barcelona

FORUM
VIRIUM
HELSINKI

www.iris-h2020.eu

IRIS H2020 Project

@iris_h2020

coordinator@iris-h2020.eu

@iris_H2020

IRIS H2020 Project