SUNRISE Project

Pablo de Juan Fidalgo (ATOS)

20/09/2023

1st Annual Conference On Critical Infrastructure Resilience: “Reinventing Resilience”

SUNRISE

This project has received funding from the European Union’s Horizon Europe research and innovation programme under Grant Agreement No. 101073821

The material presented and views expressed here are the responsibility of the author(s) only.
The EU Commission takes no responsibility for any use made of the information set out.

Agenda

SUNRISE

- Project Overview
- Main pillars
- SUNRISE tools
- CPR tool
- Pilots

Project Overview

SUNRISE at a glance

SUNRISE

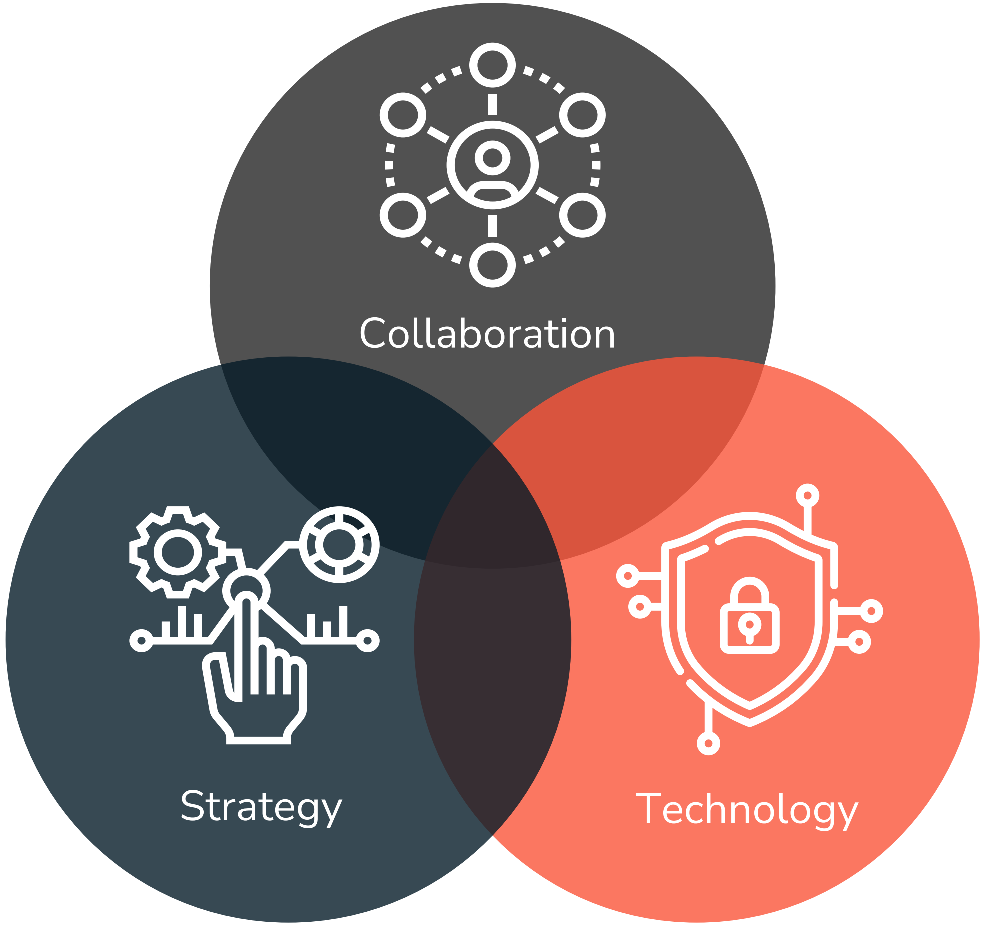
Strategies and Technologies for United and Resilient Critical Infrastructures and Vital Services in Pandemic-Stricken Europe	
Call	HORIZON-CL3-2021-INFRA-01
Grant Agreement	101073821
Website	https://sunrise-europe.eu/
Duration	36 Months (01-10/2022 – 30/09/2025)
Budget	Around 11,5 M€
Consortium	41 partners
Project Coordinator	Antonio Álvarez Romero (Atos IT)
Objectives	***O1:*** *Facilitate collaboration among CIs within and across European borders, between different sectors and between public and private stakeholders.* ***O2:*** *Identify pandemic-specific vital services and CIs in Europe, their interaction and dependencies, the risks and cascading effects among them, and effective countermeasures at European level.* ***O3:*** *Develop a comprehensive strategy and a set of mature technologies for CIs resilience and business continuity in a pandemic.* ***O4:*** *Pilot the new strategy and technologies in real-world conditions across Europe.* ***O5:*** *Enhance knowledge, awareness and capacities for unity and resilience in Europe.*

Mission Statement

SUNRISE

"Strengthening Critical Infrastructures through Collaboration, Strategy and Technology"

- Critical infrastructures' preparedness for emergency scenarios
- Mitigation when those scenarios materialize



Main Pillars

Main Pillars (I)

- **Collaboration**
  - Wide discussion **forum** for critical infrastructure operators
    - Critical infrastructures operators must not work in **silos** anymore!
  - SUNRISE is **triggering** collaboration
    - **Public** and **private stakeholders, cross-border, cross-sector**
    - **7** collaboration **workshops** in **9 months**! (6 national + 1 pan-European)
  - The project has **18 pilots** from **8** different **countries**
      - Slovenia, Spain, Italy, Serbia, France, Estonia, Israel and Czech Republic
      - Health, Digital, Energy, Transport, Water, Public Admin

Main Pillars (II)

+ Strategy

- Develop a **strategic plan** to make critical infrastructures more resilient
- Identify pandemic-specific **vital services, risks** and **cascading effects** and effective **countermeasures**
- Develop an integral approach for **risk evaluation** and **mitigation**

+ Cutting-Edge Technology

- Use it as an **enabler** to complement collaboration and strategy with supporting tools that facilitate both preparation and mitigation

SUNRISE Tools

Scenarios Addressed in the Project

SUNRISE

- Although SUNRISE mentions specifically **pandemics**, and in particular building upon experiences from **COVID**, we acknowledge a wide range of **emergency scenarios** threatening citizens´ security
- **Different emergency scenarios that may arise (with possible cascading effects)**
  - Another pandemic
  - Disasters related to climate: floods, earthquakes, hurricanes…
  - Scarcity of vital supplies: water, electricity, food
  - Limited mobility: blocked roads, rails, non-operating airports or stations…
  - Disruption of telecommunications
  - Massive cyber attacks against key targets

Risk-based Access Control

+ Access to workplaces in a pandemic scenario

- Workers need **proper identification** + ensuring they are in **proper health conditions** to access the premises
- **Efficiency** is required -> avoid **long queues** and **bottlenecks**
- **Privacy concerns** and **ethical issues** regarding **personal information** arise
- **Technology** is an **enabler** but must be used in **fair** conditions and putting people's **rights** and **needs** first
- Potentially applicable to any kind of public space

Image credit: Internal SUNRISE Presentation

Demand Prediction and Management

SUNRISE

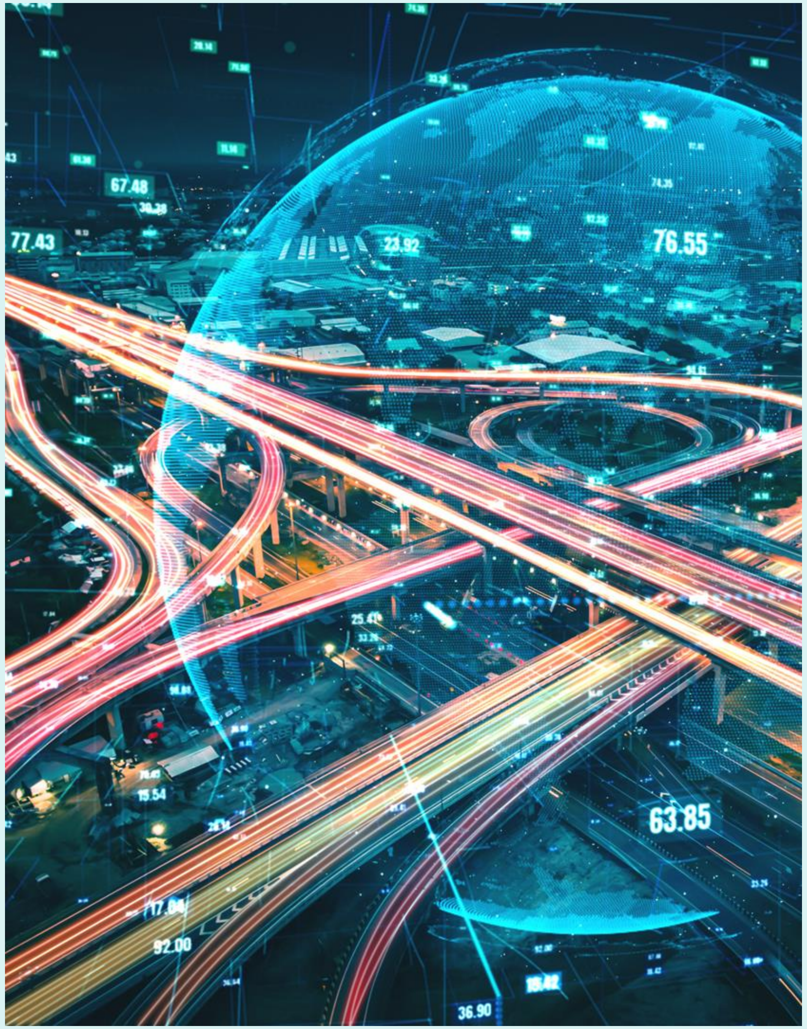
Scarcity of vital resources: hospital example

- **Medical material** is vital to treat patients
- Its scarcity might be fatal but an excess of stock is also negative as materials usually have an expiry date
    - The material becomes useless
    - Waste of money
- **Demand forecast** is an excellent instrument for hospitals to adequately dimension their stocks and schedules their purchases
- However, emergency scenarios drastically change **demand patterns** and this has to be analysed and anticipated in case of emergency materialization
- Usage of **AI-based analysis algorithms** may be of help to characterize unusual demand patterns

Image Credit: https://www.idafoundation.org/en/medical-supplies

Cyber-Physical Resilience

- **Successful cyber attacks against key cyber physical assets**
  - Critical infrastructures are fully dependent on **IT/OT modules** of different levels of importance
  - A **disruption** in the operation of a key network element might be **catastrophic**



Remote Infrastructure Inspection

+ Understaffing and caring for employees

- Avoid **dangerous activities** such as **on-site inspection** of critical infrastructures **physical components**
  - Pump stations and pipes (water)
  - Pylons and transmission powerlines (electrical grids)
  - Porcelain isolators, catenaries, pylons, rails (railway)
  - Issues faced
    - **Leaks, corrosion, rust, outgrown vegetation**
    - **Worn** and **deteriorated** infrastructures **underperform** and are a potential **danger**
- Using **satellite imagery** and **drones** for remote inspection saves time and are a safer approach for employees

Image Credit: SUNRISE Internal Deliverables

CPR tool

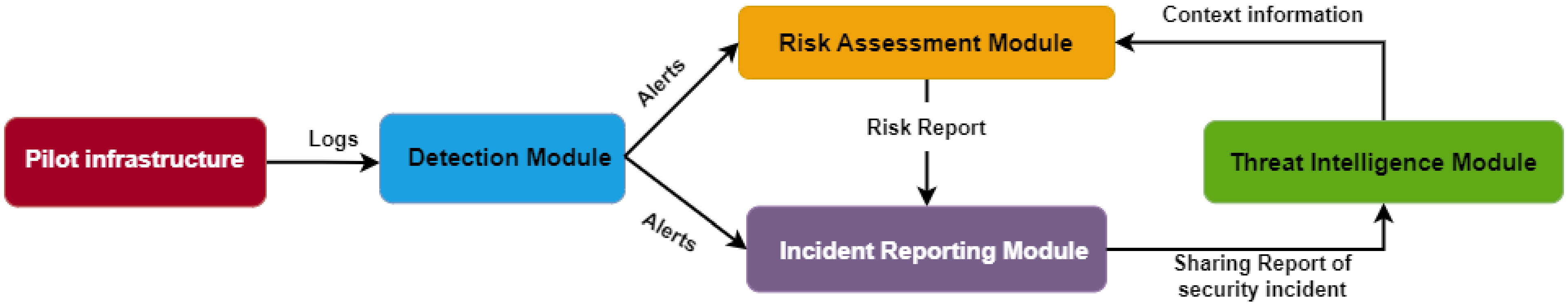
CPR Tool

- **Successful cyber attacks against key cyber physical assets**
  - Introducing AI and ML techniques for more **sophisticated detection**
  - Bidirectional **sharing** of information about relevant cyber incidents with the **community** (**threat intelligence**)
  - Moving a step forward concerning **cyber physical risk evaluation**
    - Traditional evaluation is done combining information about the **company´s business profile** and ongoing **cyber incidents** in **company´s owned infrastructure**
    - New **physical risk indicators** are introduced: outages, sickness of employees, scarcity of chips…
  - **Notifying** the authorities in **compliance** with new **legislation** by developing a new tool that **partially automates** the process of notification

CPR Tool (II)

- **AI Detection Module**
  - State Of The Art technology powered by XLAB
- **Risk Assessment Module**
  - Qualitative & Quantitative measurements
  - Interconnection between cyber and physical indicators
- **Threat Intelligence Module**
  - Raising context-awareness for CI operators
- **Incident Reporting Module**
  - Automated reports to national authorities

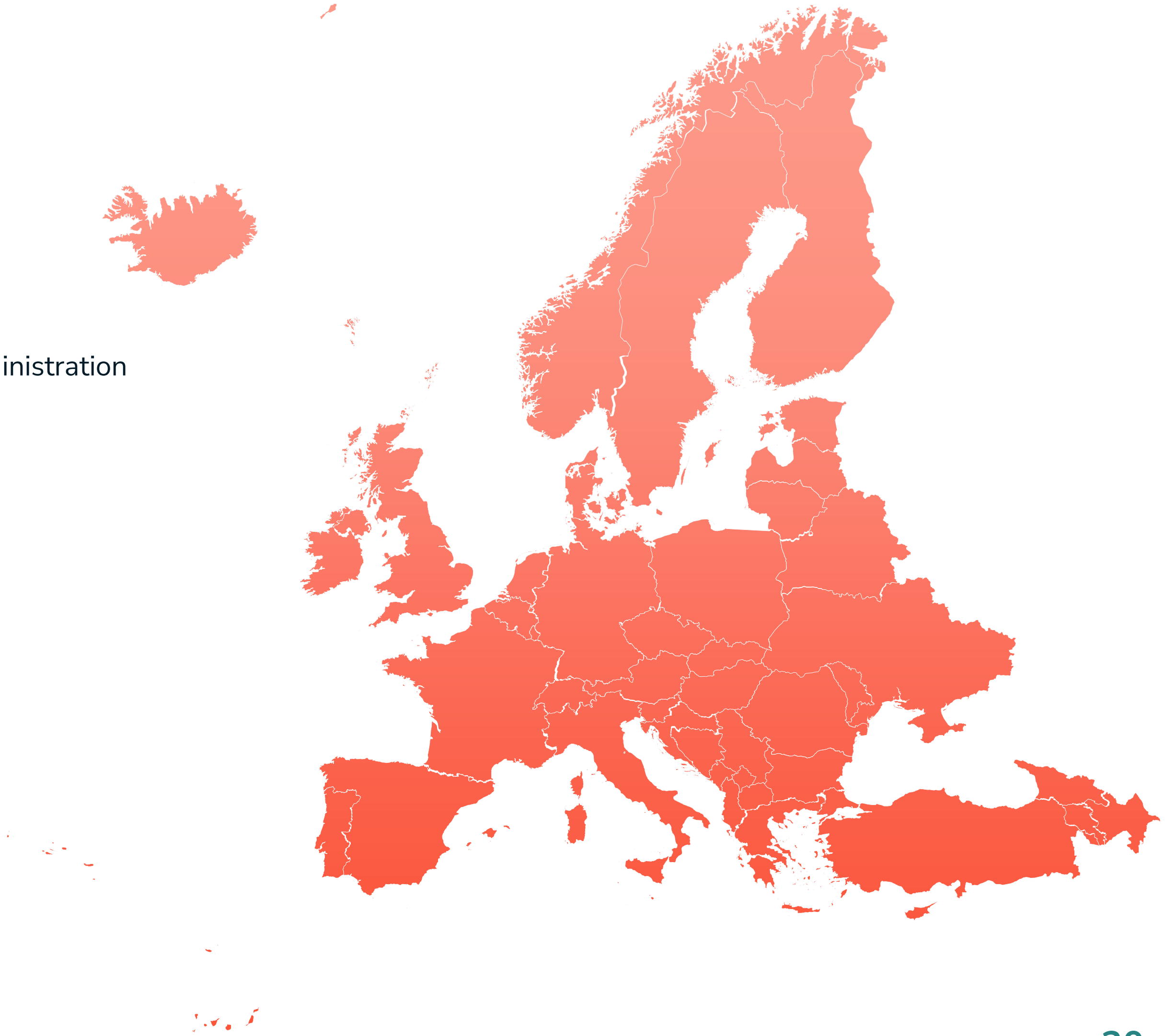
CPR Tool Architecture



SUNRISE Pilots

SUNRISE Pilots

- **18 pilots in 8 different countries**
  - Most pilots are in ES, IT and SI, defined as strategic national clusters
  - There are some others in FR, EE, RS, IL and CZ
  - Represented sectors: Health, Digital, Energy, Transport, Water and Public Administration
- **Participation of National Ministries**
  - Internal Affairs in ES
  - Infrastructures in SI
- **Participation of Regional Government:** Friuli Venezia Giulia in IT
- **Participation of Municipality:** Jerusalem in IL



SUNRISE Pilots (II)

- Pilots run in yearly iterations: TRL 5 (Y1), TRL 6 (Y2), TRL 7 (Y3)
- Each pilot is focused on a specific tool
- The strategic plans and the results of collaboration in terms of alignment of business continuity plans have their own pilots, too

SUNRISE

Thank you for your time

Any Questions?

This project has received funding from the European Union’s Horizon Europe research and innovation programme under Grant Agreement No. 101073821

The material presented and views expressed here are the responsibility of the author(s) only. The EU Commission takes no responsibility for any use made of the information set out.

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

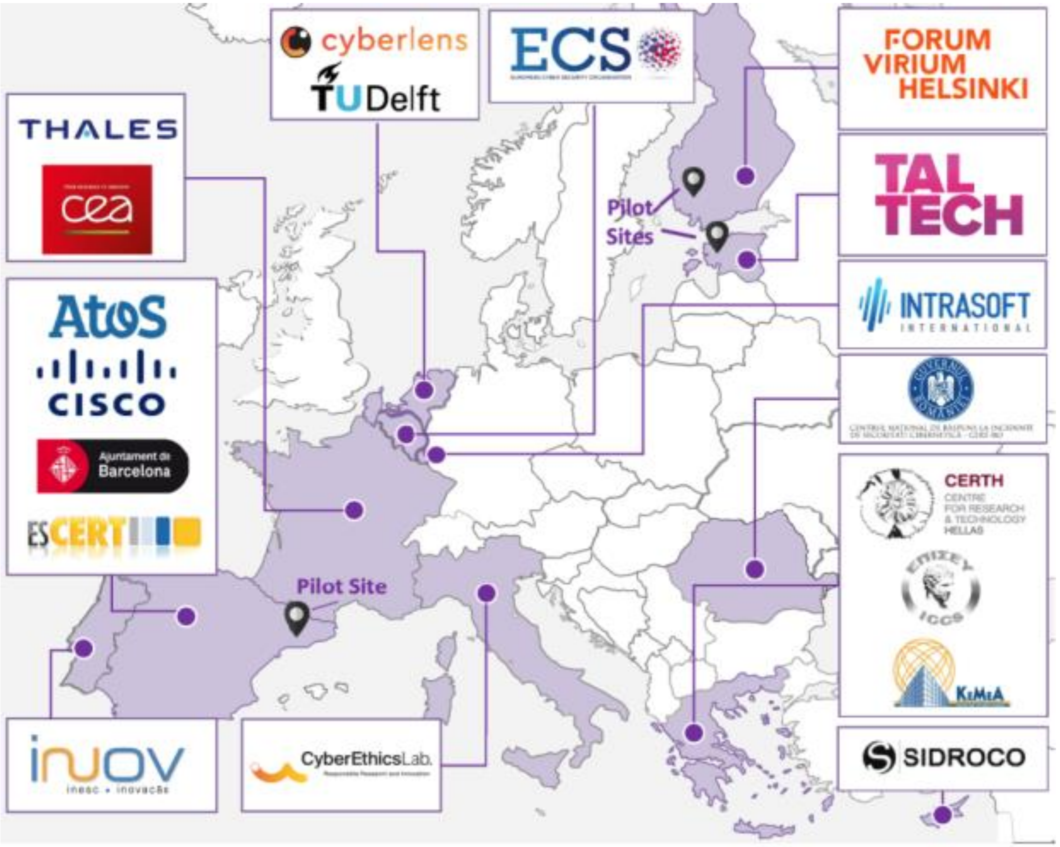
E-mail: sofia.tsekeridou@netcompany.com

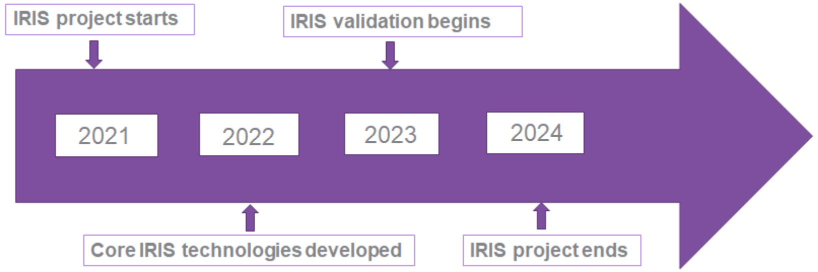
EU-CIP Project & ECSCI Cluster 1st Annual Conference on Critical Infrastructure Resilience: “Reinventing European resilience”

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.**

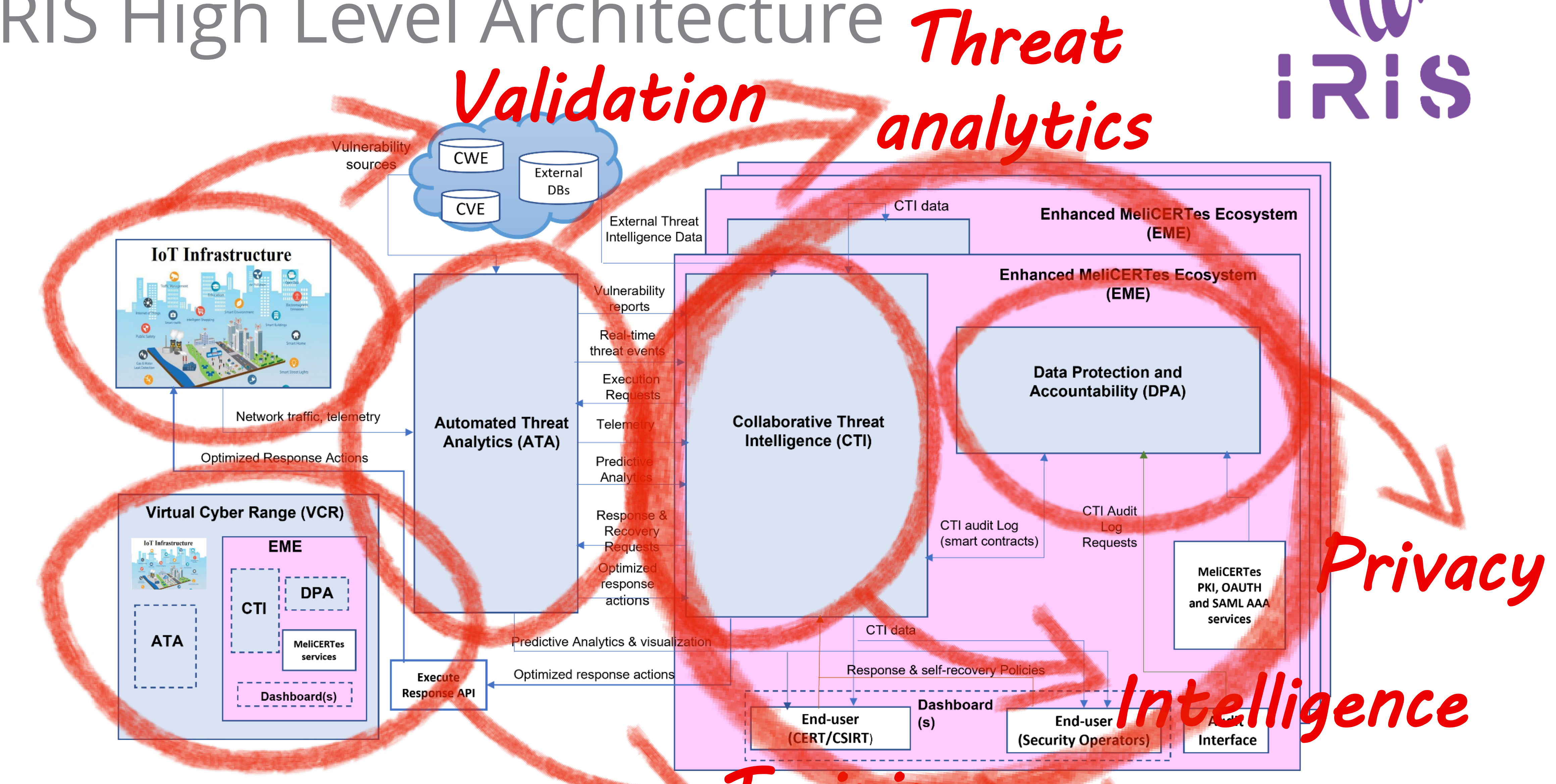
Complement the existing MeliCERTes open platform and tools.

melicertes

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

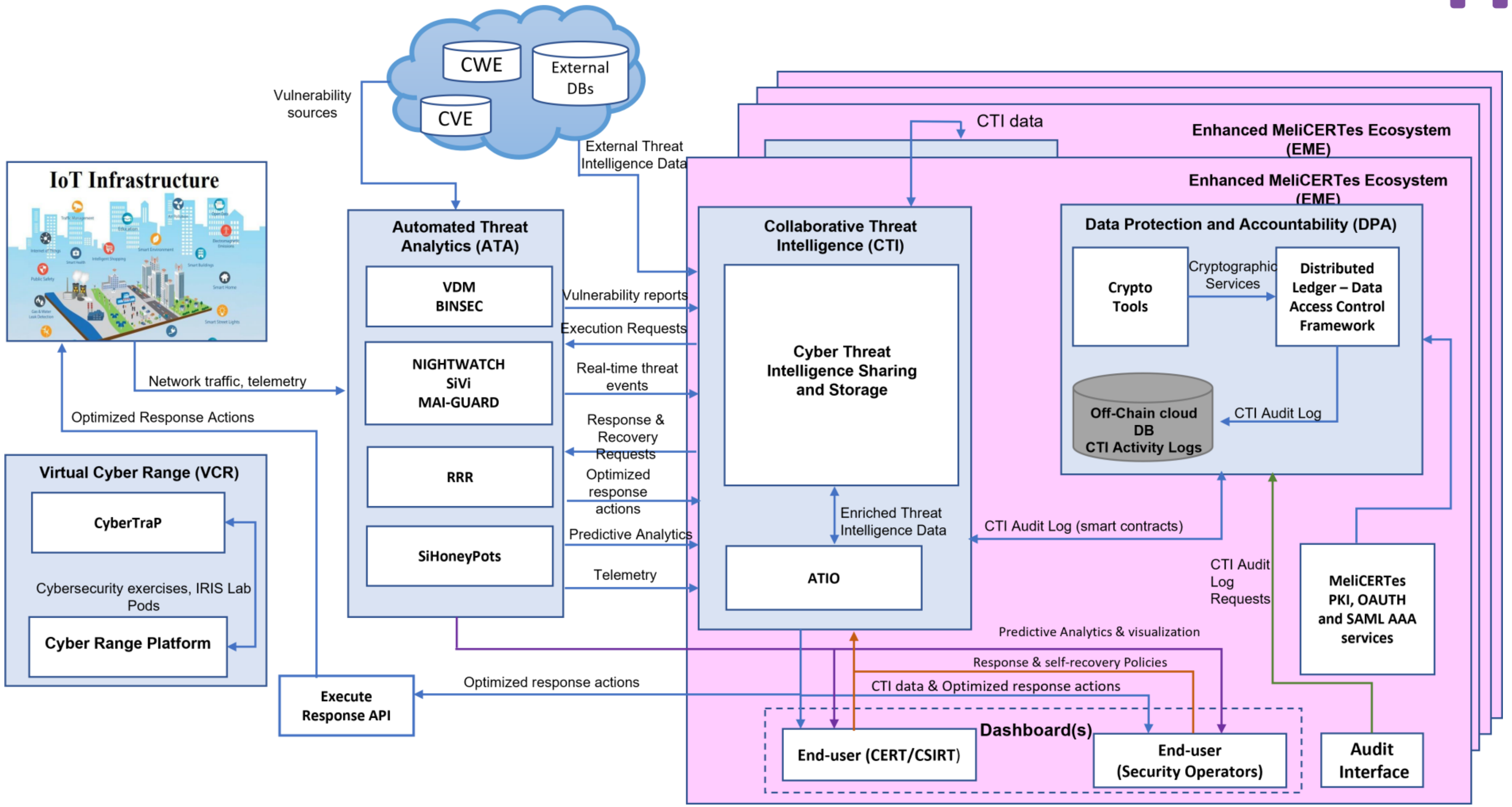
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727. This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

IRIS High Level Architecture


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

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
Virtual Cyber Range (VCR)
CyberTraP
Cybersecurity exercises, IRIS Lab Pods
Cyber Range Platform
Execute Response API
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
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

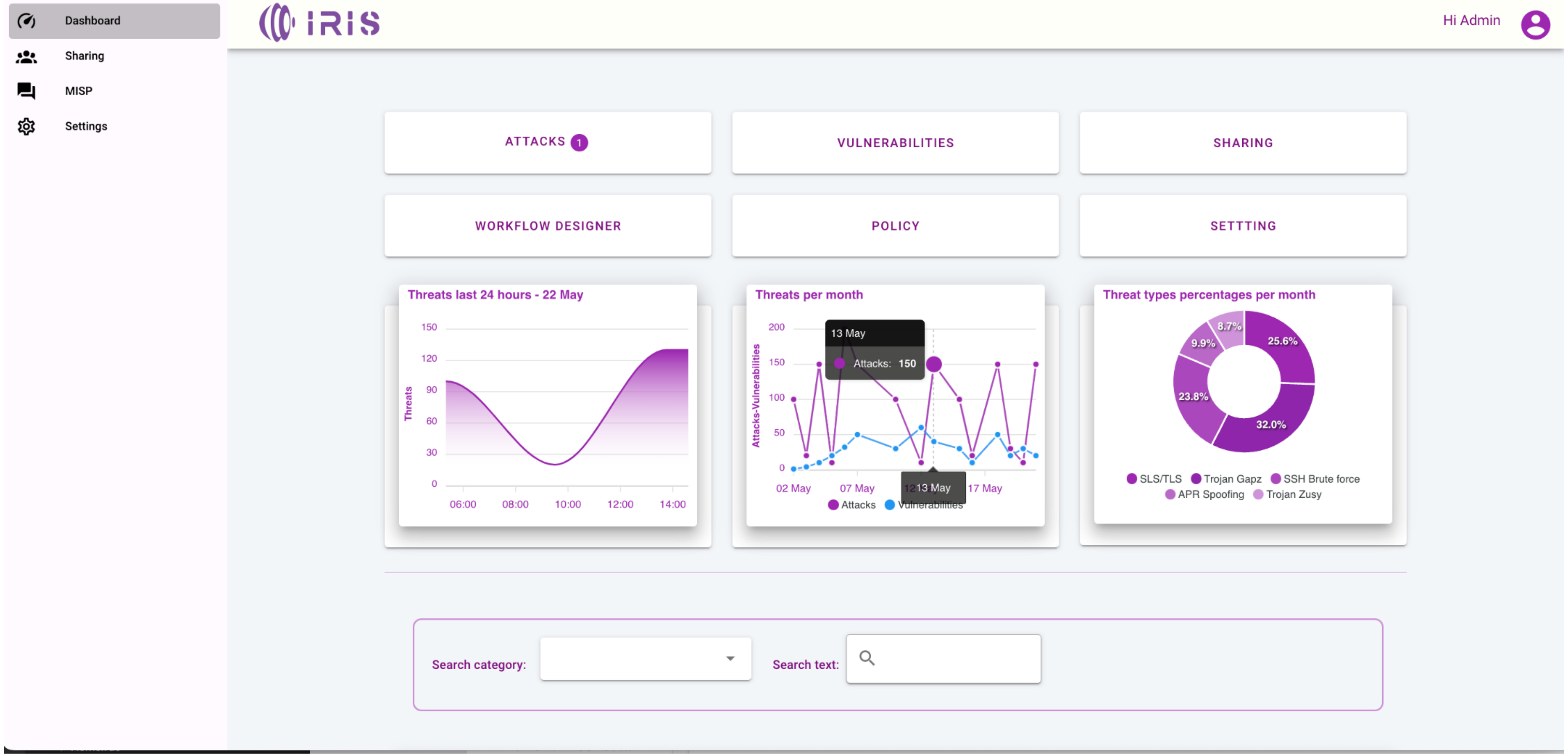
This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 101021727. This material reflects only the authors’ view and European Commission is not responsible for any use that may be made of the information it contains.

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.

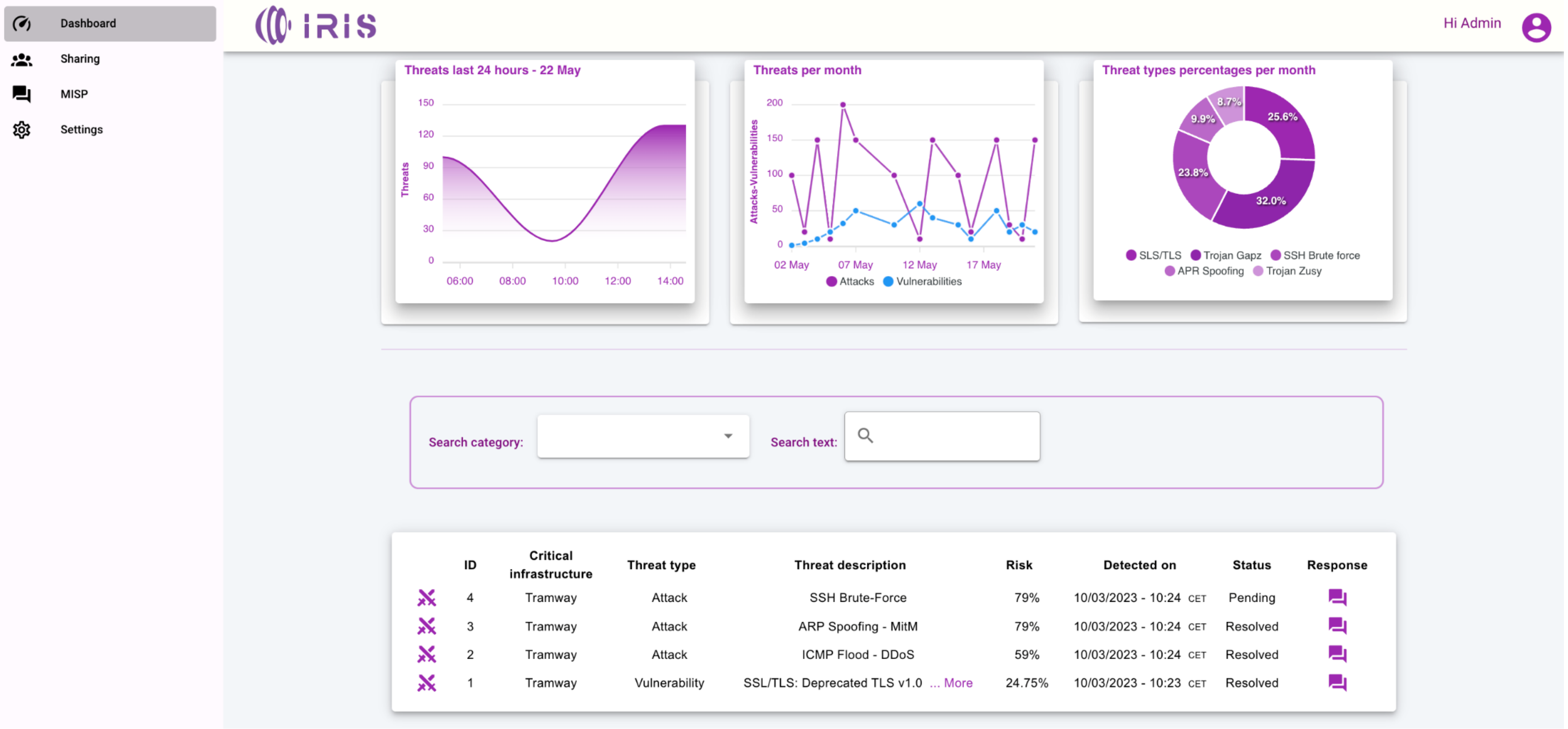
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727. This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

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



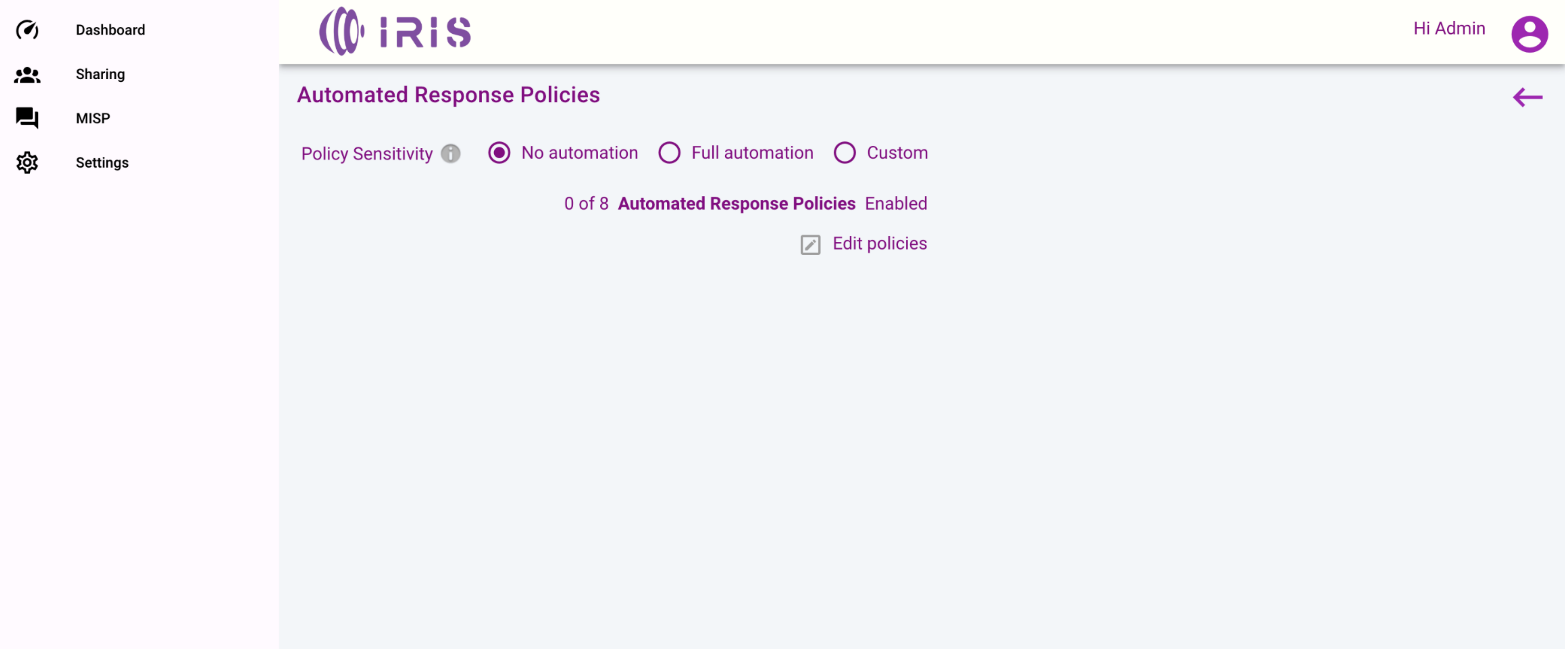
Search category:

Search text:

	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

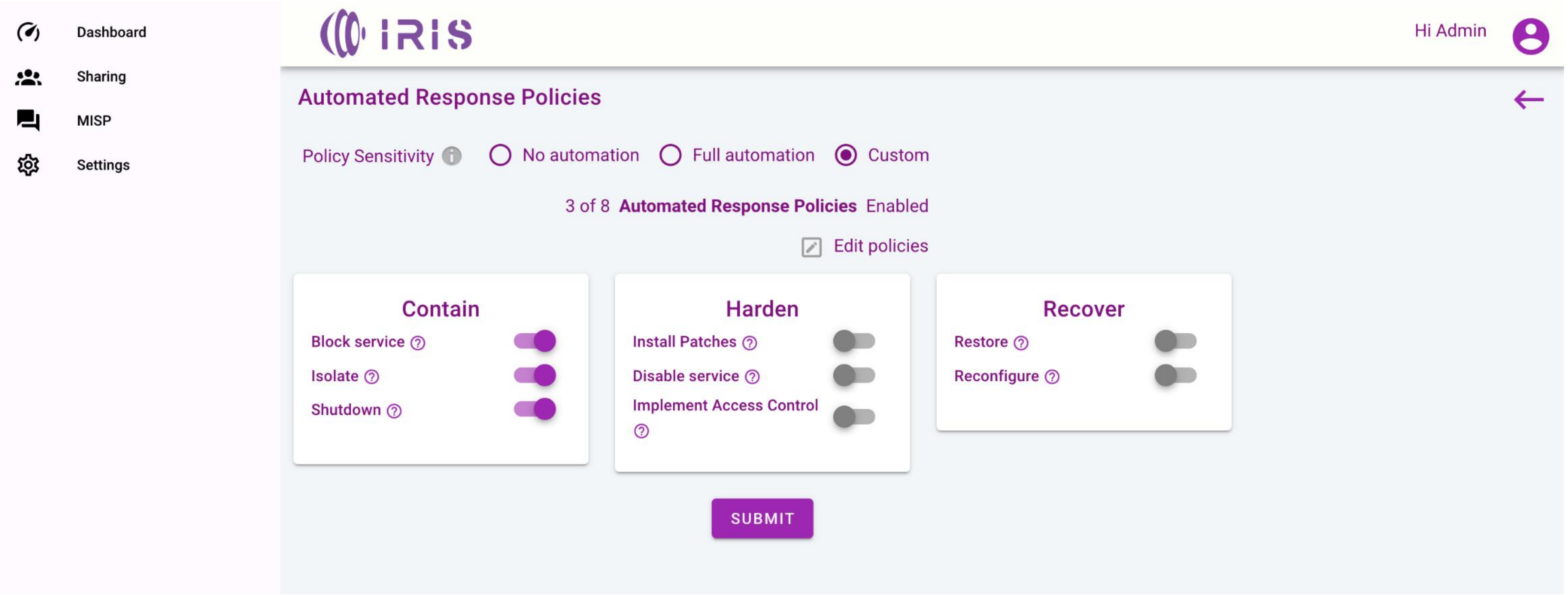
Policy Sensitivity ● No automation ○ Full automation ○ Custom

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

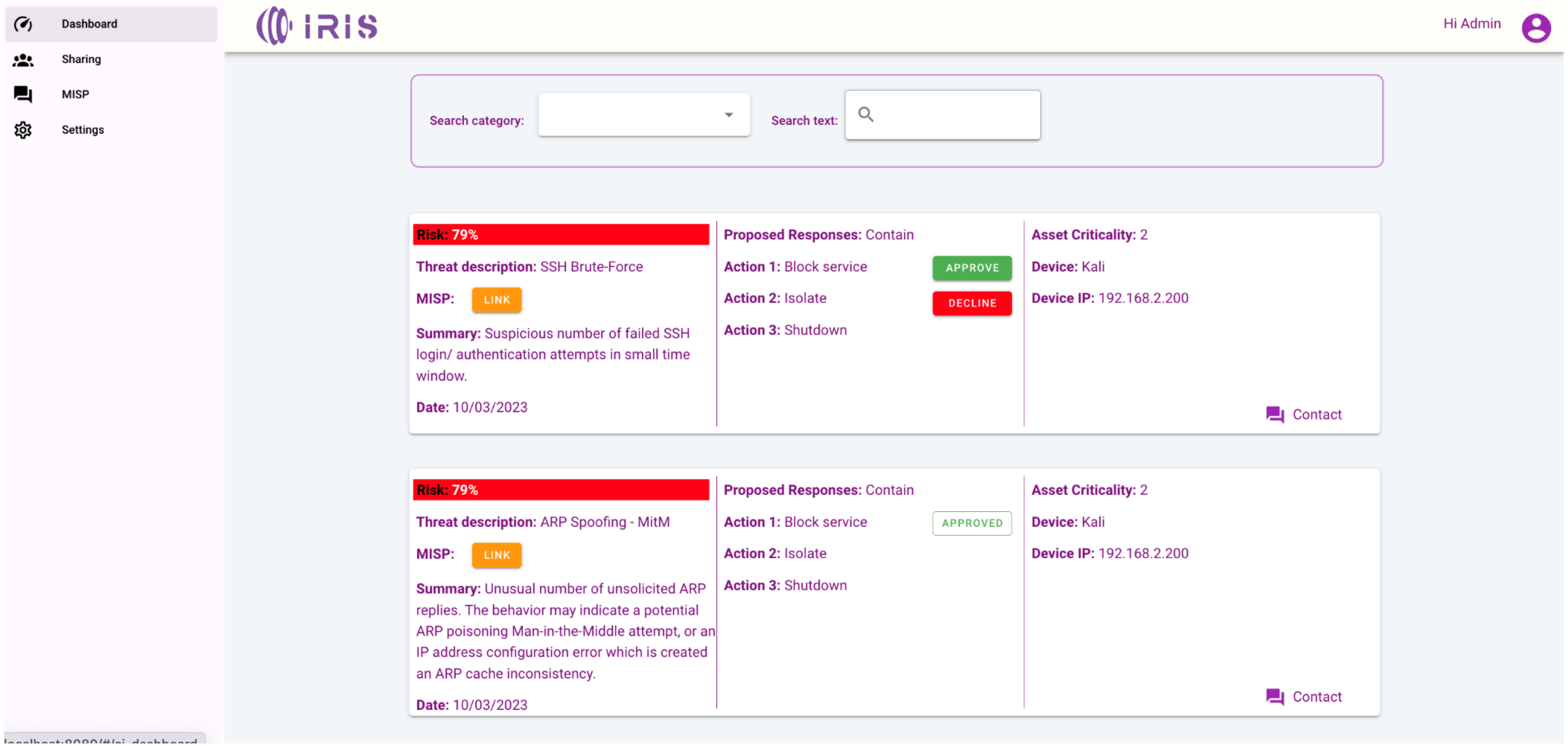
Recover

- 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



Search category:

Search text:

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

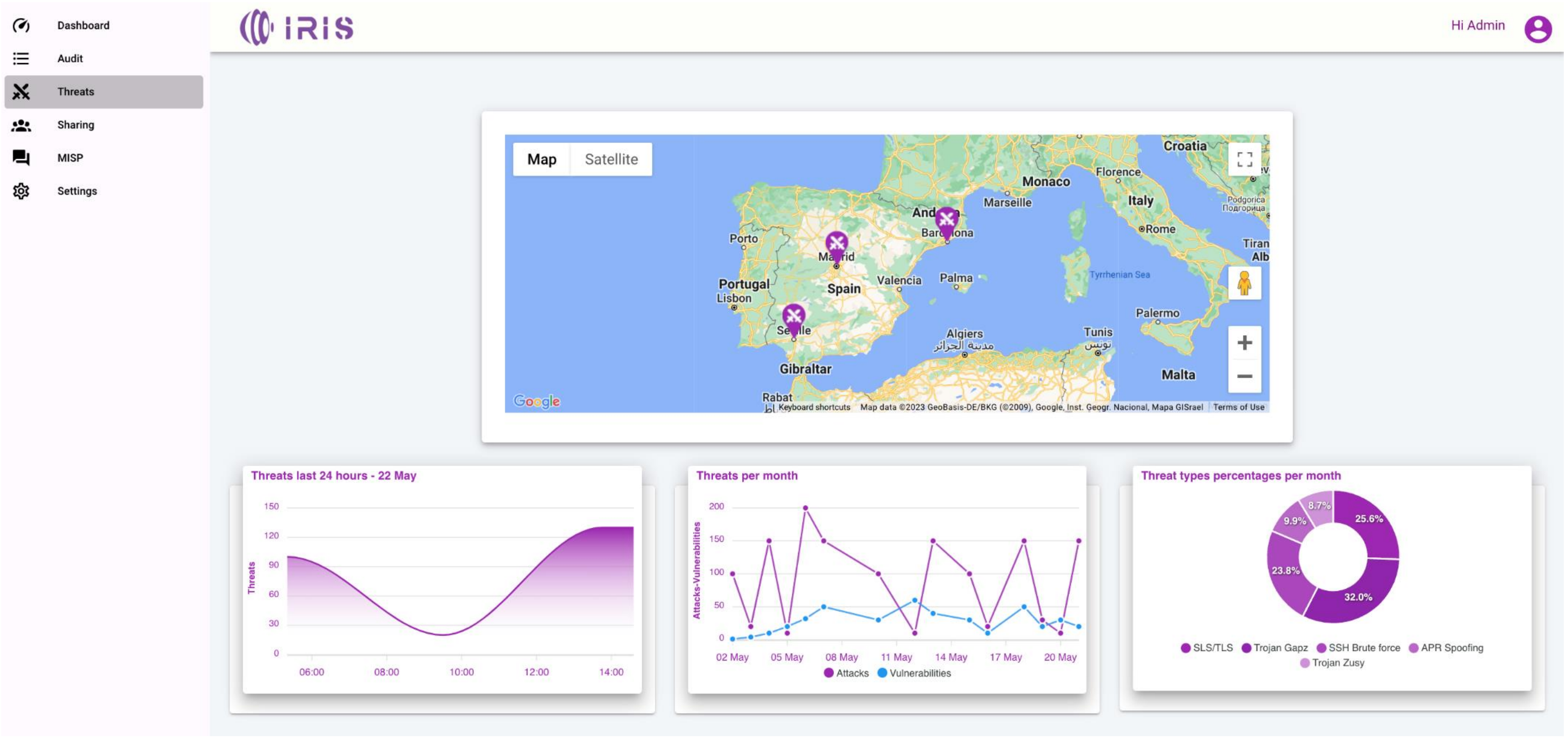
Asset Criticality: 2

Device: Kali

Device IP: 192.168.2.200

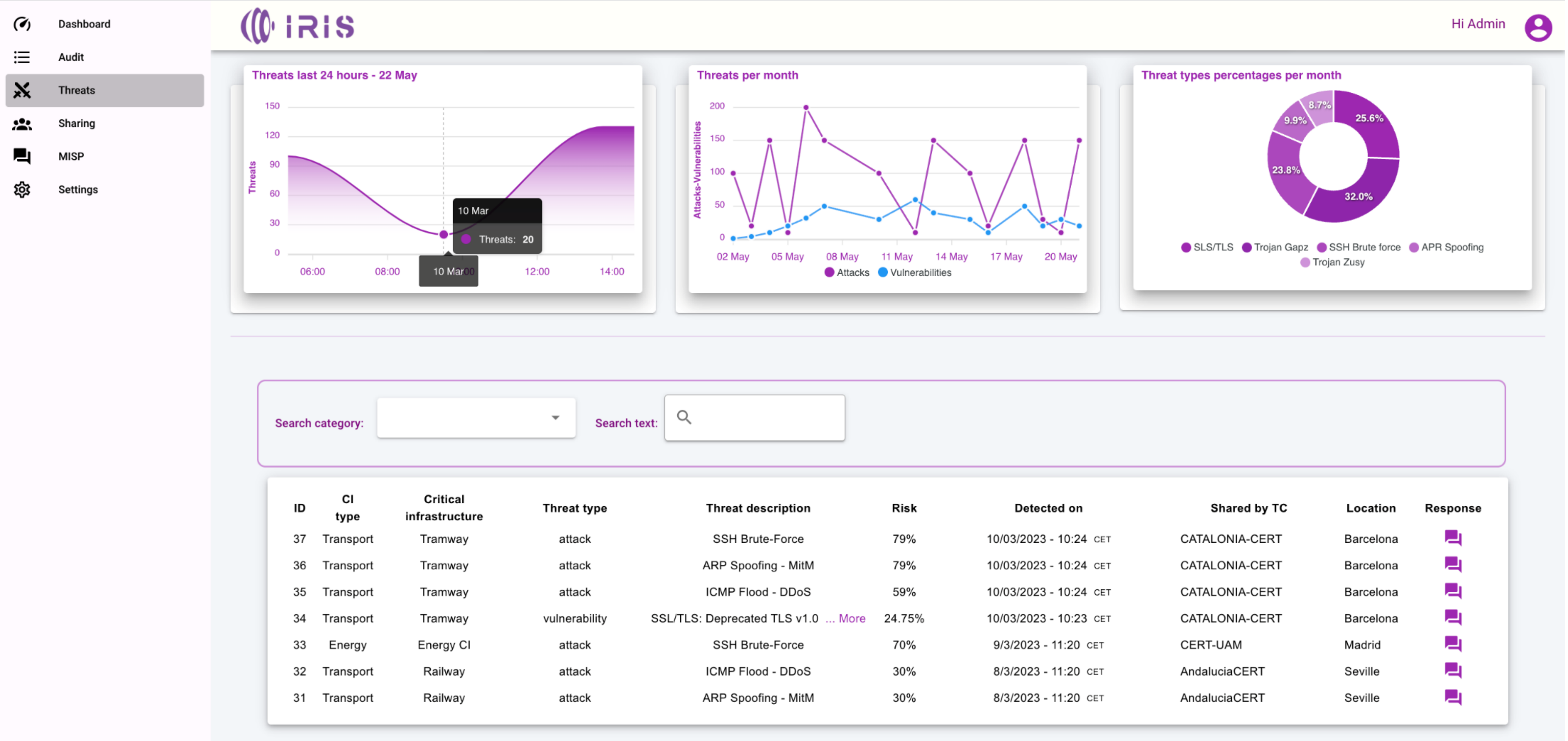
This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 101021727. This material reflects only the authors’ view and European Commission is not responsible for any use that may be made of the information it contains.

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

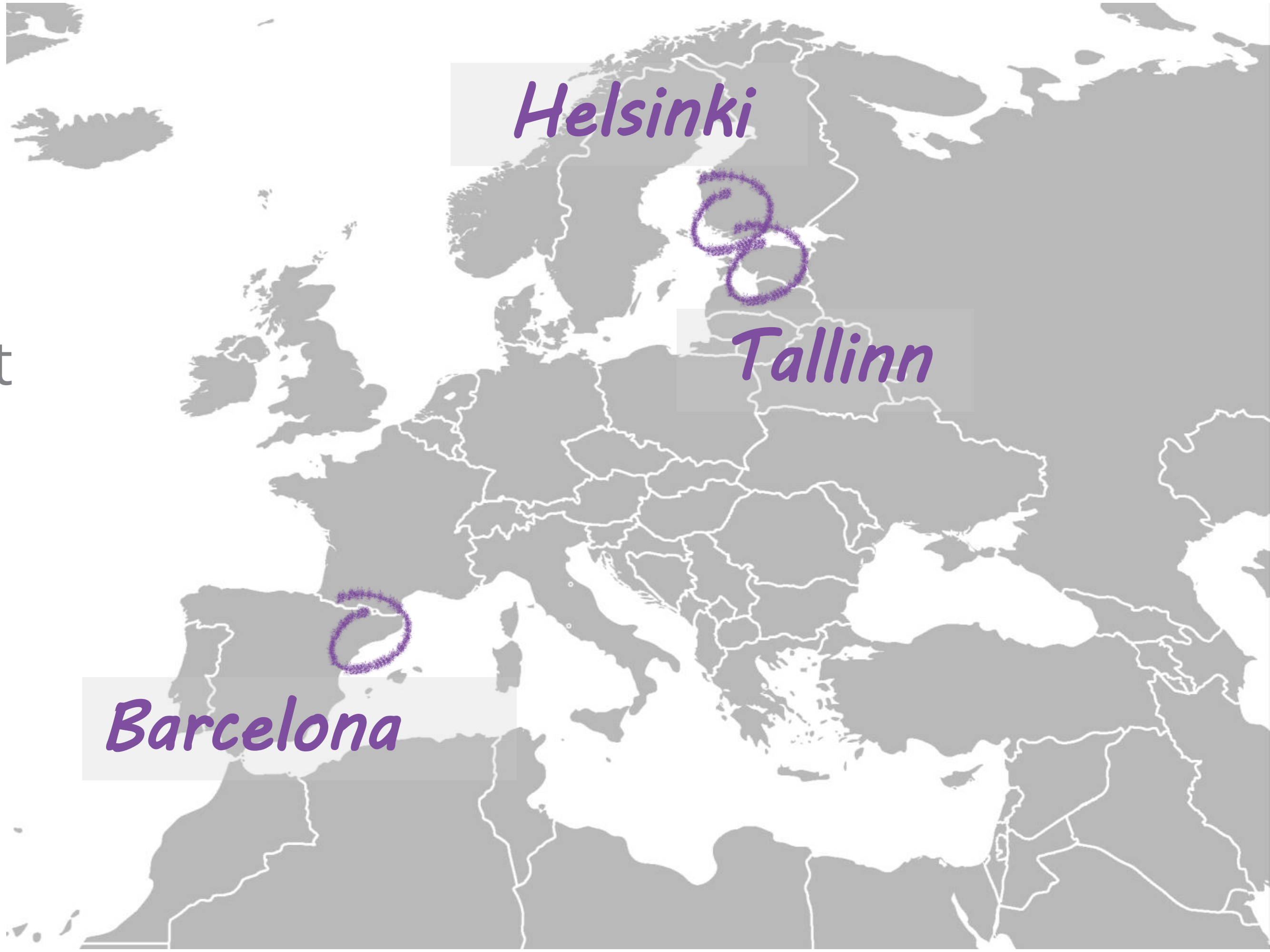
With the goal of

Identifying business requirements

Demonstrating the **AI driven** threat detection

Providing a collaborative european threat reporting environment

of the **IRIS** platform



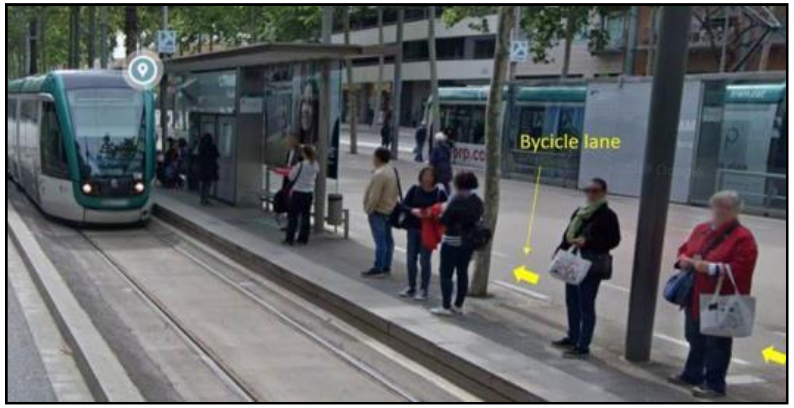
This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 101021727. This material reflects only the authors’ view and European Commission is not responsible for any use that may be made of the information it contains.

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.

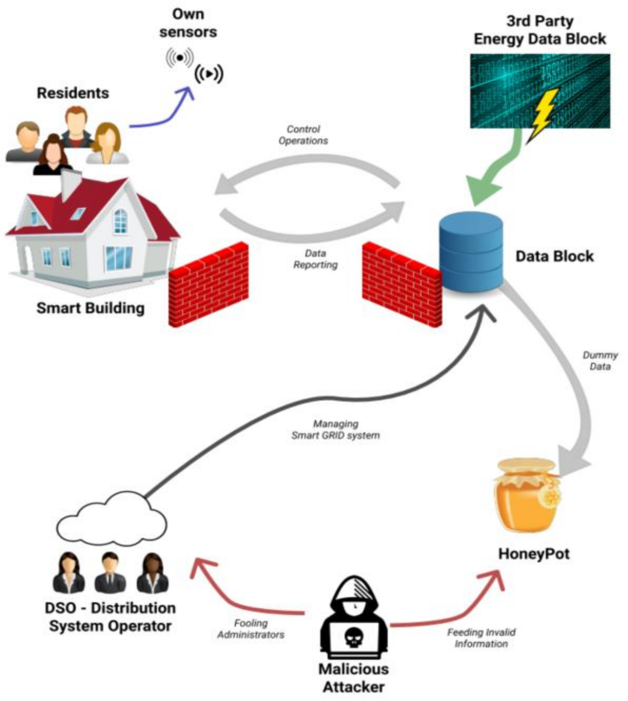
FinEst Centre
for Smart Cities

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.

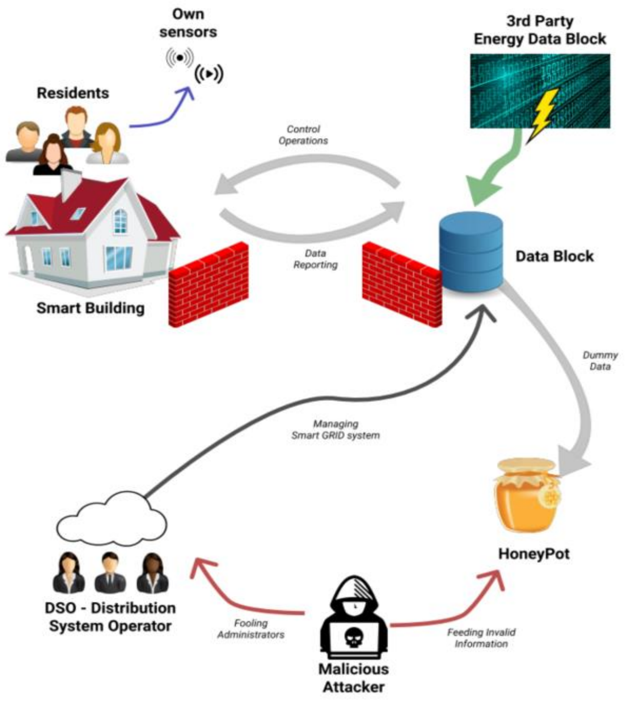


This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727. This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

Helsinki pilot

Goals and Challenges:

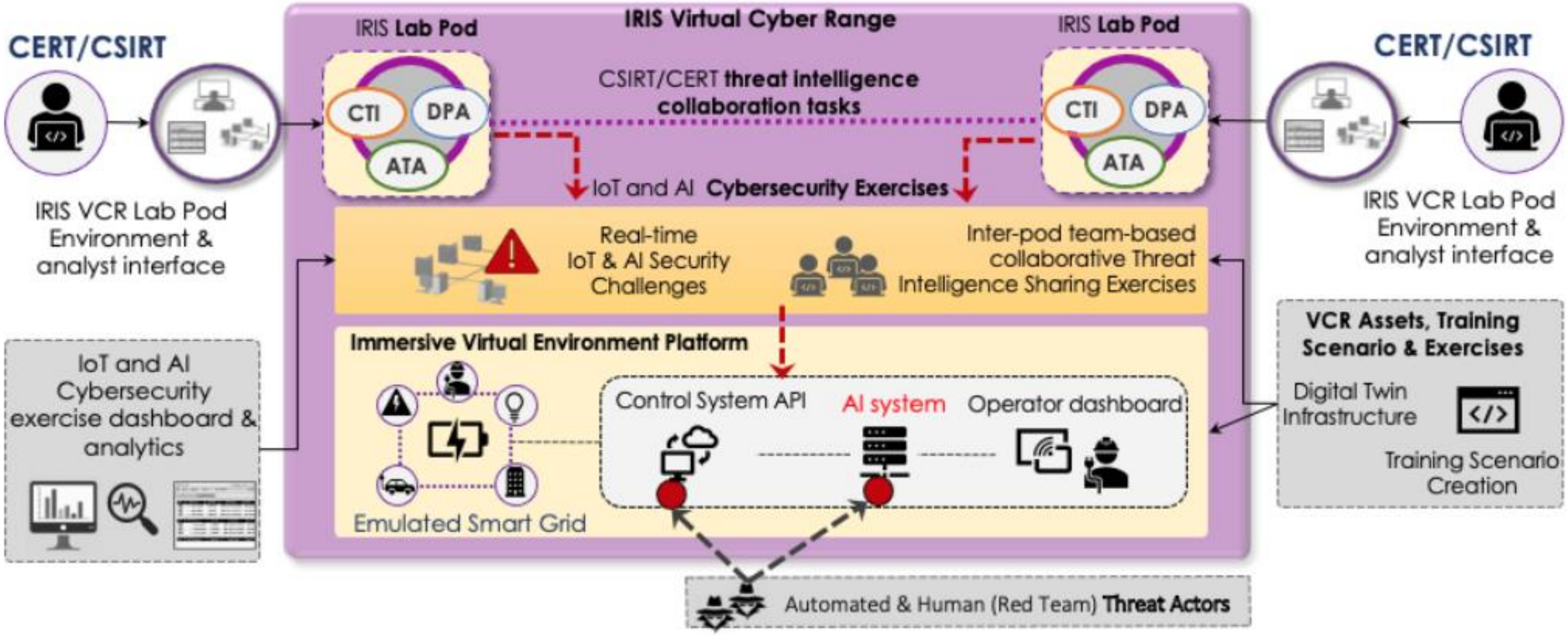
- Effective incident response and threat intelligence collaboration for cross-border smart grid threats
- Secure customer-facing components:
  - ✓Against threats to control functions defined for the demand control
- Secure APIs:
  - ✓Smart Grid API from Kalasatama (district of Helsinki)
  - ✓Smart Grid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

Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

CybAlliance
Healthcare Security & Privacy

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

CybAlliance (International Alliance for Strengthening Cybersecurity and Privacy in Healthcare): Norway, Germany, France and USA Partnership

Sandeep Pirbhulal

Brussels

20/09/2023

CybAlliance Introduction

- **Project Manger:** Sandeep Pirbhulal, Senior Researcher, NR
- **Duration:** 01.03.2023-29.02.2028
- **Project Owner:** Norwegian Computing Center/ Norsk Regnesentral
- **Total Project Amount:** 12.5 MNoK
  - 10 MNok from “Research Council of Norway (NFR)” (approx. 1MEuros)
  - 2.5 MNok from “Own Funding”
- **Partner Countries:** Norway, Germany, France and USA

CybAlliance Partners

- Norwegian Computing Center (NR, Norway)
- Norwegian University of Science and Technology (NTNU, Norway)
- Oslo University Hospital (OUS, Norway)
- University of Colorado Springs (UCCS, USA)
- Telecom SudParis (IMT, France)
- Goethe University Frankfurt (GUF, Germany)

INTPART Call Purpose

- INTPART International Partnerships for Excellent Education, Research and Innovation
- Long-Term Goal:
  - Research and Higher Education and efforts to develop more world-leading academic environments in Norway and partner countries
- Secondary Goals:
  - Long-term international partnerships that enhance the quality of higher education and research in Norway.
  - Strong links between higher education and research within the frameworks of the partnerships.
  - Cooperation with the business and public sectors to enhance quality and relevance within the frameworks of the partnerships, where relevant.

https://www.forskningsradet.no/utlysninger/2022/intpart-internasjonale-partnerskap/

CybAlliance Vision

CybAlliance establishes **dynamic collaboration** between research **institutes, universities, and hospitals** for excellent education, research, and innovation activities to offer efficient security and privacy solutions by observing real-world challenges of the **Norwegian and Global health sector**.

To strengthen the existing **collaboration between relevant national and international partners** of the **ASCERT** (AI-Based Scenario Management for Cyber Range Training) and **SFI NORCICS** (Norwegian Centre for Cybersecurity in Critical Sectors) projects.

Research Cooperation

Mobility: To plan the mobility plans of students, researchers, and staff at international institutions

CybAlliance will organize **24 mobility stays** of approx. one month time each, i.e., six for each NR and NTNU, and three for each OUS, IMT, UCCS and GUF

Annual Industrial workshop: To organize an annual workshop or webinar, so researchers can meet and discuss the strengths and opportunities of the cybersecurity and privacy in the telecare domain.

Annual open seminar: To provide an opportunity to discuss outcomes of the project with interested industry or academic personnel who are not part of the consortium

CybAlliance Supporting workshops

- CybAlliance Supporting workshops:
  - **CPS4CIP 2023 -** The 4th International Workshop on Cyber-Physical Security for Critical Infrastructures Protection co-located with ESORICS 2023
  - **SecAssure 2023 -** The 2nd International Workshop on System Security Assurance co-located with ESORICS 2023
  - **SecIndustry 2023 -** The 2nd Workshop on Cybersecurity in Industry 4.0 with ARES 2023
  - **CANTATA 2023 -** Cyber threAt huNTing And inTelligence in heAlthcare co-located with IEEE TrustCom-2023

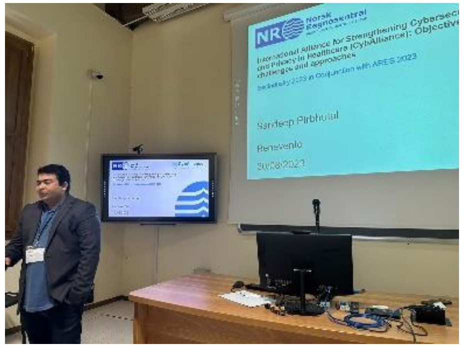
➢ The moral is to promote CybAlliance and increase its visibility and presence

CybAlliance
Healthcare Security & Privacy

SecIndustry 2023 in conjunction with ARES 2023: CybAlliance Suported Workshop

- **August 30, 2023:** University of Sannio Complesso Sant’Agostino via Giovanni De Nicastro, 13 82100 Benevento, Italy

ARES
conference
Availability • Reliability • Security


NR Norsk Regnesentral
International Alliance for Strengthening Cybersec
and Privacy in Healthcare (CybAlliance): Objective
challenges and approaches
SecIndustry 2023 in Conjunction with ARES 2023
Sandeep Pirbhulal
Benevento
30.08.2023

CybAlliance
Healthcare Security & Privacy

CybAlliance Open Seminar and Industrial Workshop

12-13 September 2023

Norsk Regnesentral (NR)/Norwegian Computing Center, Gaustadalléen 23A/B, 0373 Oslo, Norway

Day 1: 12th September 2023

Open Seminar on Strengthening Cybersecurity and Privacy in Healthcare

Objective: This Open Seminar on Strengthening Cybersecurity and Privacy in Healthcare aims to provide an open platform for national and international collaborators to meet, exchange knowledge, and facilitate discussions on the strengths and opportunities within the domain. Additionally, this seminar offers interested industry or academic professionals, who are not part of the CybAlliance project, the opportunity to actively participate and engage in discussions related to cybersecurity and privacy in healthcare. By bringing together diverse perspectives, this open seminar seeks to enhance collaboration, generate new insights, and contribute to the advancement of the field.

Target Audience: Partners + Invited Speakers + Open to all stakeholders (by registration)

Organized by NTNU

Day 2: 13th September 2023

Industrial Workshop on Cybersecurity in Digital Transformation of Healthcare and Resilient Infrastructures

Objectives: This industrial workshop aims to bring together industry practitioners and academics in a joint platform that provide an opportunity for sharing best practices, exchanging new ideas, networking, and identifying areas of collaboration related to cybersecurity in healthcare and resilient infrastructures.

This industrial workshop is supported through two Research Council of Norway (RCN)-funded INTPART projects: International Alliance for Strengthening Cybersecurity and Privacy in Healthcare (CybAlliance) and Reinforcing Competence in Cybersecurity of Critical Infrastructures: A Norway – US Partnership (RECYCIN).

Target Audience: CybAlliance and RECYCIN Partners + Invited Industry Guests (Only)

Organized by NR and IFE

CybAlliance flagship workshops

- **SUNRISE 2023** - SecUre aNd Resilient digItal tranSformation of healthcarE has been accepted by NIKT 2023
- Website has been created: https://cyballiance.nr.no/sunrise-2023/
- Deadline:22nd September 2023

Education

- **Summer schools:** Two summer schools will be organized, i) Cybersecurity Solutions for Healthcare Applications, and ii) Privacy-preserving for Health Information Systems

- **Joint supervision:** Discuss opportunities for joint supervising of master's and PhD students
  - CybAlliance will involve around 40 core participants across national and international partners, and total of 40-48 students (each MS/PhD awarding universities will invite other partners to co-supervise 2-3 students each year)

- **Guest lectures and tutorials:** Organize guest lectures and tutorials for students on critical infrastructure security, information security, dynamic risk management, privacy preserving

- **Course material:** Developing education courses on securing healthcare for specialist workforce development

Innovation Activities

1

Experience sharing: To share acquired knowledge from open seminars, summer schools, and mobility activities

2

Project proposal Ideas: Discussion of innovative research ideas to resolve current and future challenges

3

Sustainability planning: Collaborate with dissemination stakeholders for developing further strategies to ensure long-term sustainability

Digital Twin for Enhancing Security and Resilience

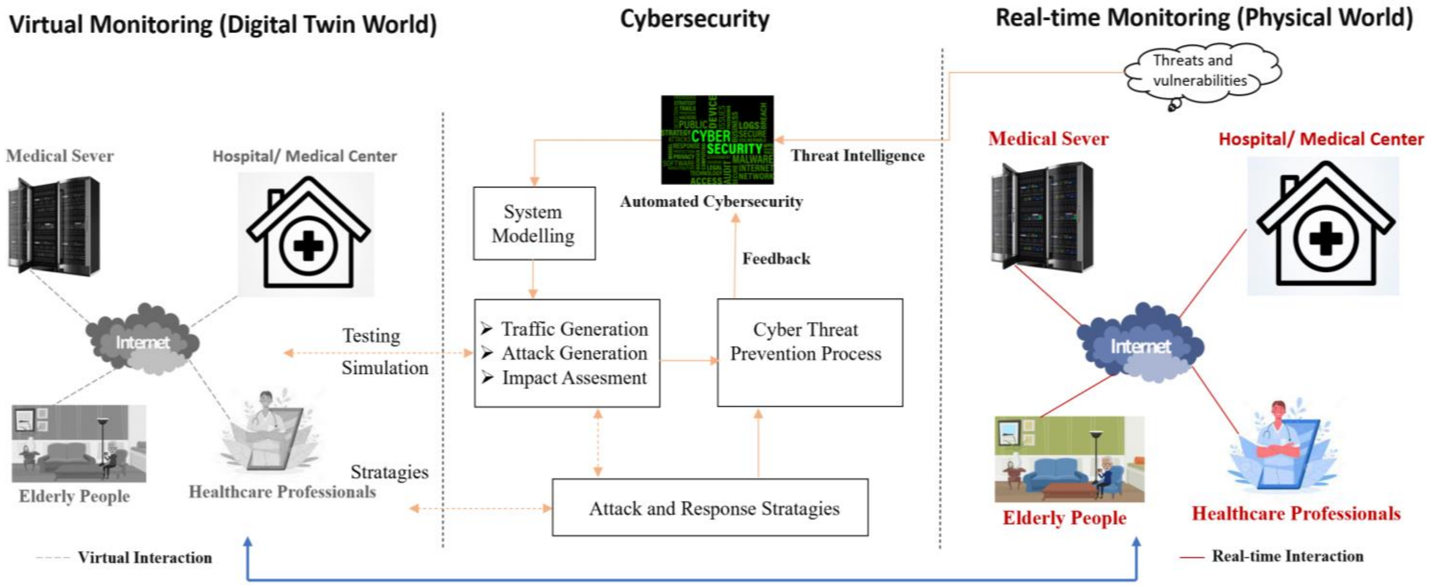
Following features of Digital Twin are useful for enhancing cybersecurity and resileince

- Improves the understanding of cyber attacks
- Gives a continuous overview of vulnerabilities, threat landscape, attack space, and mitigate them before they happen
- Allows the design of new prevention, detection, and response methods without disturbing physical world

DT facilitates toward adaptive resilience which is one of the key concerns for protecting critical sectors

Innovation Project (1/3)

- Digital Twin for Secure Smart Care: Towards Adaptive Resilience

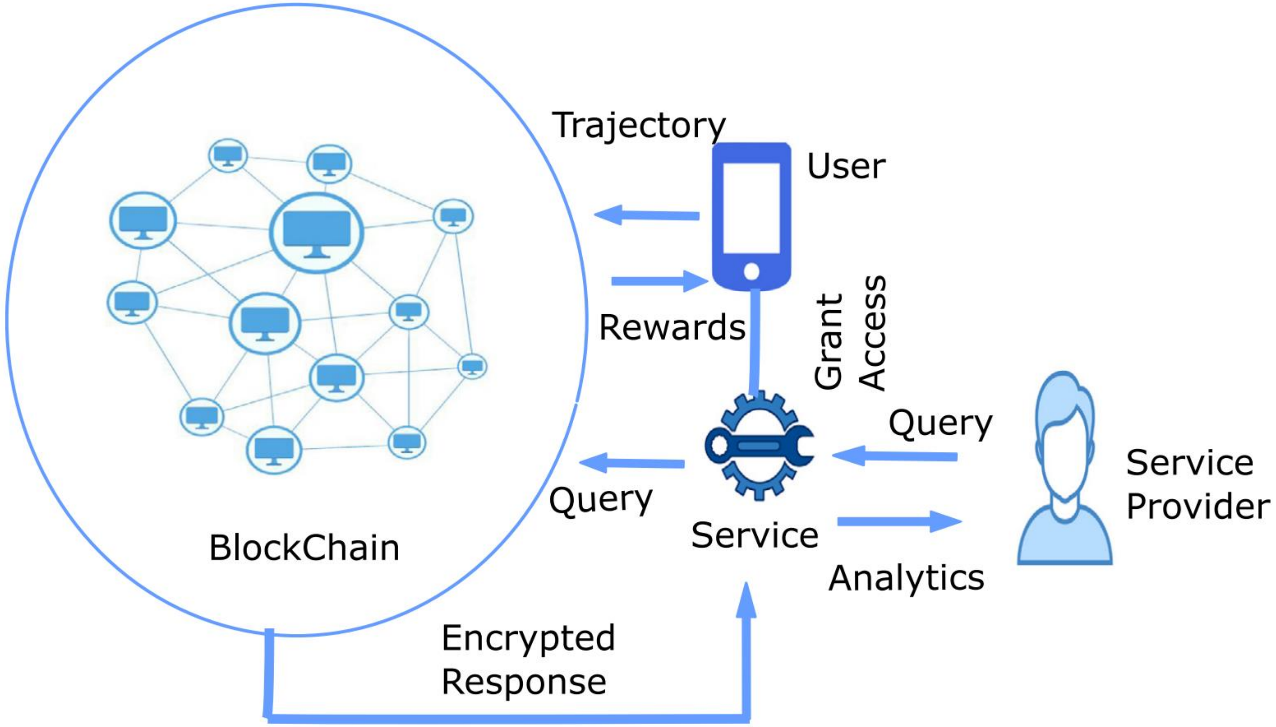


Sandeep Pirbhulal, Habtamu Abie, Ankur Shukla: Towards a Novel Framework for Reinforcing Cybersecurity using Digital Twins in IoT-based Healthcare Applications, 95th IEEE Vehicular Technology Conference, 2022

Inovation Project (2/3)

Decentralized Trust Management in Modern Healthcare Sytems

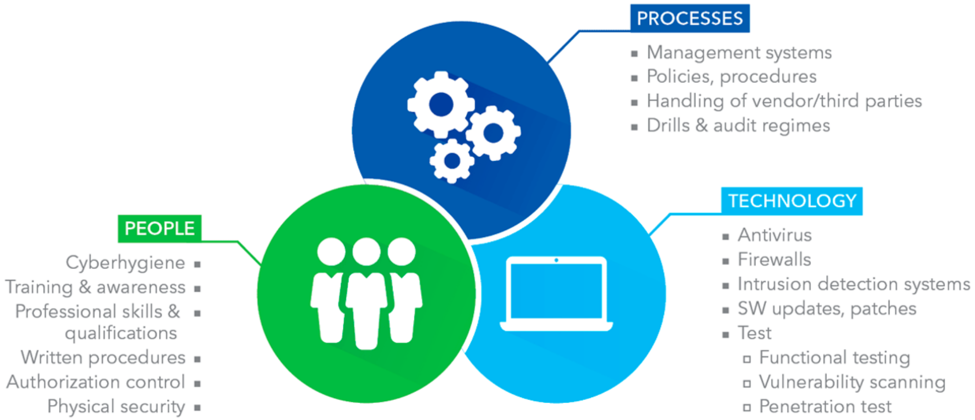
Decentralized communication accelerate the decision-making process hence play huge role for resilient infrastructures



Talat, R., Obaidat, M. S., Muzammal, M., Sodhro, A. H., Luo, Z., & Pirbhulal, S. (2020). A decentralised approach to privacy preserving trajectory mining. *Future generation computer systems*, *102*, 382-392.

Inovation Project (2/3)

➢ Human-Centered Artificial Intelligence for CyberSecurity and Resilience



https://quadrant360.com/blog/are-humans-the-weakest-link-in-cyber-security/

The synergy between people, processes and technology for secure and resilient infrastructures

Norway Health Tech

- Norway Health Tech has a vision of making Norway the world's best arena for health innovation. It is a non-for-profit member organization with close to **270 members** representing the full value chain of healthcare.

- Their main goal is to **improve the quality of treatment and care by industrializing healthcare solutions** in the global ecosystem.

- Collaborate with Health2B which results from a collaboration between Oslo University Hospital (OUS), Forskningsparken (Oslo Science Park) and Norway Health Tech

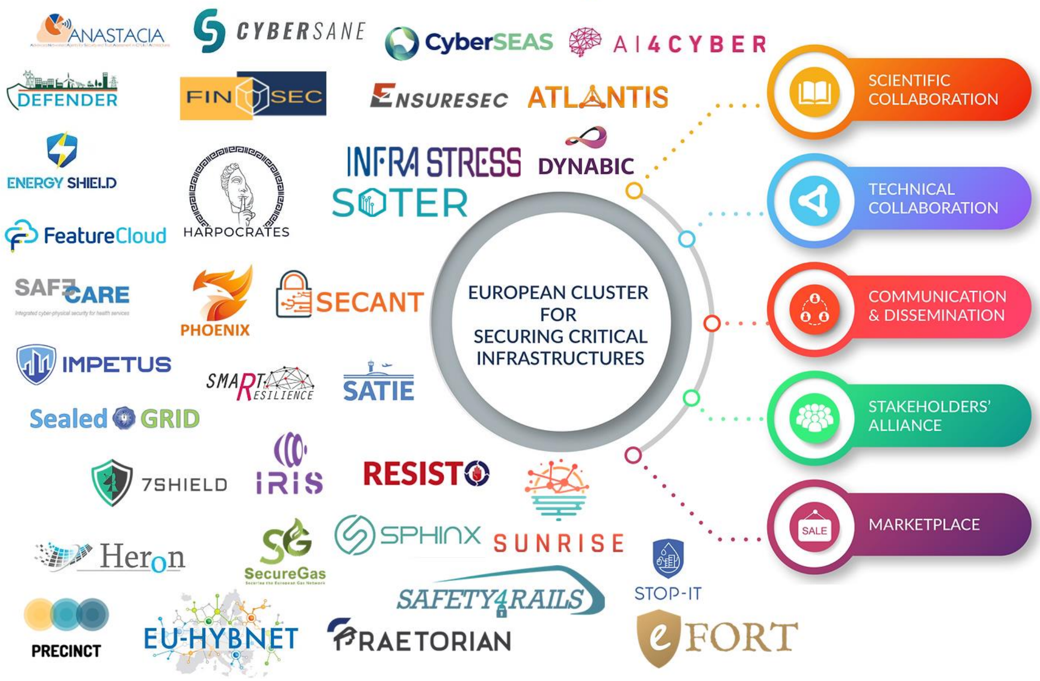
European Cluster for Securing Critical Infrastructures (ECSCI)

- NR coordinates and leads the ECSCI

- The main objective of the ECSCI cluster is to create synergies and **foster emerging disruptive solutions to security issues** via cross-projects collaboration and innovation

- Organize international conferences/workshops, **involving both policy makers, industry and academic, practitioners**, and representatives from the European Commission

ECSCI Cluster Members



New Dissemination Collaborator

Norwegian Ecosystem for Secure IT-OT Integration (NESIOT) brings together multiple stakeholders such as sensor/devices manufacturers, telecom operators, cloud and data analysis solution providers, industrial system operators etc., and to exploit enabling technologies and the secure application of those technologies.

NESIOT

https://www.ntnu.edu/norcics/it-ot-integration-nesiot

CybAlliance Collaboration for Research based Innovation

- Oslo Kommune
- VentureNet AS
- N-Abel AS
- SINTEF Digital
- Tellu (TelluCare)
- Salveo Solutions AS

- DNV Imatis
- IFE
- USN
- Health2B

Way Forward

- CybAlliance is open for collaboration to enhance excellence in healthcare security and privacy for education, research and innovation.
- Website: https://cyballiance.nr.no/
- Contact: Sandeep Pirbhulal (sandeep@nr.no)