IRIS

Components

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.

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.

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.

BINSEC (BINary SECurity tool)

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.

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.

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

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.

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.

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.

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.

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.

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.

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.

melicertes

Mattermost

KEYCLOAK

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

TU Delft

FinEst Centre for Smart Cities

UPC UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

KEMEA 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