iRiS

Artificial Intelligence Threat Reporting & Incidence report system

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.

Artificial Intelligence Threat Reporting & Incidence report system

IRIS

A collaborative CERT/CSIRT platform to combat cyber-threats in **IoT and AI-driven systems**

netcompany
intrasoft

Dr. Sofia Tsekeridou

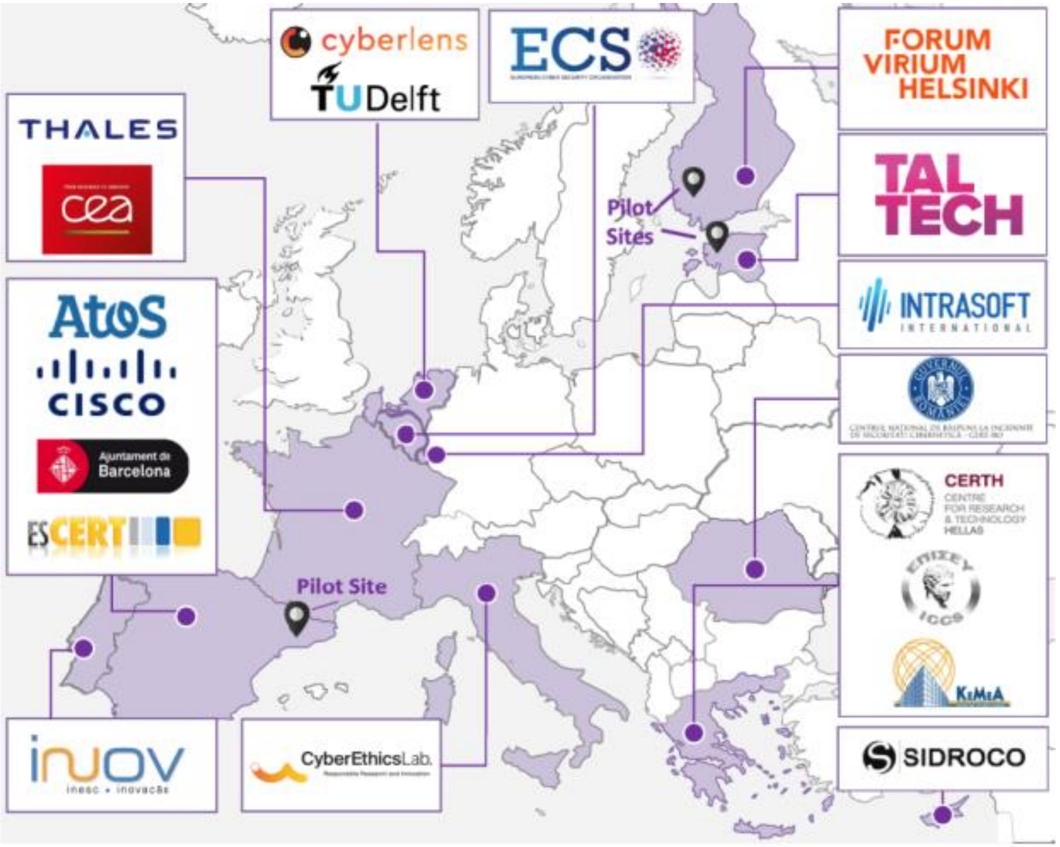
E-mail: sofia.tsekeridou@netcompany.com

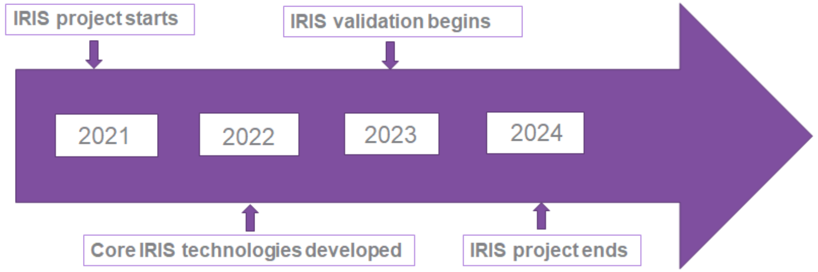
EU-CIP Project & ECSCI Cluster 1st Annual Conference on Critical Infrastructure Resilience: "Reinventing European resilience"

20-21 September 2023 , Brussels

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




IRIS project starts

IRIS validation begins

2021

2022

2023

2024

Core IRIS technologies developed

IRIS project ends

Call Identifier: 2020-SU-DS-2020

Topic: SU-DS02-2020 Intelligent security and privacy management

EC Funding: 4 918 790.00 EUR

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

Consortium

6 Public organizations
3 SMEs
4 Large ICT industries
6 Research institutions & Universities

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 Motivation

As existing and emerging **SMART CITIES** continue to **expand their IoT and AI-enabled** systems, **novel and complex threats are introduced**.

Architecture and behaviour of emerging IoT and AI technologies are **not currently well understood** by security practitioners, such as CERTs and CSIRTs.

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 Vision

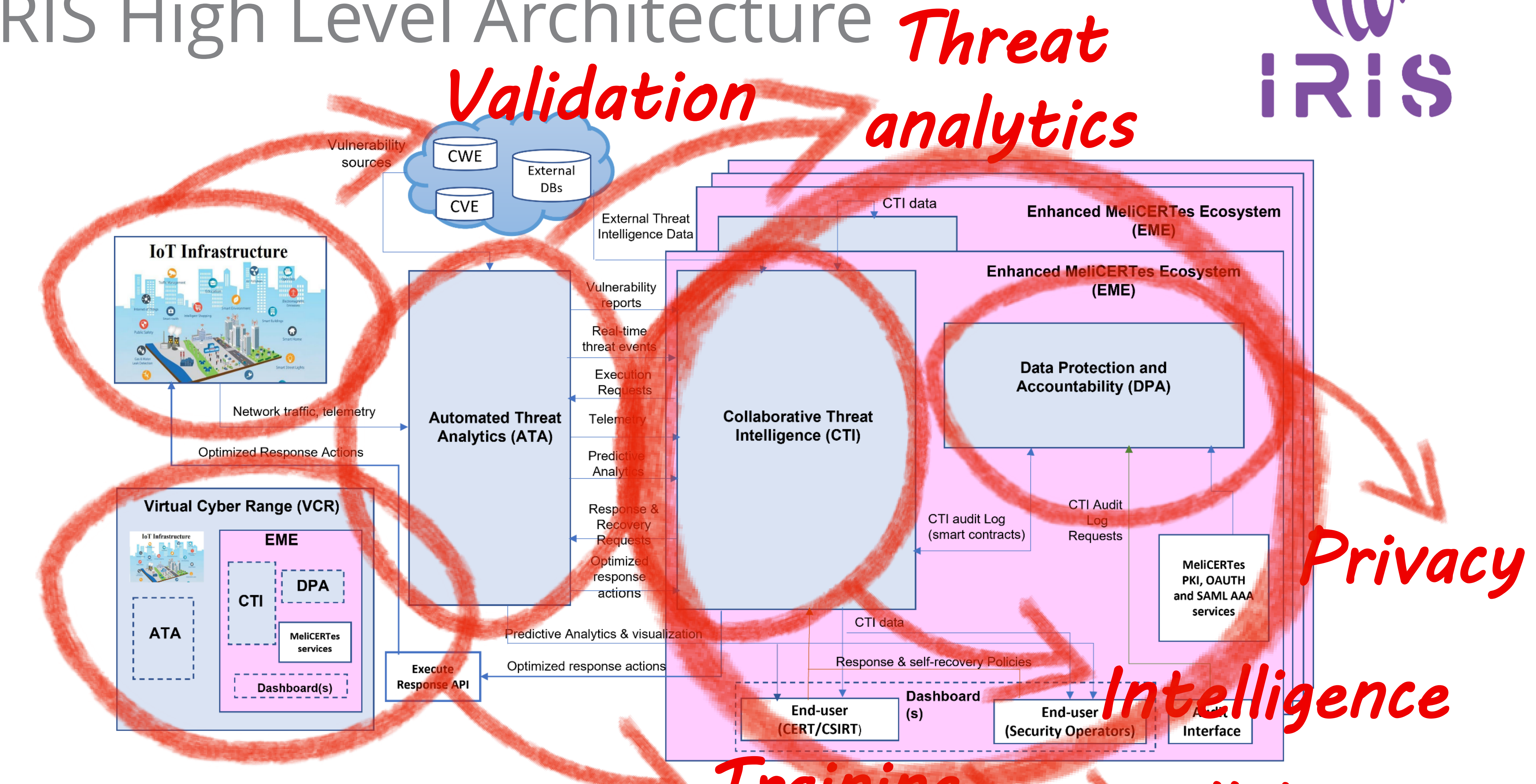
The **H2020 IRIS project** aims to deliver a framework that will support European CERT and CSIRT networks detecting, sharing, responding and recovering from **cybersecurity threats and vulnerabilities of IoT and AI-driven systems, in close collaboration with CI Operators.**

Complement the existing MeliCERTes open platform and tools.

The **IRIS Platform** will be made available, **in open source software**, to the European national CERT and CSIRTs, by the end of the project.

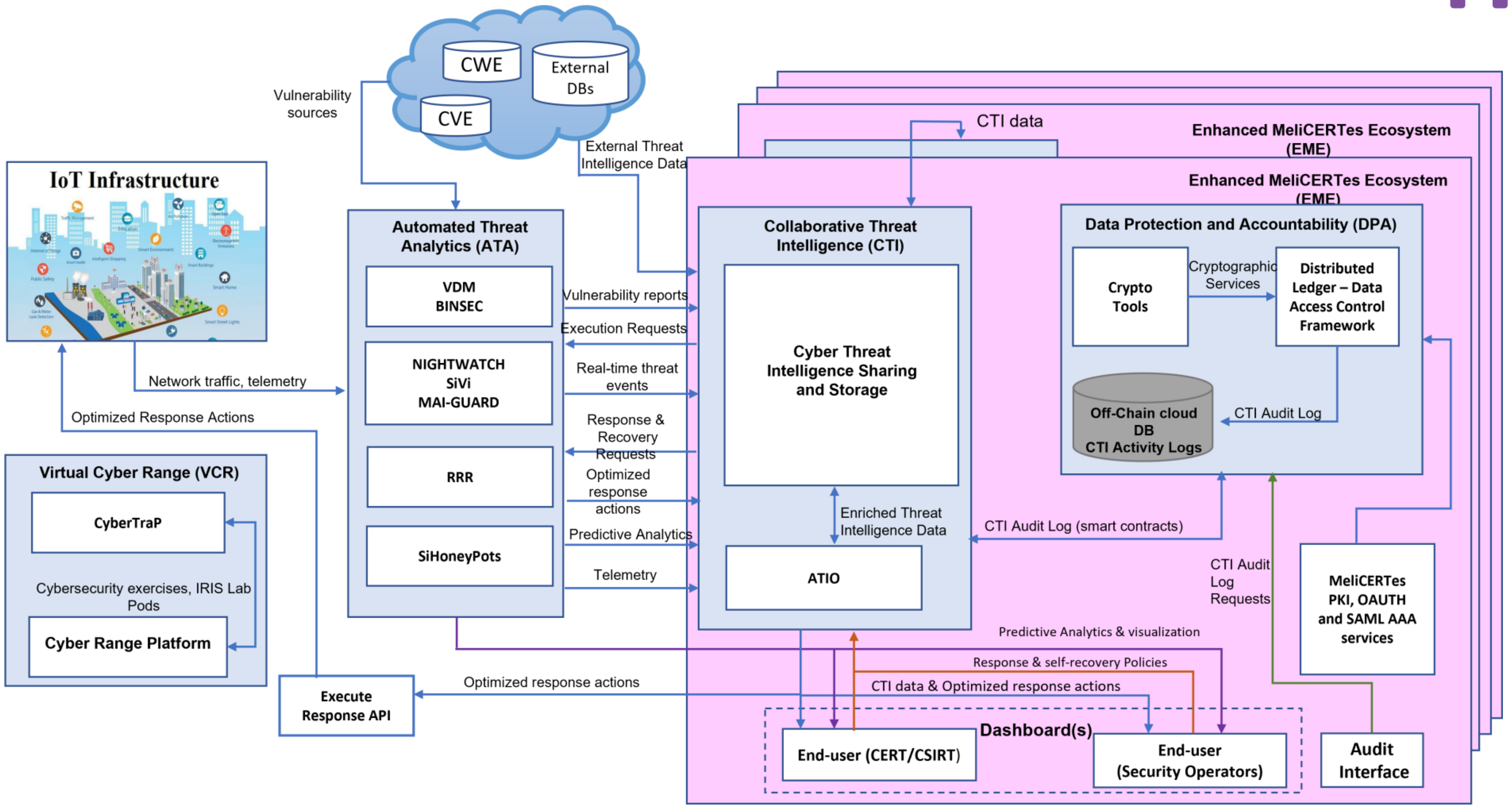
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727. This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

IRIS High Level Architecture


Threat analytics
Validation
Privacy
Intelligence
Training
Collaboration
Vulnerability sources
CWE
External DBs
CVE
IoT Infrastructure
External Threat Intelligence Data
CTI data
Enhanced MeliCERTes Ecosystem (EME)
Enhanced MeliCERTes Ecosystem (EME)
Vulnerability reports
Real-time threat events
Execution Requests
Telemetry
Predictive Analytics
Response & Recovery Requests
Optimized response actions
Network traffic, telemetry
Optimized Response Actions
Automated Threat Analytics (ATA)
Collaborative Threat Intelligence (CTI)
Data Protection and Accountability (DPA)
CTI audit Log (smart contracts)
CTI Audit Log Requests
MeliCERTes PKI, OAUTH and SAML AAA services
Virtual Cyber Range (VCR)
IoT Infrastructure
EME
CTI
DPA
ATA
MeliCERTes services
Dashboard(s)
Execute Response API
Predictive Analytics & visualization
Optimized response actions
CTI data
Response & self-recovery Policies
Dashboard (s)
End-user (CERT/CSIRT)
End-user (Security Operators)
Audit Interface

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 – Tool View


CWE
External DBs
CVE
Vulnerability sources
External Threat Intelligence Data
IoT Infrastructure
Network traffic, telemetry
Optimized Response Actions
Automated Threat Analytics (ATA)
VDM
BINSEC
NIGHTWATCH
SiVi
MAI-GUARD
RRR
SiHoneyPots
Vulnerability reports
Execution Requests
Real-time threat events
Response & Recovery Requests
Optimized response actions
Predictive Analytics
Telemetry
Virtual Cyber Range (VCR)
CyberTraP
Cybersecurity exercises, IRIS Lab Pods
Cyber Range Platform
Execute Response API
Optimized response actions
CTI data
Enhanced MeliCERTes Ecosystem (EME)
Enhanced MeliCERTes Ecosystem (EME)
Collaborative Threat Intelligence (CTI)
Cyber Threat Intelligence Sharing and Storage
Enriched Threat Intelligence Data
ATIO
Data Protection and Accountability (DPA)
Crypto Tools
Cryptographic Services
Distributed Ledger – Data Access Control Framework
Off-Chain cloud DB
CTI Activity Logs
CTI Audit Log
CTI Audit Log (smart contracts)
CTI Audit Log Requests
MeliCERTes PKI, OAUTH and SAML AAA services
Predictive Analytics & visualization
Response & self-recovery Policies
CTI data & Optimized response actions
Dashboard(s)
End-user (CERT/CSIRT)
End-user (Security Operators)
Audit Interface

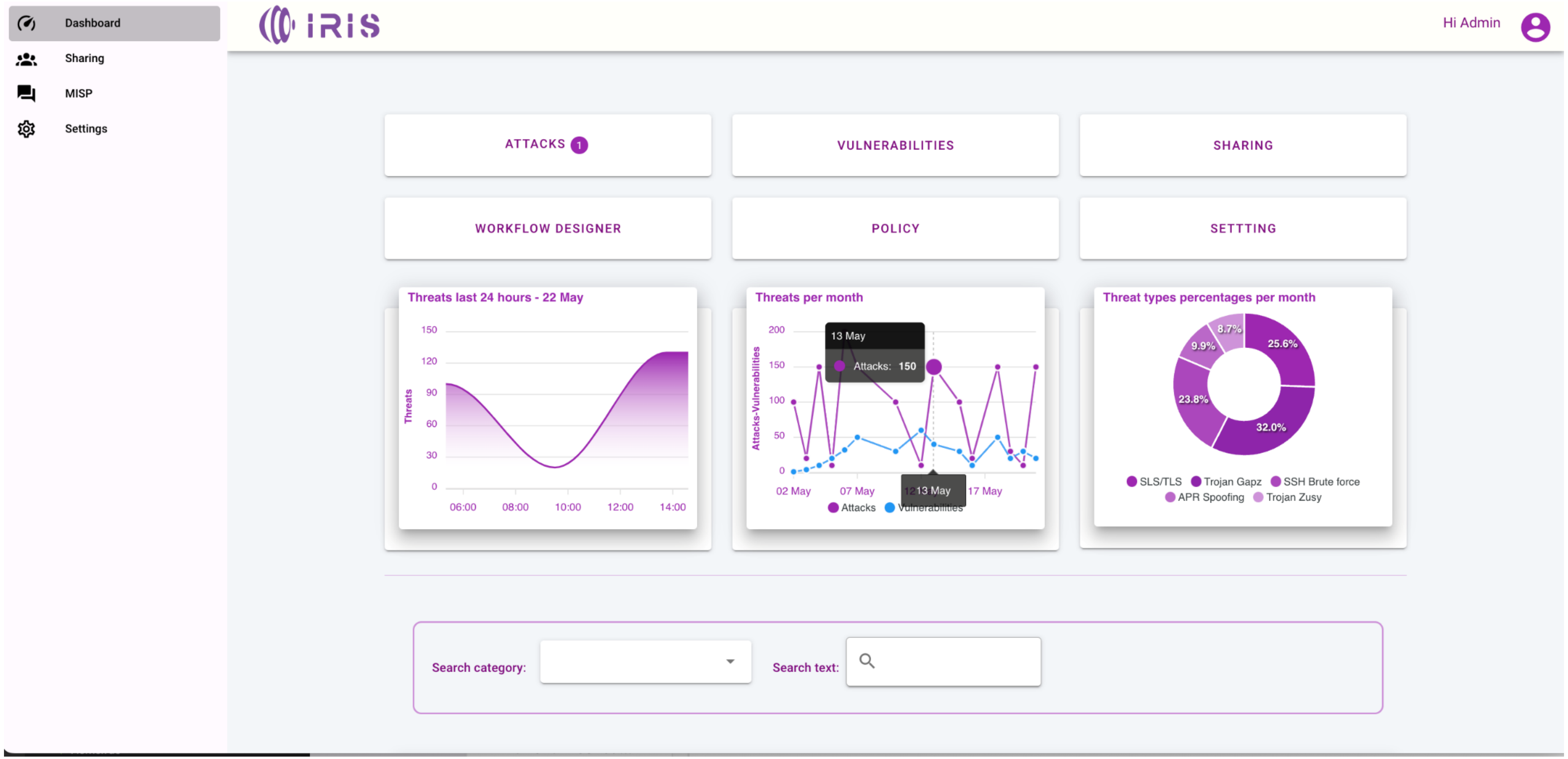
This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 101021727. This material reflects only the authors’ views and European Commission is not responsible for any use that may be made of the information it contains.

EME – Unified Dashboard & SIEM

- AI/IoT CTI event overview, management, response.
- Distinct views for the CI operator and the CERT/CSIRT authority operator
  - ✓ Aggregated and Detailed view of the detected events
- CTI orchestration information
  - ✓ Presenting CTI mitigation/response actions
    - ➢ Including automated response policy
  - ✓ CTI response workflows design
  - ✓ Collecting IRIS users' feedback enabling effective cooperation and collaboration
    - ➢ Capitalizing on standardized CTI tools
- IRIS generated AI/IoT CTI relevant information structured in a standardized format.

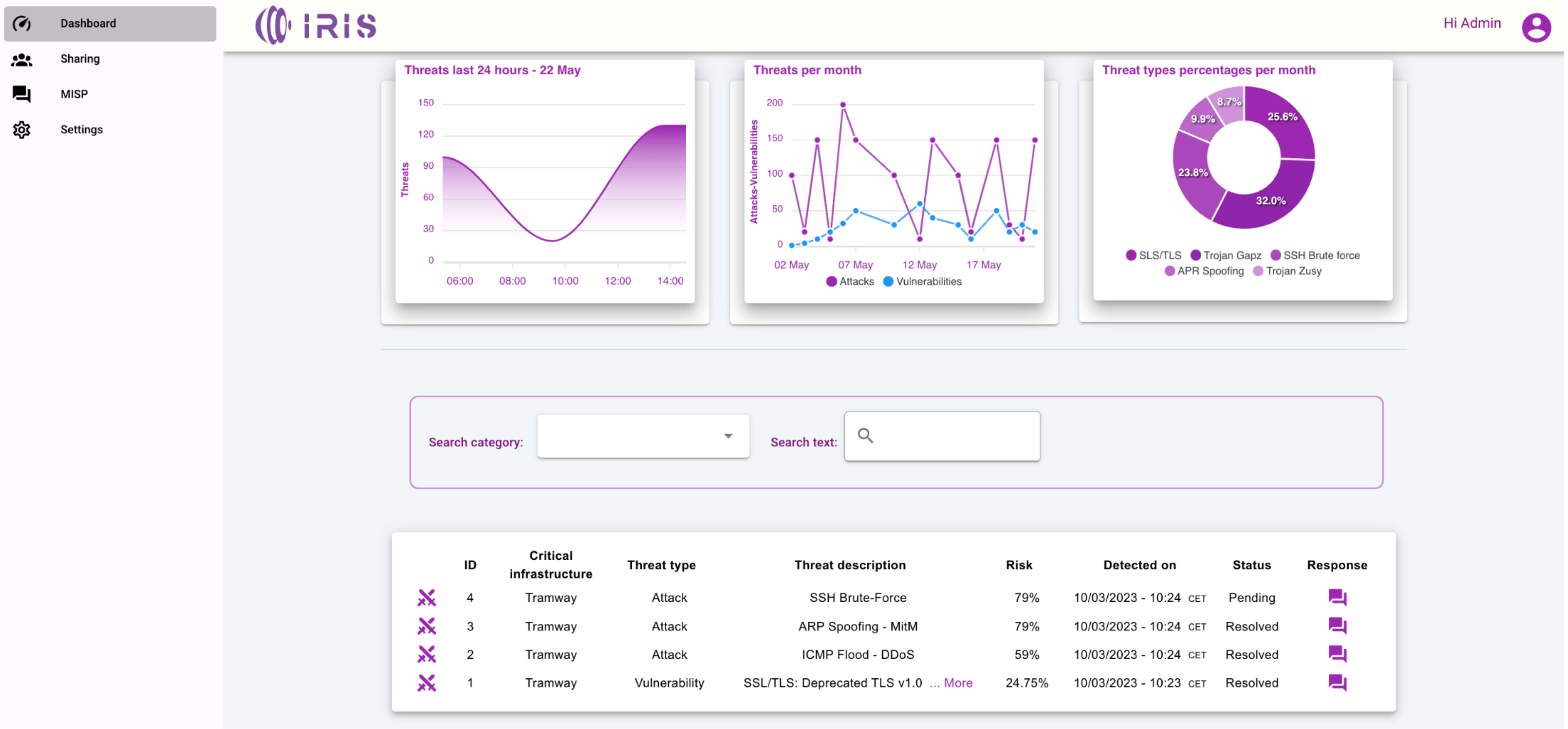
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727. This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

EME – CI operator view



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.

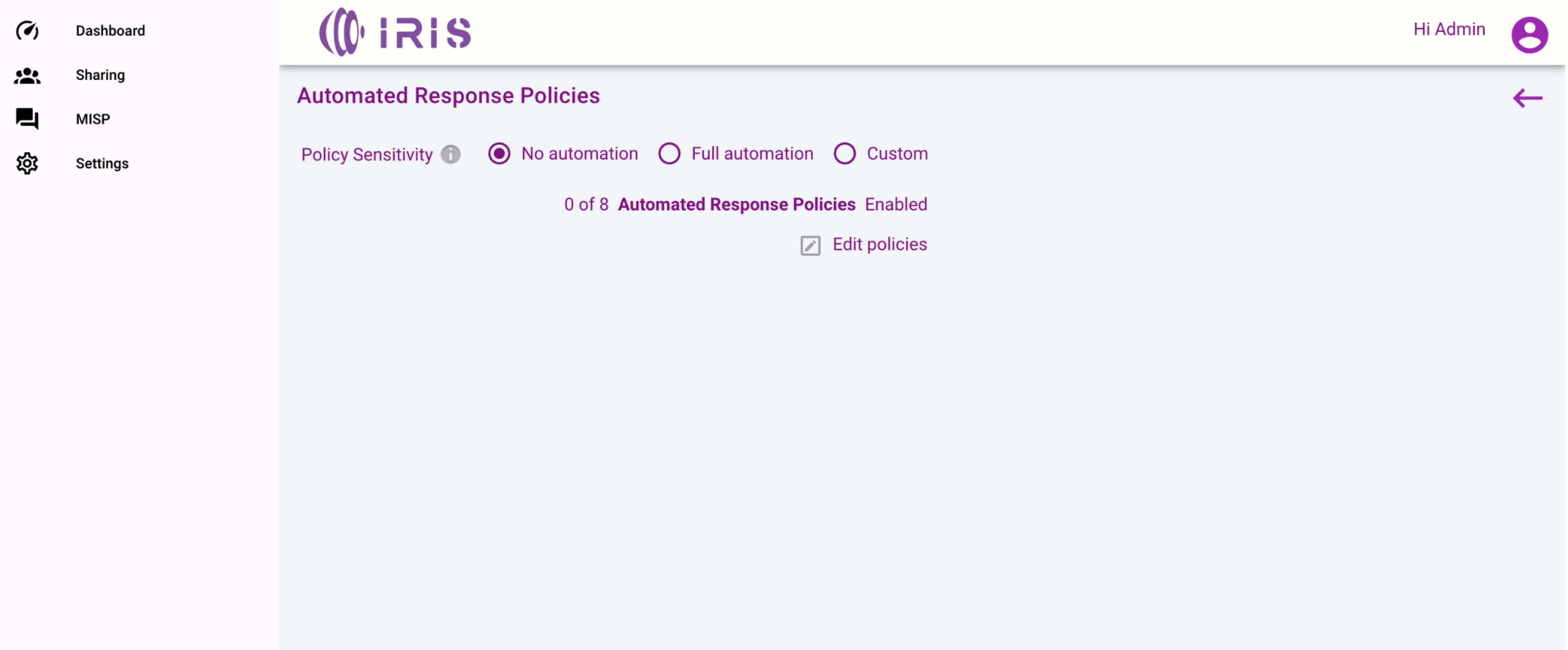
EME – CI operator view



	ID	Critical infrastructure	Threat type	Threat description	Risk	Detected on	Status	Response
	4	Tramway	Attack	SSH Brute-Force	79%	10/03/2023 - 10:24 CET	Pending	
	3	Tramway	Attack	ARP Spoofing - MitM	79%	10/03/2023 - 10:24 CET	Resolved	
	2	Tramway	Attack	ICMP Flood - DDoS	59%	10/03/2023 - 10:24 CET	Resolved	
	1	Tramway	Vulnerability	SSL/TLS: Deprecated TLS v1.0 ... More	24.75%	10/03/2023 - 10:23 CET	Resolved	

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.

EME – Automated response Policy management



Automated Response Policies

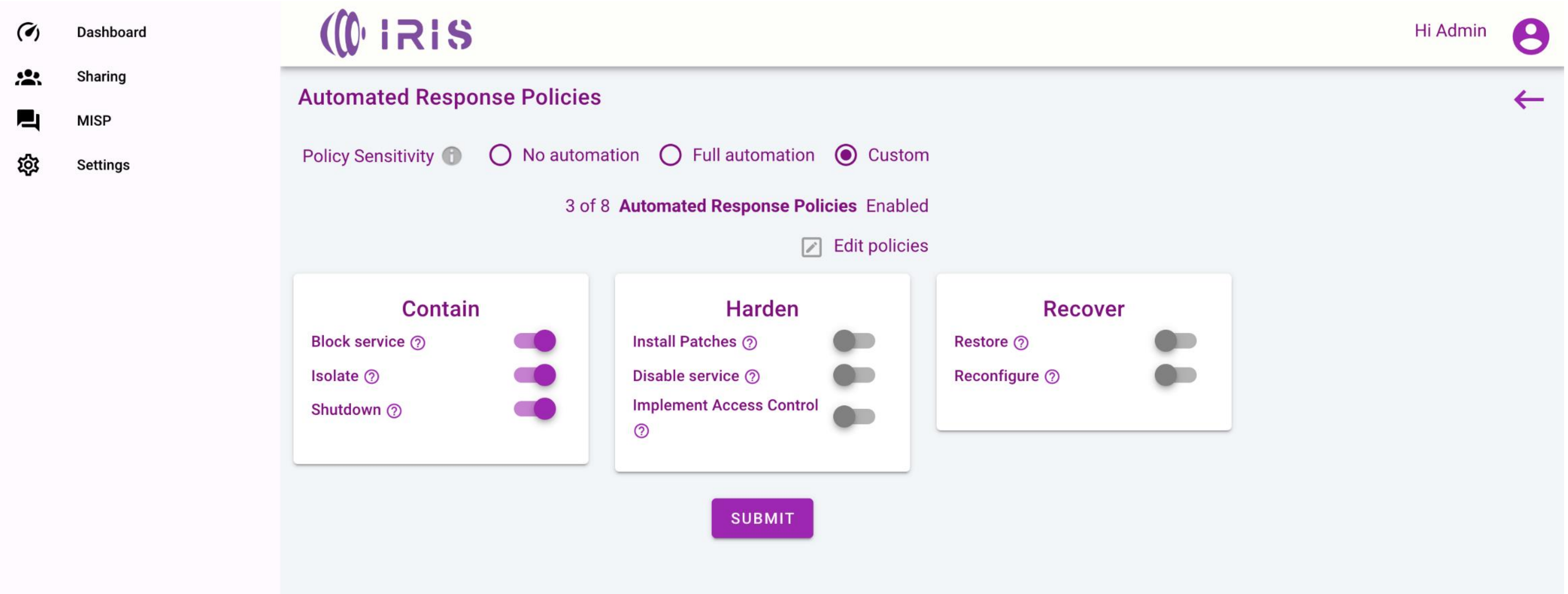
Policy Sensitivity ● No automation ○ Full automation ○ Custom

0 of 8 **Automated Response Policies** Enabled

Edit policies

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.

EME – Automated response Policy management



Automated Response Policies

Policy Sensitivity ○ No automation ○ Full automation ● Custom

3 of 8 **Automated Response Policies** Enabled

Edit policies

Contain

- Block service ?: on
- Isolate ?: on
- Shutdown ?: on

Harden

- Install Patches ?: off
- Disable service ?: off
- Implement Access Control ?: off

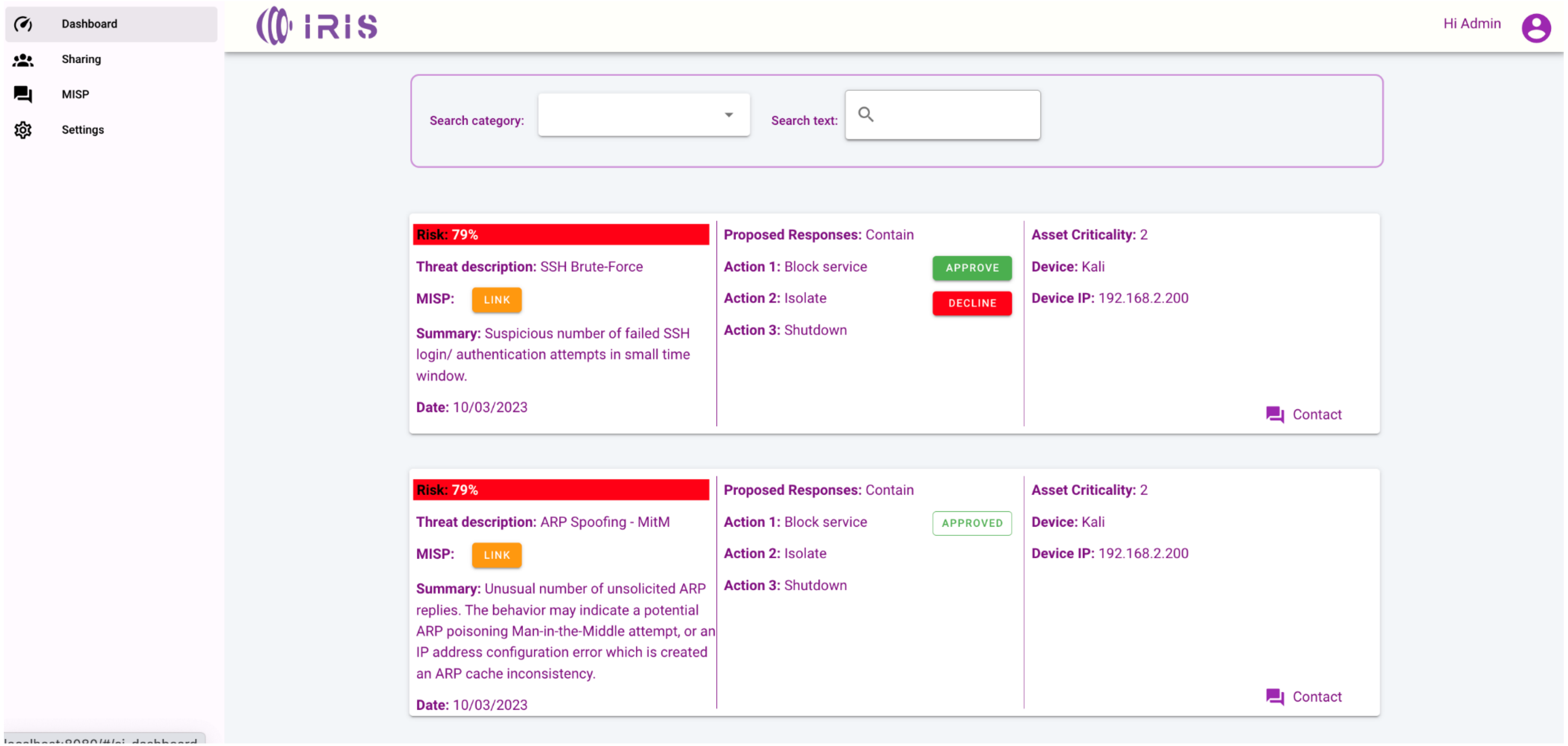
Recover

- Restore ?: off
- Reconfigure ?: off

SUBMIT

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.

EME – CI Operator Attacks view



Risk: 79%

Threat description: SSH Brute-Force

MISP: LINK

Summary: Suspicious number of failed SSH login/ authentication attempts in small time window.

Date: 10/03/2023

Proposed Responses: Contain

Action 1: Block service APPROVE

Action 2: Isolate DECLINE

Action 3: Shutdown

Asset Criticality: 2

Device: Kali

Device IP: 192.168.2.200

Risk: 79%

Threat description: ARP Spoofing - MitM

MISP: LINK

Summary: Unusual number of unsolicited ARP replies. The behavior may indicate a potential ARP poisoning Man-in-the-Middle attempt, or an IP address configuration error which is created an ARP cache inconsistency.

Date: 10/03/2023

Proposed Responses: Contain

Action 1: Block service APPROVED

Action 2: Isolate

Action 3: Shutdown

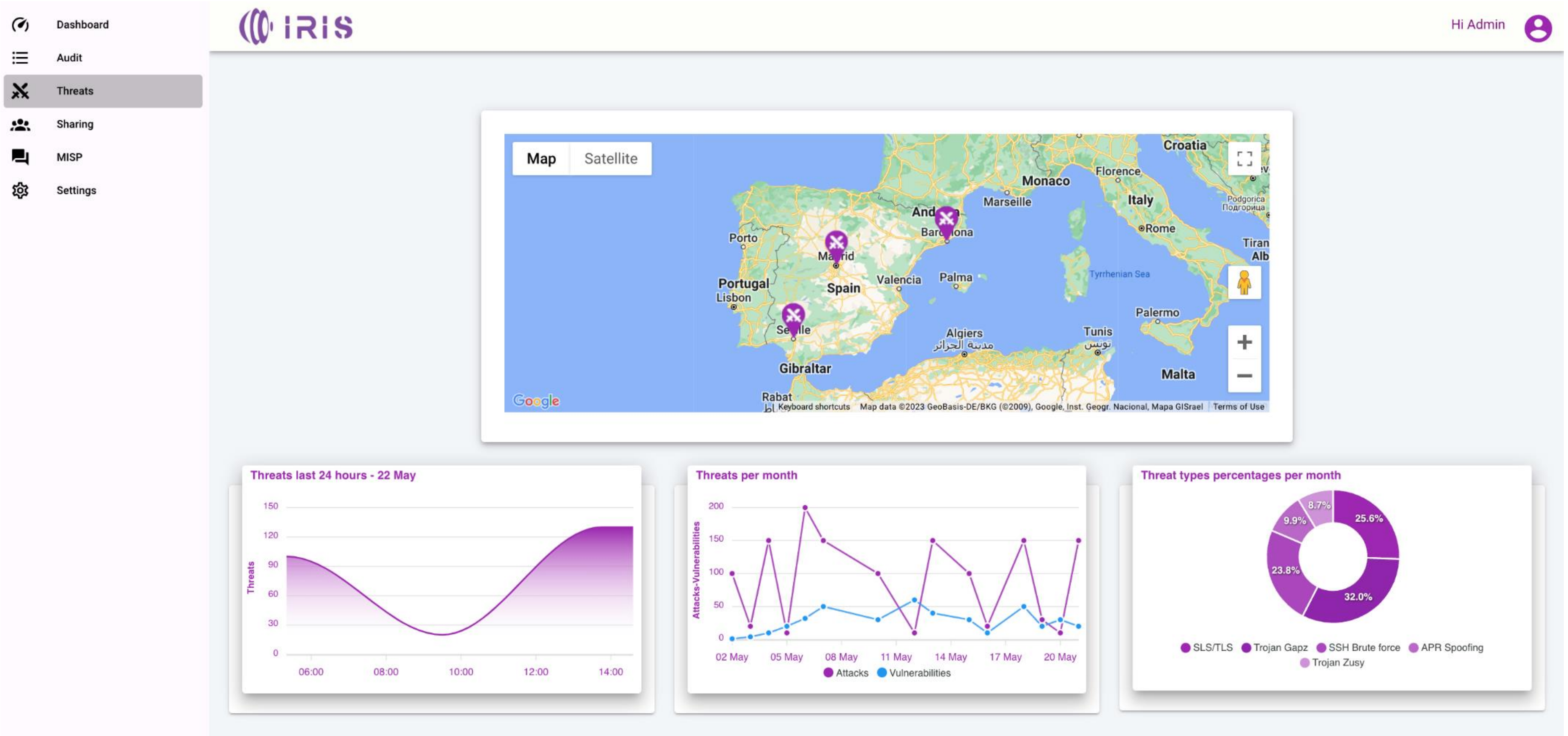
Asset Criticality: 2

Device: Kali

Device IP: 192.168.2.200

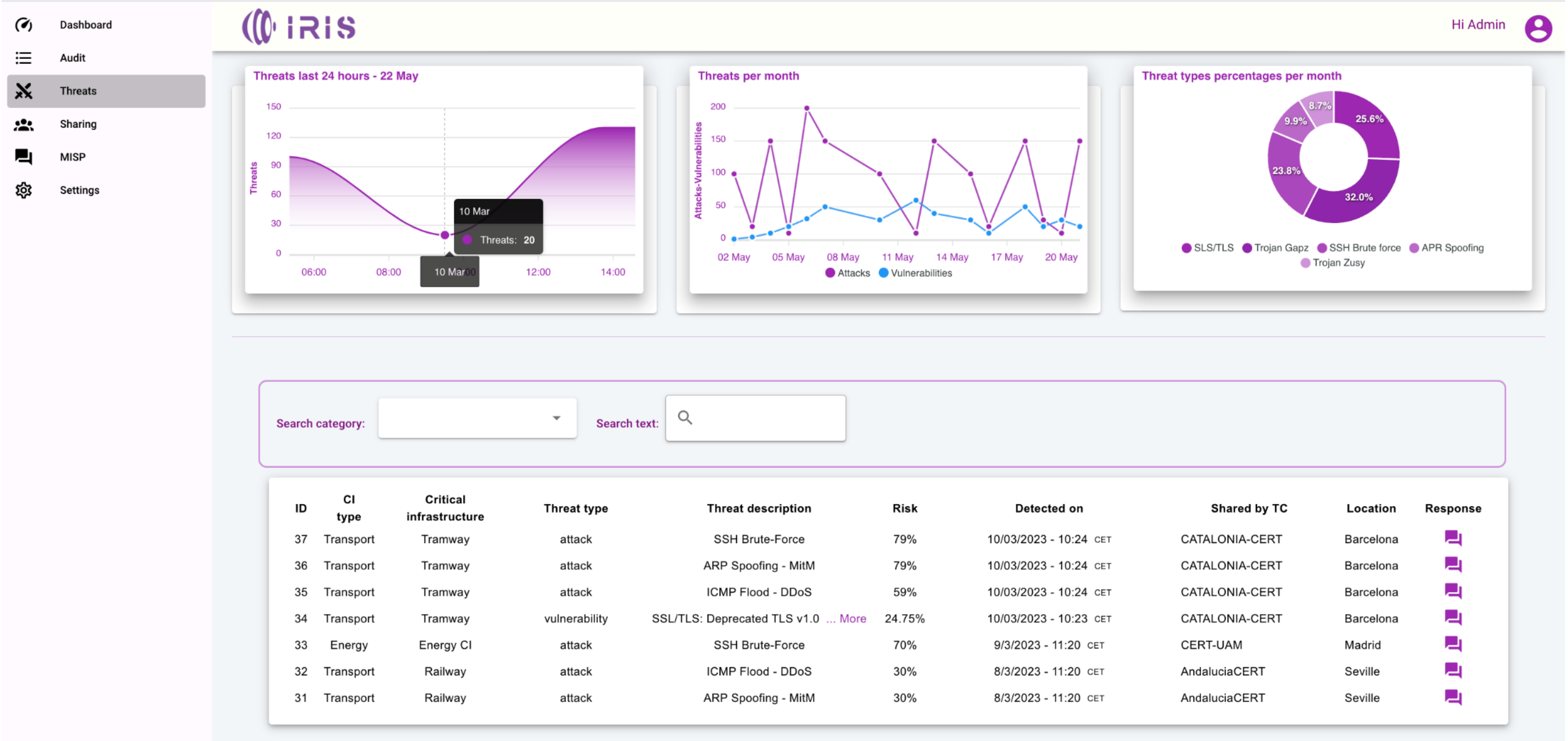
This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 101021727. This material reflects only the authors’ view and European Commission is not responsible for any use that may be made of the information it contains.

EME – CERT/CSIRT authority view



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.

EME – CERT/CSIRT authority view



ID	CI type	Critical infrastructure	Threat type	Threat description	Risk	Detected on	Shared by TC	Location	Response
37	Transport	Tramway	attack	SSH Brute-Force	79%	10/03/2023 - 10:24 CET	CATALONIA-CERT	Barcelona	
36	Transport	Tramway	attack	ARP Spoofing - MitM	79%	10/03/2023 - 10:24 CET	CATALONIA-CERT	Barcelona	
35	Transport	Tramway	attack	ICMP Flood - DDoS	59%	10/03/2023 - 10:24 CET	CATALONIA-CERT	Barcelona	
34	Transport	Tramway	vulnerability	SSL/TLS: Deprecated TLS v1.0 ... More	24.75%	10/03/2023 - 10:23 CET	CATALONIA-CERT	Barcelona	
33	Energy	Energy CI	attack	SSH Brute-Force	70%	9/3/2023 - 11:20 CET	CERT-UAM	Madrid	
32	Transport	Railway	attack	ICMP Flood - DDoS	30%	8/3/2023 - 11:20 CET	AndaluciaCERT	Seville	
31	Transport	Railway	attack	ARP Spoofing - MitM	30%	8/3/2023 - 11:20 CET	AndaluciaCERT	Seville	

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 Pilots

The Project is composed by 3 Pilots

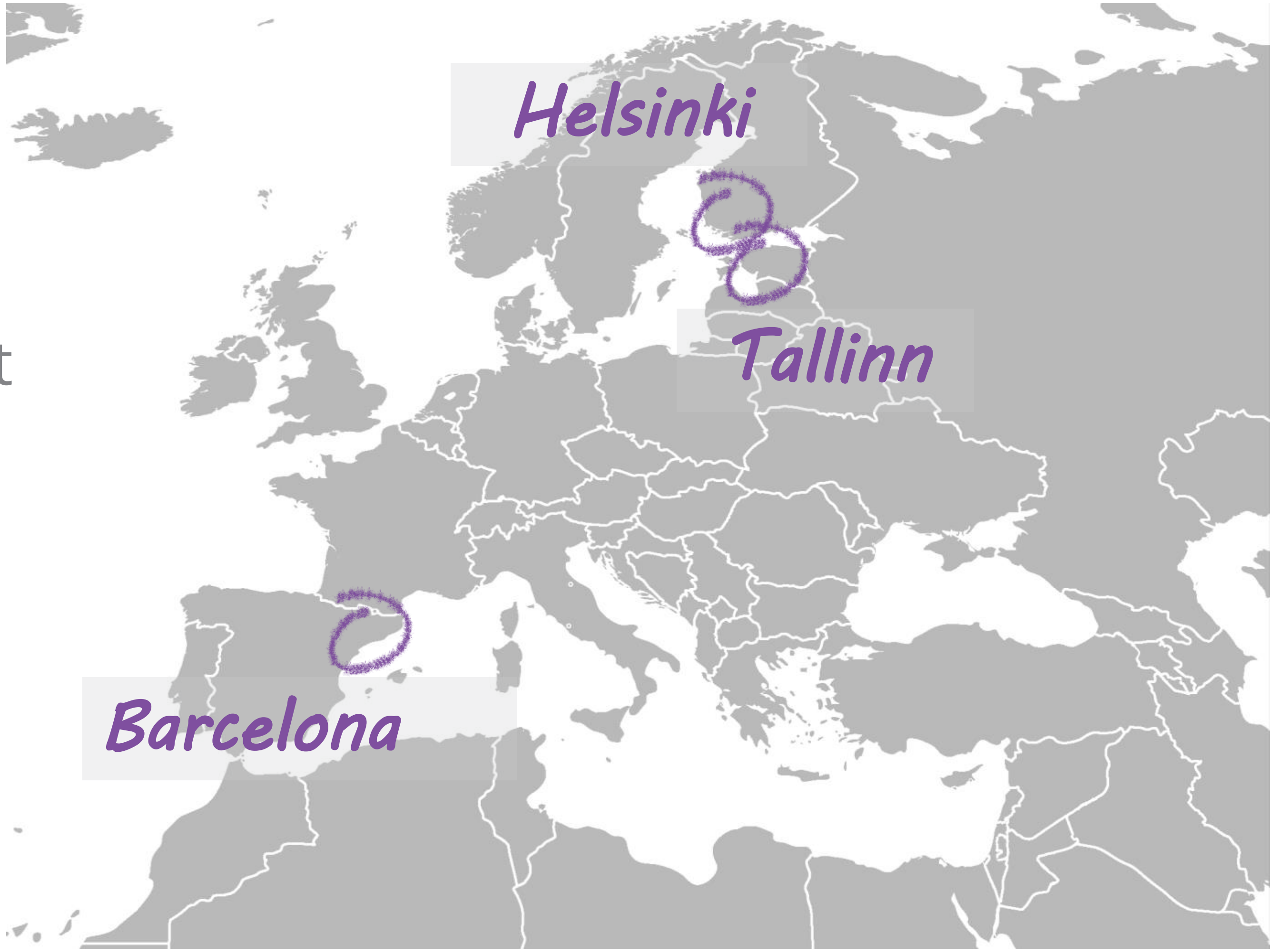
With the goal of

Identifying business requirements

Demonstrating the **AI driven** threat detection

Providing a collaborative european threat reporting environment

of the **IRIS** platform



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.

Barcelona pilot

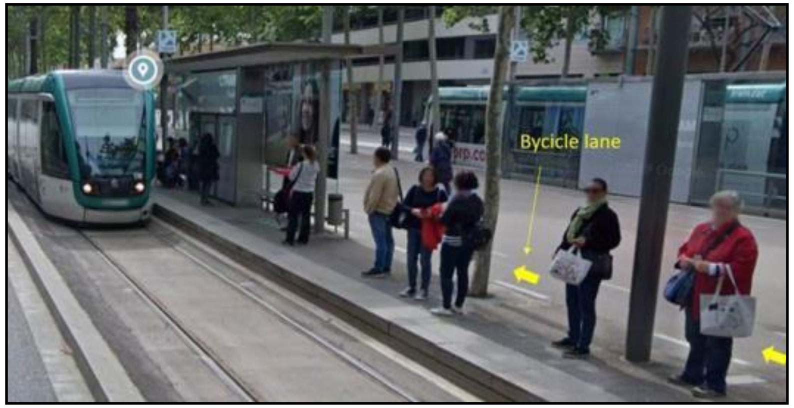
❑ **Featuring: AI computer vision system and an IoT infrastructure deployed at a Tramway station** to avoid potential accidents between bicycles and pedestrians getting off the train.

Goals and Challenges:

- Ensuring availability of IoT and IA infrastructure for the safety of tram users.

- Ensuring confidentiality on the communications of the IoT infrastructure

- Lack of experience as well as of tools, for detecting and reporting IoT & AI attack vectors.



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.

Tallinn pilot

❑ **Featuring:** AI-enabled autonomous vehicle **shuttles** (AV shuttle) that are monitored by a centralized remote operation centre.

Goals and Challenges:

- Ensuring availability of data and the operations of autonomous vehicle and supporting infrastructure.
- Lack of investigation of cyber defence mechanisms that facilitate autonomous detection and risk-based response for privacy breaches.

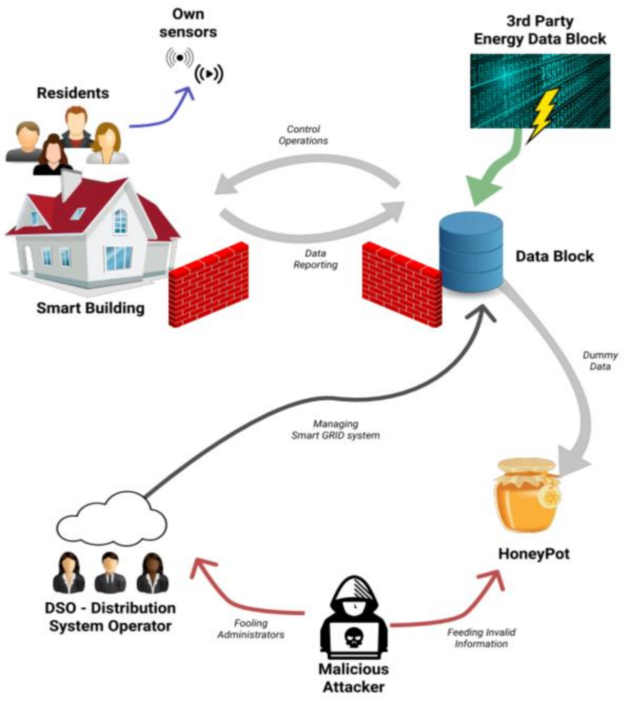
FinEst Centre
for Smart Cities

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.

Helsinki pilot

❑ **Helsinki City:** The use case will make use of an **energy distribution system** to connect Helsinki and Tallinn energy infrastructures

- **Kalasatama**: Smart Buildings can participate on energy market, since they have a **smart meter** data interface that provides information on consumption of electricity. Additionally, they provide **load control** functions that the distribution system operator (DSO) can use in situations where the production has reached its peak.

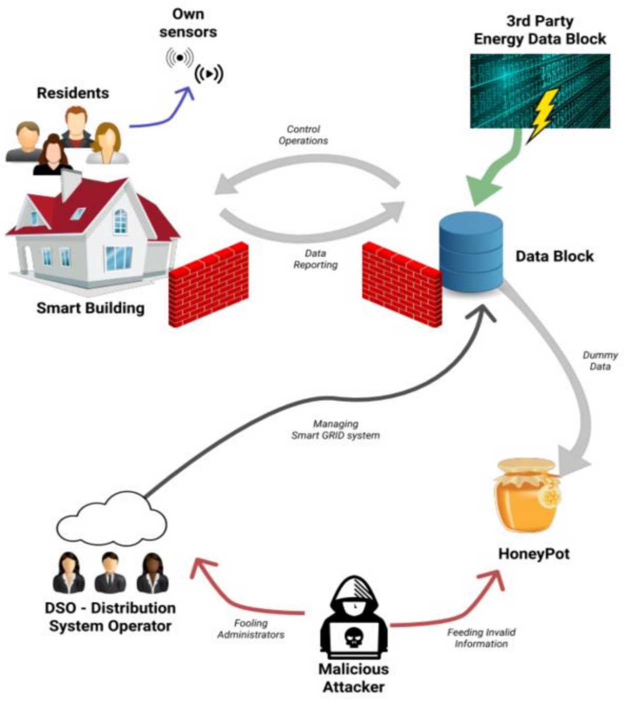


This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 101021727. This material reflects only the authors’ view and European Commission is not responsible for any use that may be made of the information it contains.

Helsinki pilot

Goals and Challenges:

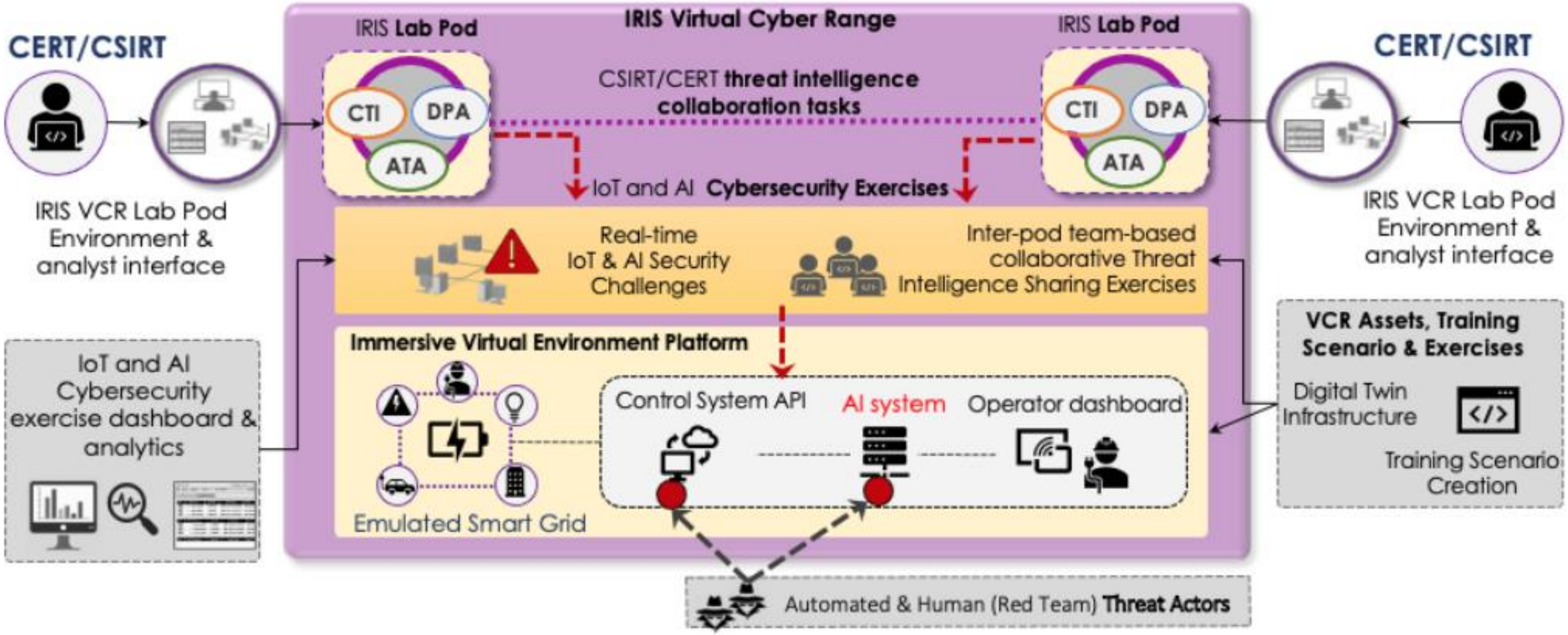
- Effective incident response and threat intelligence collaboration for cross-border smart grid threats
- Secure customer-facing components:
  - ✓ Against threats to control functions defined for the demand control
- Secure APIs:
  - ✓ Smart Grid API from Kalasatama (district of Helsinki)
  - ✓ Smart Grid APIs from the city of Tallinn.



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.

Helsinki pilot: Cyber Range

This demonstration will be emulated as a cross-border crisis management exercise on the Virtual Cyber Range (VCR), with Digital Twins of the target smart grid systems, as well as Digital Twin honeypots



CERT/CSIRT
IRIS VCR Lab Pod Environment & analyst interface
IRIS Lab Pod
IRIS Virtual Cyber Range
IRIS Lab Pod
CTI
DPA
ATA
CSIRT/CERT threat intelligence collaboration tasks
CTI
DPA
ATA
CERT/CSIRT
IRIS VCR Lab Pod Environment & analyst interface
IoT and AI Cybersecurity Exercises
Real-time IoT & AI Security Challenges
Inter-pod team-based collaborative Threat Intelligence Sharing Exercises
IoT and AI Cybersecurity exercise dashboard & analytics
Immersive Virtual Environment Platform
Emulated Smart Grid
Control System API
AI system
Operator dashboard
VCR Assets, Training Scenario & Exercises
Digital Twin Infrastructure
Training Scenario Creation
Automated & Human (Red Team) Threat Actors

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.

Key takeaways

- Smart Cities => **novel**, cutting edge AI/IoT-driven technology
- This implies **Emerging Threats** ! High risks!

- Currently, **lack of experience as well as of tools** for incident management that tackle IoT & AI attack vectors
- **IRIS** will enhance the capabilities (knowledge, toolset, training) of CERTs/CSIRTs and CI Operators, to address these challenges.

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.

Thank you for your attention!

Dr. Sofia Tsekeridou

E-mail: sofia.tsekeridou@netcompany.com

netcompany

intrasoft

iris-h2020.eu

in IRIS H2020 Project

iris_h2020

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.