Artificial Intelligence Threat Reporting & Incidence report system

IRIS in Resilience Standardisation & Policy Making

ECSCI SPM Workshop on Collaborative Standardisation and Policy Making
For Greater CI Resilience in Europe
5th Dec 2023

Dr. Sofia Tsekeridou, sofia.tsekeridou@netcompany.com

Senior Research and Innovation Manager – Expert

Netcompany - Intrasoft

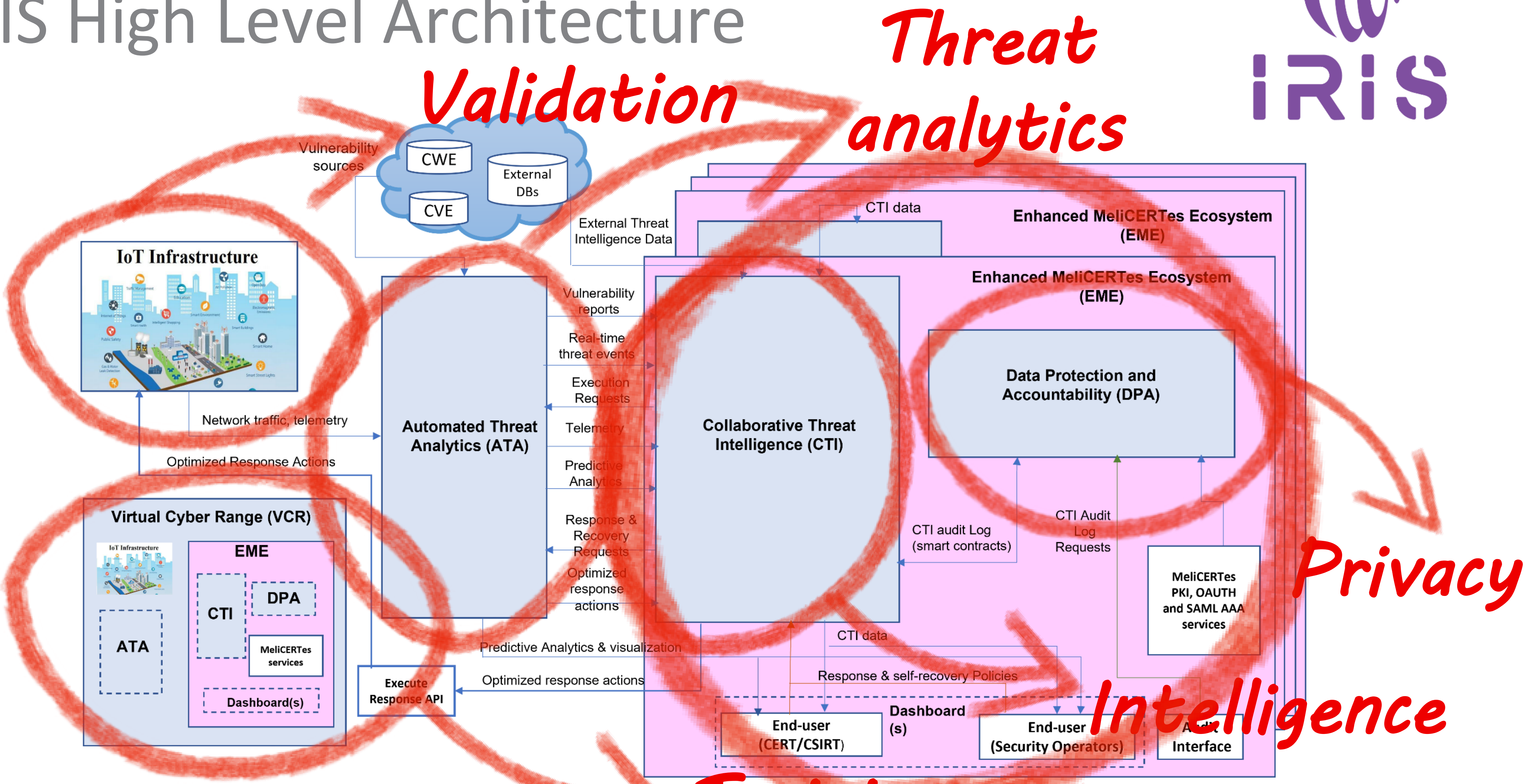
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

IRIS in a Nutshell

- **H2020 IRIS Project -** A collaborative CERT/CSIRT platform to combat cyber-threats in IoT and AI-driven systems – now in its **3rd year**
- 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.
- Aim:
  - ✓ Deliver a framework supporting **European CERTs/CSIRTs in close collaboration with CI Operators** to detect, share, respond and recover from **cybersecurity threats and vulnerabilities of IoT and AI-driven systems.**
- Focus is primarily on Cyber Resilience in Transport/Mobility and Energy Sectors

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
External Threat Intelligence Data
CTI data
Enhanced MeliCERTes Ecosystem (EME)
Enhanced MeliCERTes Ecosystem (EME)
IoT Infrastructure
Automated Threat Analytics (ATA)
Vulnerability reports
Real-time threat events
Execution Requests
Telemetry
Predictive Analytics
Response & Recovery Requests
Optimized response actions
Collaborative Threat Intelligence (CTI)
Data Protection and Accountability (DPA)
Network traffic, telemetry
Optimized Response Actions
Virtual Cyber Range (VCR)
IoT Infrastructure
EME
CTI
DPA
MeliCERTes services
ATA
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

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 Adoption of Relevant Standards

- **IRIS** capitalizes on **well-known cybersecurity standards** for **CTI information representation and sharing**, thus promoting and guaranteeing **interoperability**
  - ✓ CTI standard data format (**STIX v2.1**) **allowing CTI data to be shared in a consistent way across different systems**, guaranteeing **interoperability (cross-domain and cross-sector)**
    - ➢ The ability to convert from **MISP Objects (MISP standards) to STIX** and back is also provided
  - ✓ CERT/CSIRT authorities and CI Operators can leverage **CACAO playbooks** to establish **standardized, scalable, and consistently effective incident response procedures** for **common threats**.

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 Compliance to Policies/ Directives

- IRIS targets **regulatory compliance** and **alignment with current Policies/ Directives**
  - ✓ **NIS2 Directive**: IRIS addresses **wider range** of CI sectors (OESs), obligation to **report incidents** and **manage cybersecurity risks**, **collaboration among diverse stakeholders and information sharing**
  - ✓ **Critical Entities Resilience Directive** (CER): IRIS addresses obligation to **report incidents and define response procedures** in case of **cyber attacks to AI and IoT relevant components of the digital infrastructure of a smart city**, to ensure business continuity
  - ✓ **Cybersecurity Resilience Act** (CRA): IRIS adopts **DevSecOps**, incl. **security testing (SAST, DAST) to ensure cybersecurity resilience** of IRIS platform software

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 Standardised and Interoperable tools

- **MISP** threat and malware information sharing platform, led by CIRCL
  - ✓ Open-source threat intelligence platform providing effective threat intelligence, by sharing indicators of compromise.
    - ➢ collect enriched IRIS generated CTI data such as threats, attacks and vulnerabilities that are targeted to IoT and AI-driven ICT systems.
- **MeliCERTes v2** integrated in IRIS **Enhanced MeliCERTes Ecosystem**, supervised by ENISA
  - ✓ **Cerebrate**
  - ✓ **EME UI**
    - ➢ Incorporating IRIS web applications dashboards
    - ➢ Extended to include User Group of CI Operators
  - ✓ **MISP**
  - ✓ **INTEL MQ**
  - ✓ Keycloak
  - ✓ Mattermost & Big Blue Button

MISP Threat Sharing

melicertes

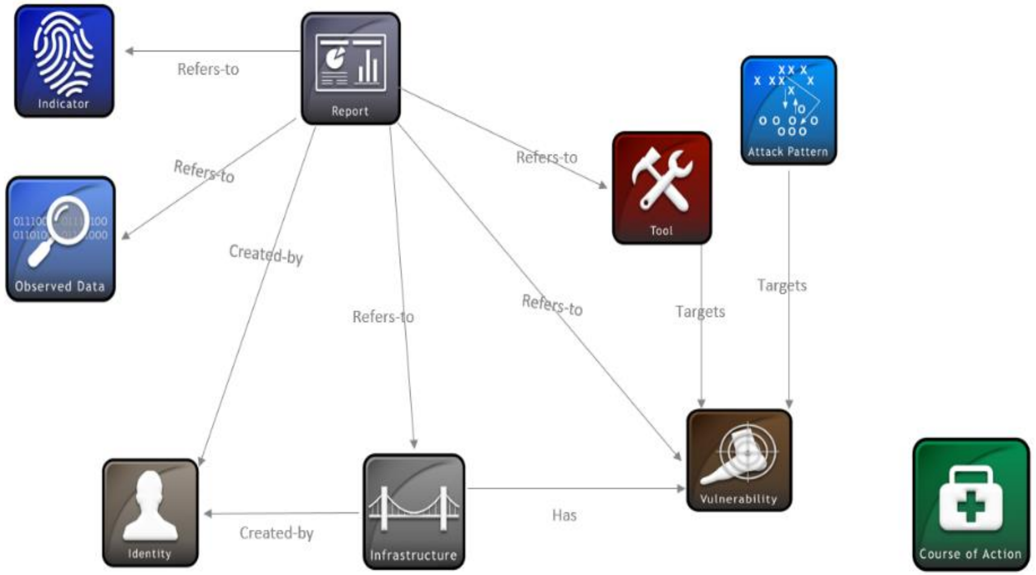
This project has been co-funded by "**Connecting Europe Facility – Cybersecurity Digital Service Infrastructure Maintenance and Evolution of Core Service Platform Cooperation Mechanism for CSIRTs – MeliCERTes Facility**" **(SMART 2018/1024)** and CIRCL Computer Incident Response Center Luxembourg.

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 – STIX v2.1 data model for Incident Report

iRiS

- **Indicator object:**
  - ➢ corresponds to some suspicious or malicious cyber activity detected by **Threat Detection ATA** tools of IRIS architecture.
- **Vulnerability object:**
  - ➢ refers to a weakness or defect identified in the infrastructure by the tools of IRIS architecture for identifying either network or software vulnerabilities.
- **Tool object:**
  - ➢ corresponds to the **ATA tools** of IRIS architecture. More specifically, VDM, BINSEC, Sivi, NIGHTWATCH, MAI-GUARD.
- **Identity object:**
  - ➢ represents either to the tool organisation or to the infrastructure entity.
- **Infrastructure object**:
  - ➢ corresponds to PUC1, PUC2, PUC3 infrastructures
- **Attack pattern object:**
  - ➢ is used to **categorize a potential attack** that could be performed taking advantage of some of the vulnerabilities identified in the infrastructure.
- **Observed data object:**
  - ➢ corresponds to **raw information (e.g. an IP address, URLs, domain names, email addresses, network activity evidence, files, registry keys, etc.)** that has been observed by some of the ATA tools of IRIS architecture, but without any context.
- **Course of action:**
  - ➢ corresponds to the proposed **mitigation response actions** of IRIS – **CACAO formatted**



STIX v2.1 Data model of IRIS incident report

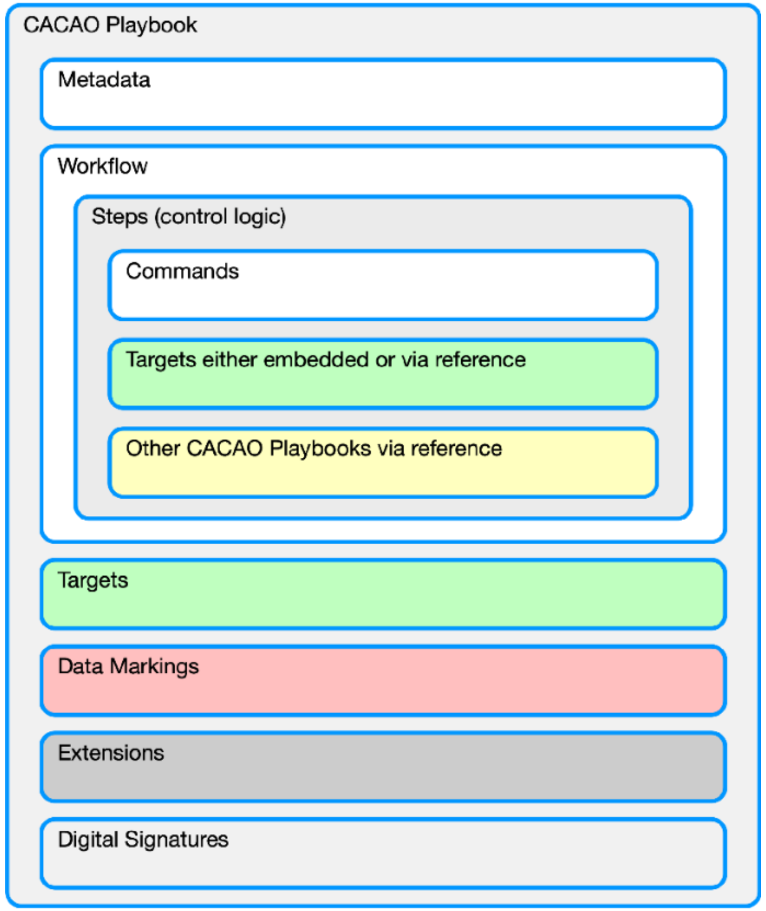
OASIS OPEN

STIX™

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 – STIX/CACAO playbooks

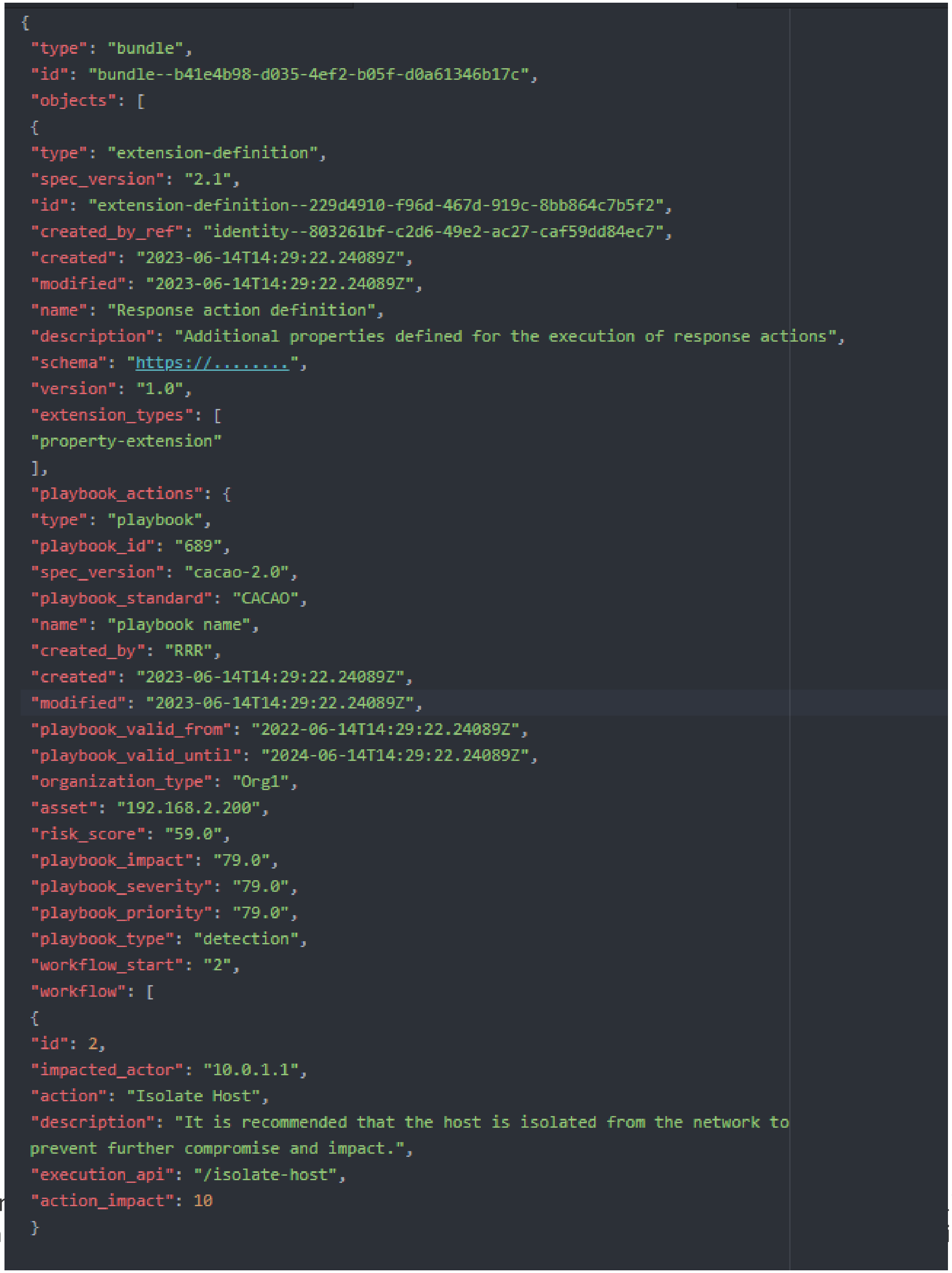
- **CACAO – Collaborative Automated Course of Action Operations playbook**
  - ✓ To **defend against cyber threats**, organizations must **manually identify, create, and document the prevention, mitigation, and remediation steps that, together, form a course of action playbook**. This is performed with **CACAO in a standardized way** to **document** and **share** these playbooks **across organizational boundaries and technology solutions**.
  - ✓ It is a **workflow for security orchestration and automation** represented in JSON that contains a set of steps to perform based on a logical process, like how Business Process Model and Notation (BPMN) defines a playbook for business processes.
  - ✓ A CACAO playbook comprises of:
    - ➢ Metadata
    - ➢ workflow steps that integrate logic to control the **commands** to be performed, **targets** that receive, process, and execute commands, **data markings** that specify the playbook's handling and sharing requirements and **extensions** that allow to granularly introduce additional functionality



Architecture and components of a CACAO security playbook

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 – STIX/CACAO data model example



```
{
 "type": "bundle",
 "id": "bundle--b41e4b98-d035-4ef2-b05f-d0a61346b17c",
 "objects": [
 {
 "type": "extension-definition",
 "spec_version": "2.1",
 "id": "extension-definition--229d4910-f96d-467d-919c-8bb864c7b5f2",
 "created_by_ref": "identity--803261bf-c2d6-49e2-ac27-caf59dd84ec7",
 "created": "2023-06-14T14:29:22.24089Z",
 "modified": "2023-06-14T14:29:22.24089Z",
 "name": "Response action definition",
 "description": "Additional properties defined for the execution of response actions",
 "schema": "https://........",
 "version": "1.0",
 "extension_types": [
 "property-extension"
 ],
 "playbook_actions": {
 "type": "playbook",
 "playbook_id": "689",
 "spec_version": "cacao-2.0",
 "playbook_standard": "CACAO",
 "name": "playbook name",
 "created_by": "RRR",
 "created": "2023-06-14T14:29:22.24089Z",
 "modified": "2023-06-14T14:29:22.24089Z",
 "playbook_valid_from": "2022-06-14T14:29:22.24089Z",
 "playbook_valid_until": "2024-06-14T14:29:22.24089Z",
 "organization_type": "Org1",
 "asset": "192.168.2.200",
 "risk_score": "59.0",
 "playbook_impact": "79.0",
 "playbook_severity": "79.0",
 "playbook_priority": "79.0",
 "playbook_type": "detection",
 "workflow_start": "2",
 "workflow": [
 {
 "id": 2,
 "impacted_actor": "10.0.1.1",
 "action": "Isolate Host",
 "description": "It is recommended that the host is isolated from the network to
 prevent further compromise and impact.",
 "execution_api": "/isolate-host",
 "action_impact": 10
 }
```

This project has received funding from the European Unior 727.
This material reflects only the authors' view and European ins.

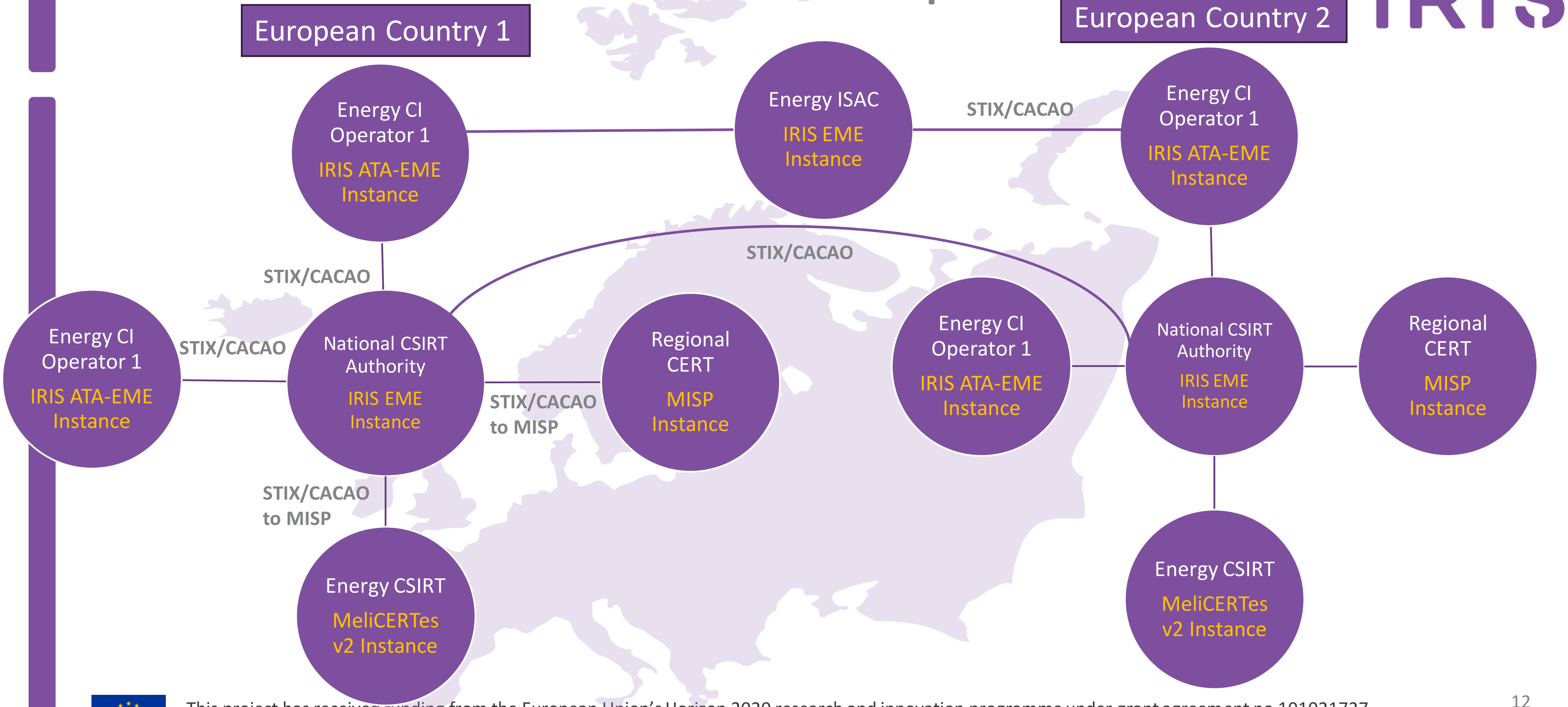
IRIS-enhanced MeliCERTes Ecosystem for NIS2 and CER Directives Compliance

Key objectives: Extend MeliCERTes v2 open-source platform incorporating IRIS CTI developments to enable:

- **Secure and efficient security information representation** in **standardized** formats (STIX v2.1 / CACAO / MISP) → interoperability within and across IRIS Platform
- **Secure disclosable AI-relevant & IoT-relevant CTI information sharing**
  - ✓ Promote **wider awareness, better preparation, detection and response capabilities**
  - ✓ Define **sharing policies** and **communities of trust**
  - ✓ **Securely communicate and collaborate within and across CERT/CSIRT authorities and CI Operators**
- **Secure storage and augmentation** of the **AI and IoT focused cybersecurity knowledge base** at a **European level**
- Provision of **advanced and unified dashboard for incident reporting, situational awareness, response actions configuration and recommendation (EME UI)**
- Offering Authentication and Authorization **AAA** services
  - ✓ OATH2, SAML, PKI etc.
  - ✓ **CTI log auditing** (via **DPA**)
- **Distributed architecture – ecosystem**
  - ✓ **Instances** deployed at **stakeholders' premises (CI Operators & CERTs/CSIRTS authorities)**

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-enhanced MeliCERTes Ecosystem for NIS2 and CER Directives Compliance



European Country 1

European Country 2

Energy CI Operator 1
IRIS ATA-EME Instance

Energy ISAC
IRIS EME Instance

Energy CI Operator 1
IRIS ATA-EME Instance

National CSIRT Authority
IRIS EME Instance

Regional CERT
MISP Instance

Energy CSIRT
MeliCERTes v2 Instance

Energy CI Operator 1
IRIS ATA-EME Instance

National CSIRT Authority
IRIS EME Instance

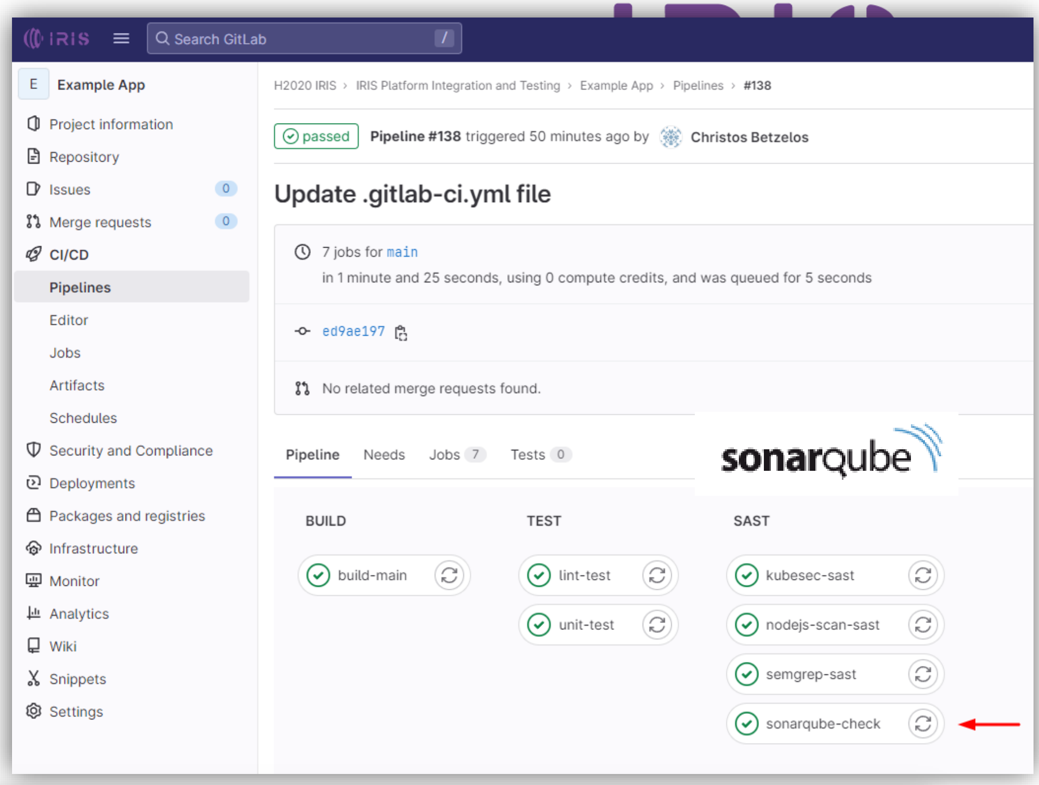
Regional CERT
MISP Instance

Energy CSIRT
MeliCERTes v2 Instance

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-enhanced MeliCERTes Ecosystem for CRA Compliance

- IRIS adopts a **DevSecOps** approach in all phases of software system design, development, integration, testing and operation
- A **CI/CD environment and respective tools** have been setup to support developer teams to security harden their software while in development/increase their resilience/minimize their vulnerabilities
- **Security-by-design** has been followed during architecture specification
- **Security testing, both SAST and DAST**, are part of the software security testing activities



H2020 IRIS › IRIS Platform Integration and Testing › Example App › Pipelines › #138

passed Pipeline #138 triggered 50 minutes ago by Christos Betzelos

Update .gitlab-ci.yml file

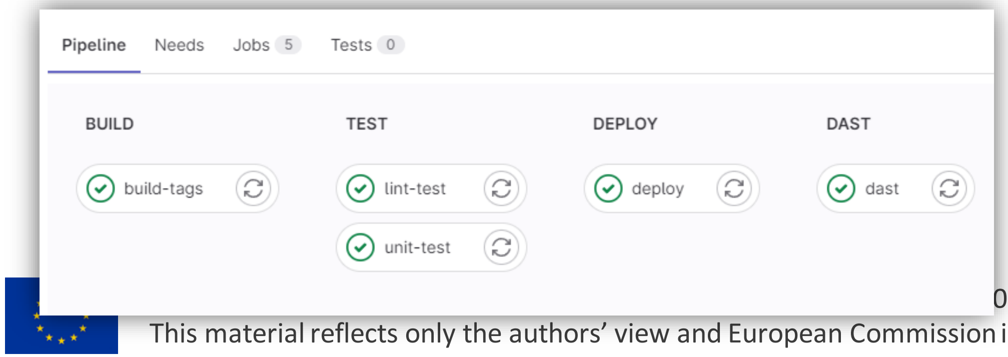
7 jobs for main
in 1 minute and 25 seconds, using 0 compute credits, and was queued for 5 seconds

ed9ae197

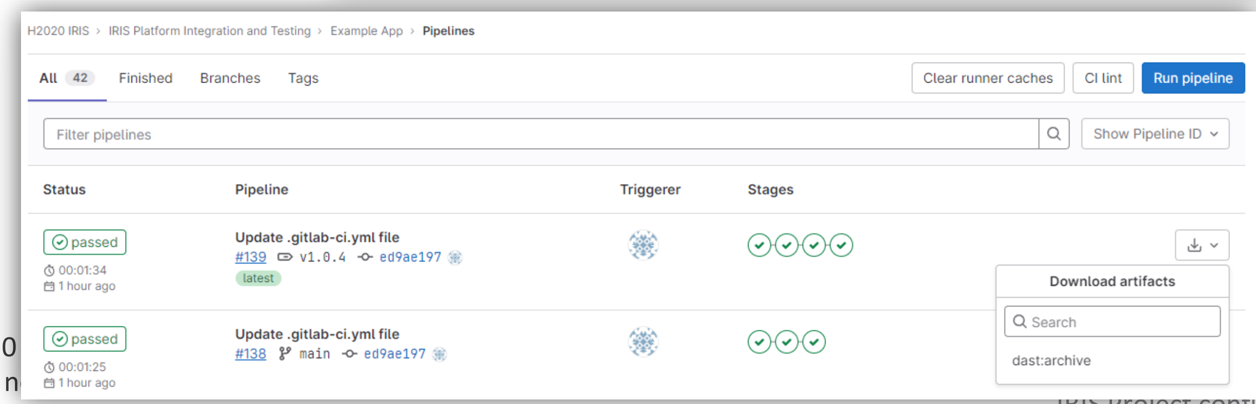
No related merge requests found.

Pipeline | Needs | Jobs 7 | Tests 0

BUILD	TEST	SAST
build-main	lint-test	kubesec-sast
	unit-test	nodejs-scan-sast
		semgrep-sast
		sonarqube-check


Pipeline | Needs | Jobs 5 | Tests 0

BUILD	TEST	DEPLOY	DAST
build-tags	lint-test	deploy	dast
	unit-test		



H2020 IRIS › IRIS Platform Integration and Testing › Example App › Pipelines

Status	Pipeline	Triggerer	Stages
passed 00:01:34 1 hour ago	Update .gitlab-ci.yml file #139 v1.0.4 ed9ae197 latest		✓✓✓✓
passed 00:01:25 1 hour ago	Update .gitlab-ci.yml file #138 main ed9ae197		✓✓✓

IRIS – A snapshot to IRIS EME Secure Sharing, Collaboration, Incident Reporting and Response

- EME Unified Dashboard (UI) & SIEM
  - ✓ Integrates all the IRIS provided visual environments, safeguarding the coherence of the IRIS platform towards its users.
  - ✓ **Customized views per target User** and **incident reporting** capabilities
    - ➢ **CI Operator view**
    - ➢ **CERT/CSIRT cybersecurity operator view**
  - ✓ **CTI information and report details**
  - ✓ **CTI response (mitigation) actions** and associated workflows
  - ✓ **Automated response actions policy management**
  - ✓ **Access control and access rights to shared data** based on
    - ➢ The type of user/operator
    - ➢ The type of service/infrastructure they provide
    - ➢ The sensitivity of the information to be shared / communicated

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.

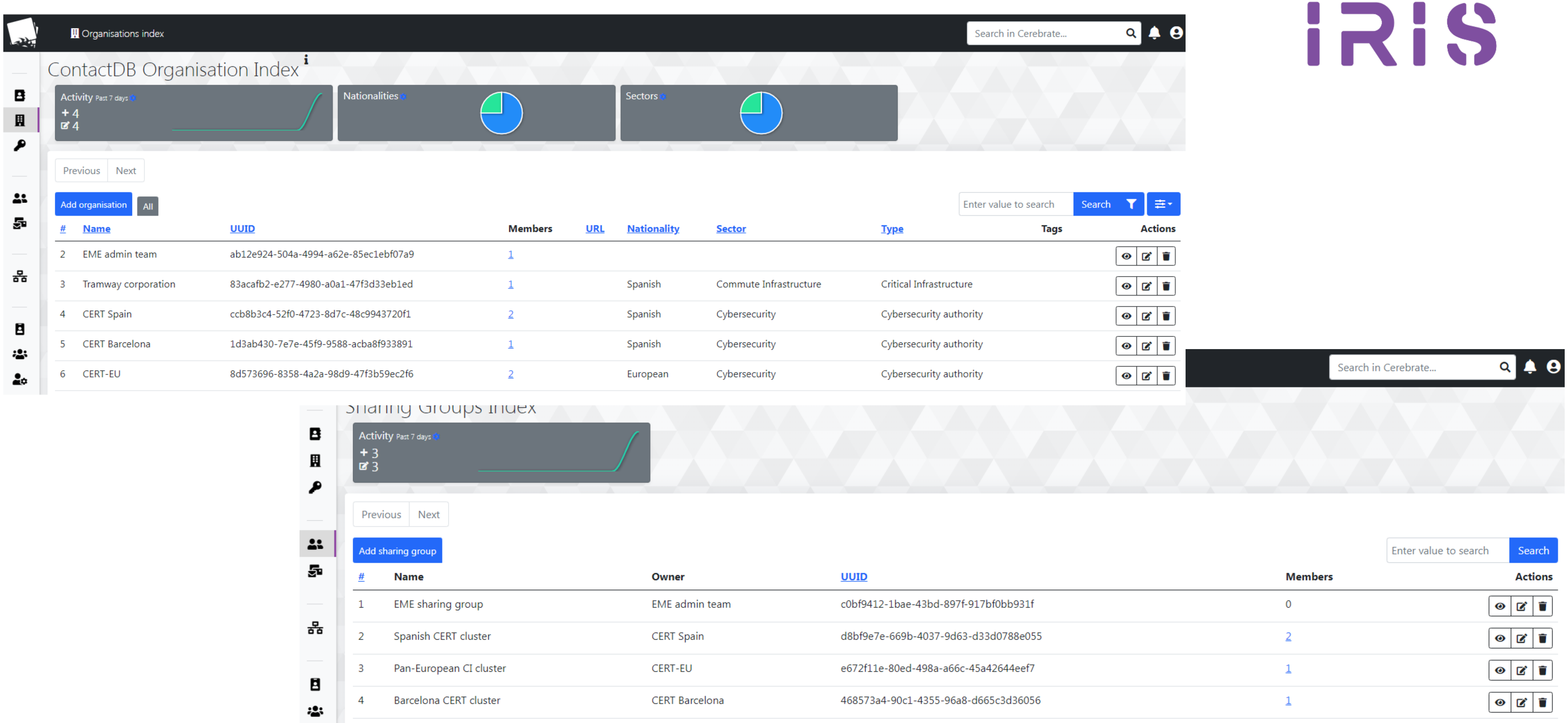
IRIS-EME Cerebrate for Trust Communities

melicertes

- Cerebrate is an open-source platform developed in the framework of MeliCERTes v2.0
  - ✓ Acts as a **trusted contact information provider** and interconnection orchestrator for other security tools
- Features
  - ✓ Advanced repository to manage individuals and organisations
    - ➢ Management of **individuals** and their affiliations to each organisation
    - ➢ **Sharing groups as Trust Circles**
    - ➢ **Dynamic model for creating new organisational structures** (FIRST.org, EU CSIRTs)
  - ✓ Distributed synchronisation model
  - ✓ **Key store for public encryption and signing cryptographic keys**

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.

MeliCERTes v2 – Cerebrate



ContactDB Organisation Index

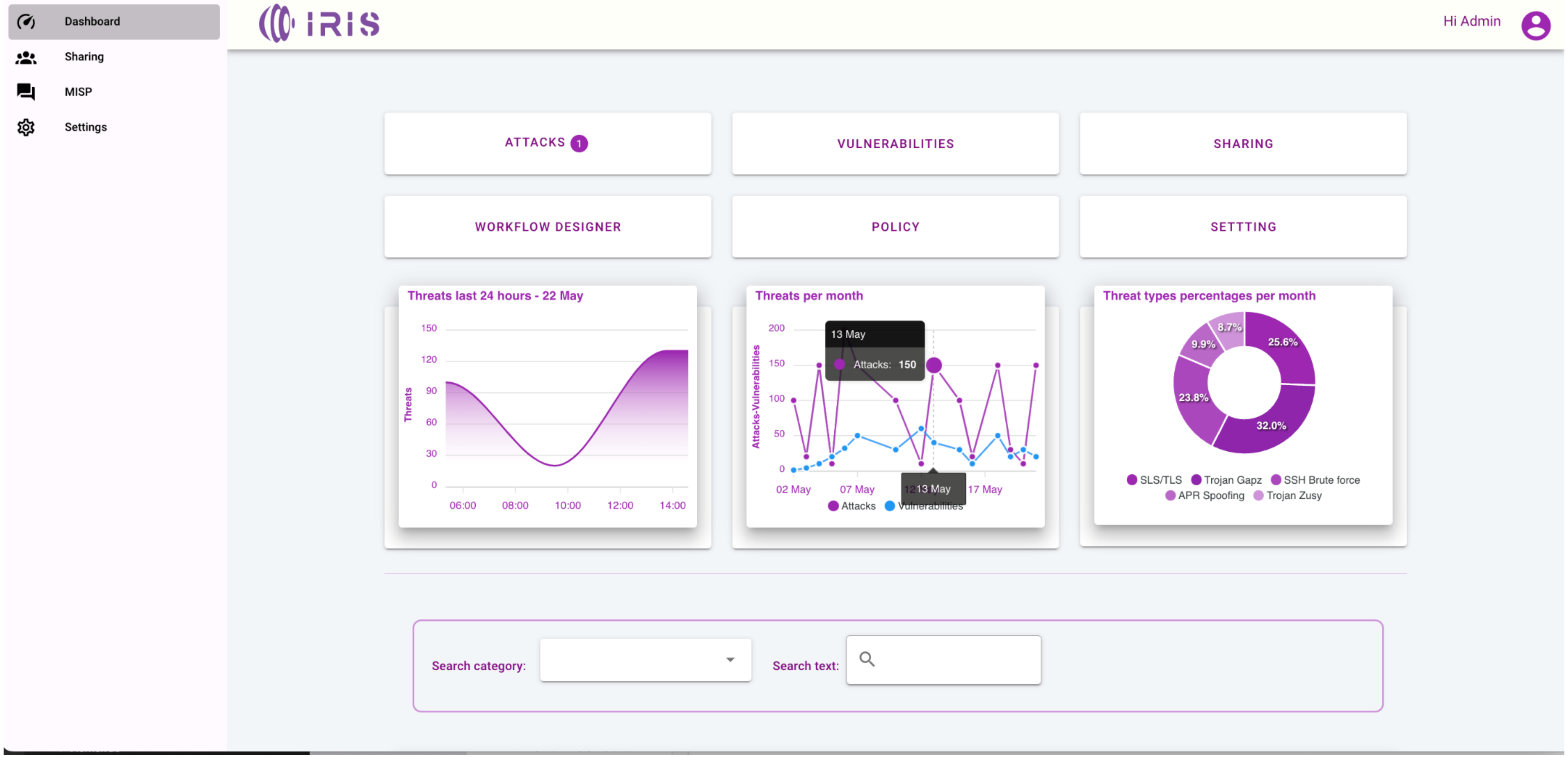
#	Name	UUID	Members	URL	Nationality	Sector	Type	Tags	Actions
2	EME admin team	ab12e924-504a-4994-a62e-85ec1ebf07a9	1						
3	Tramway corporation	83acafb2-e277-4980-a0a1-47f3d33eb1ed	1		Spanish	Commute Infrastructure	Critical Infrastructure		
4	CERT Spain	ccb8b3c4-52f0-4723-8d7c-48c9943720f1	2		Spanish	Cybersecurity	Cybersecurity authority		
5	CERT Barcelona	1d3ab430-7e7e-45f9-9588-acba8f933891	1		Spanish	Cybersecurity	Cybersecurity authority		
6	CERT-EU	8d573696-8358-4a2a-98d9-47f3b59ec2f6	2		European	Cybersecurity	Cybersecurity authority		

Sharing Groups Index

#	Name	Owner	UUID	Members	Actions
1	EME sharing group	EME admin team	c0bf9412-1bae-43bd-897f-917bf0bb931f	0	
2	Spanish CERT cluster	CERT Spain	d8bf9e7e-669b-4037-9d63-d33d0788e055	2	
3	Pan-European CI cluster	CERT-EU	e672f11e-80ed-498a-a66c-45a42644eef7	1	
4	Barcelona CERT cluster	CERT Barcelona	468573a4-90c1-4355-96a8-d665c3d36056	1	

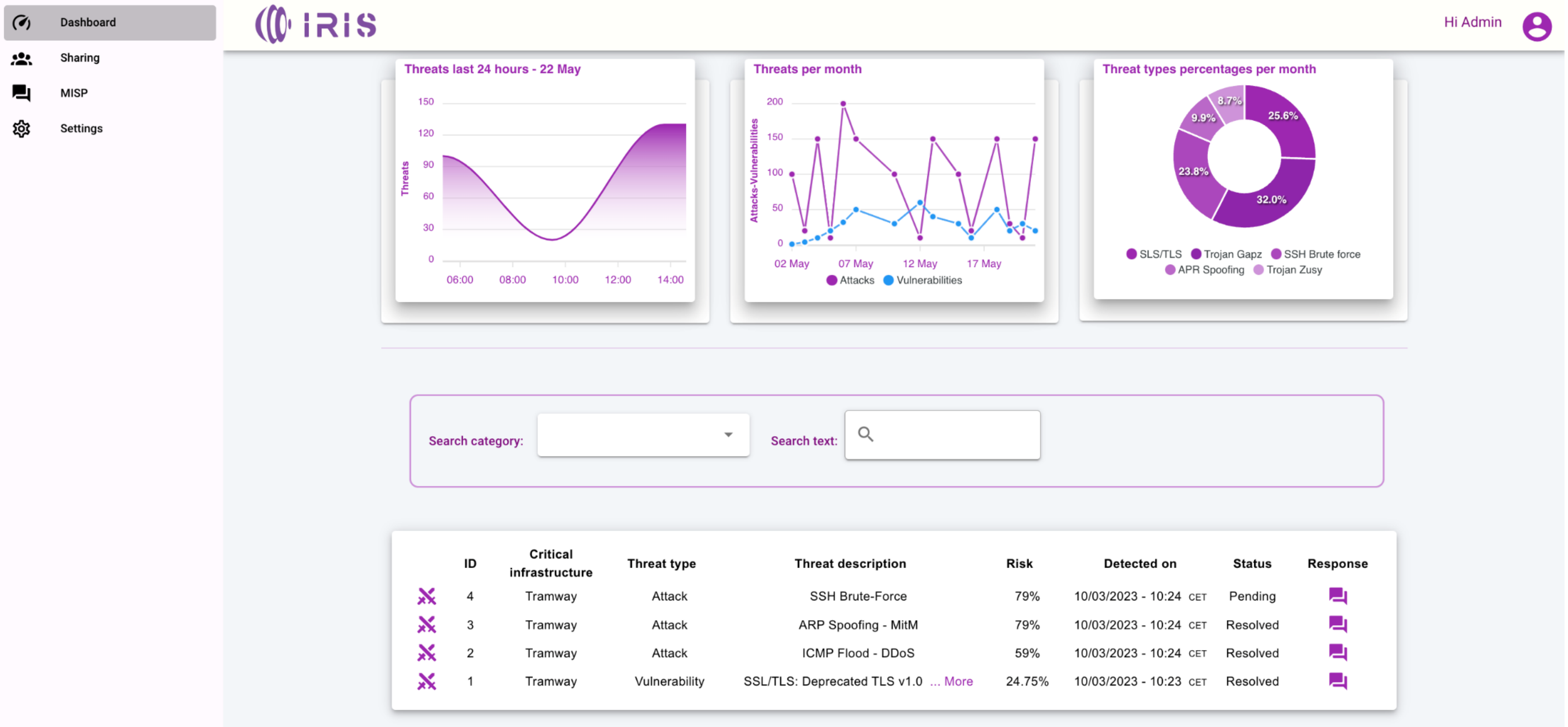
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

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.

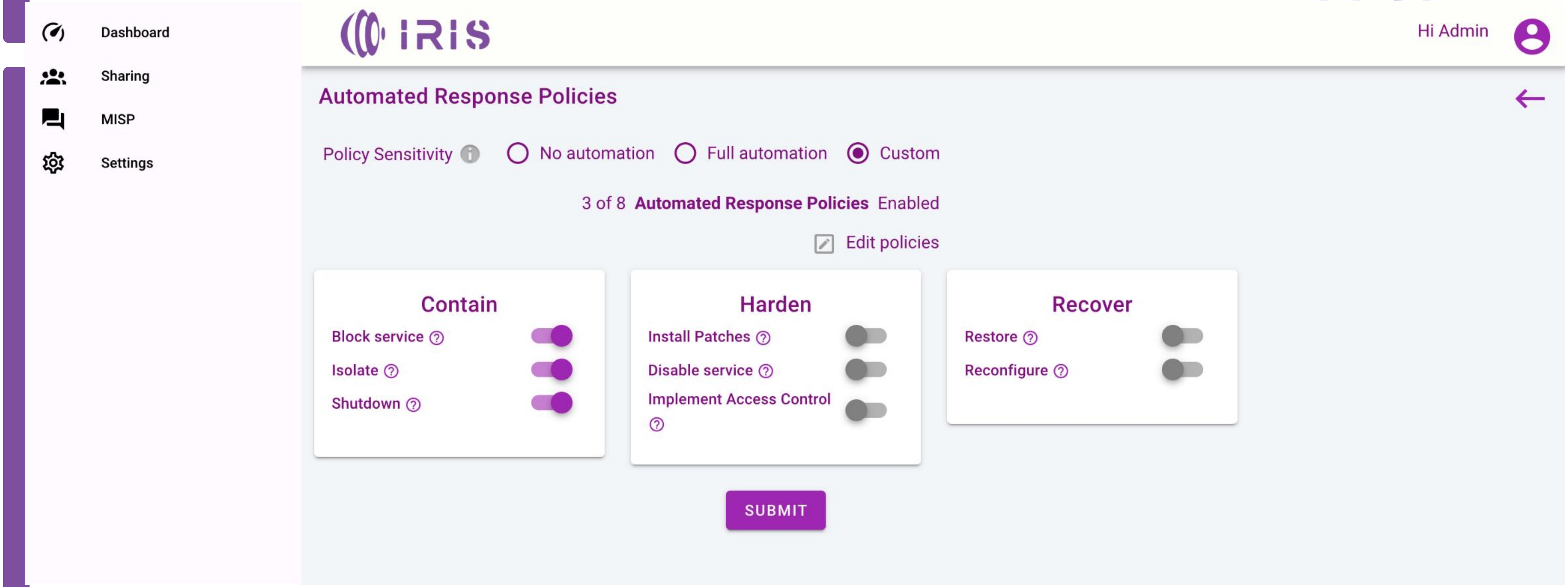
EME – CI operator view



	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

3 of 8 **Automated Response Policies** Enabled

Edit policies

Contain

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

Harden

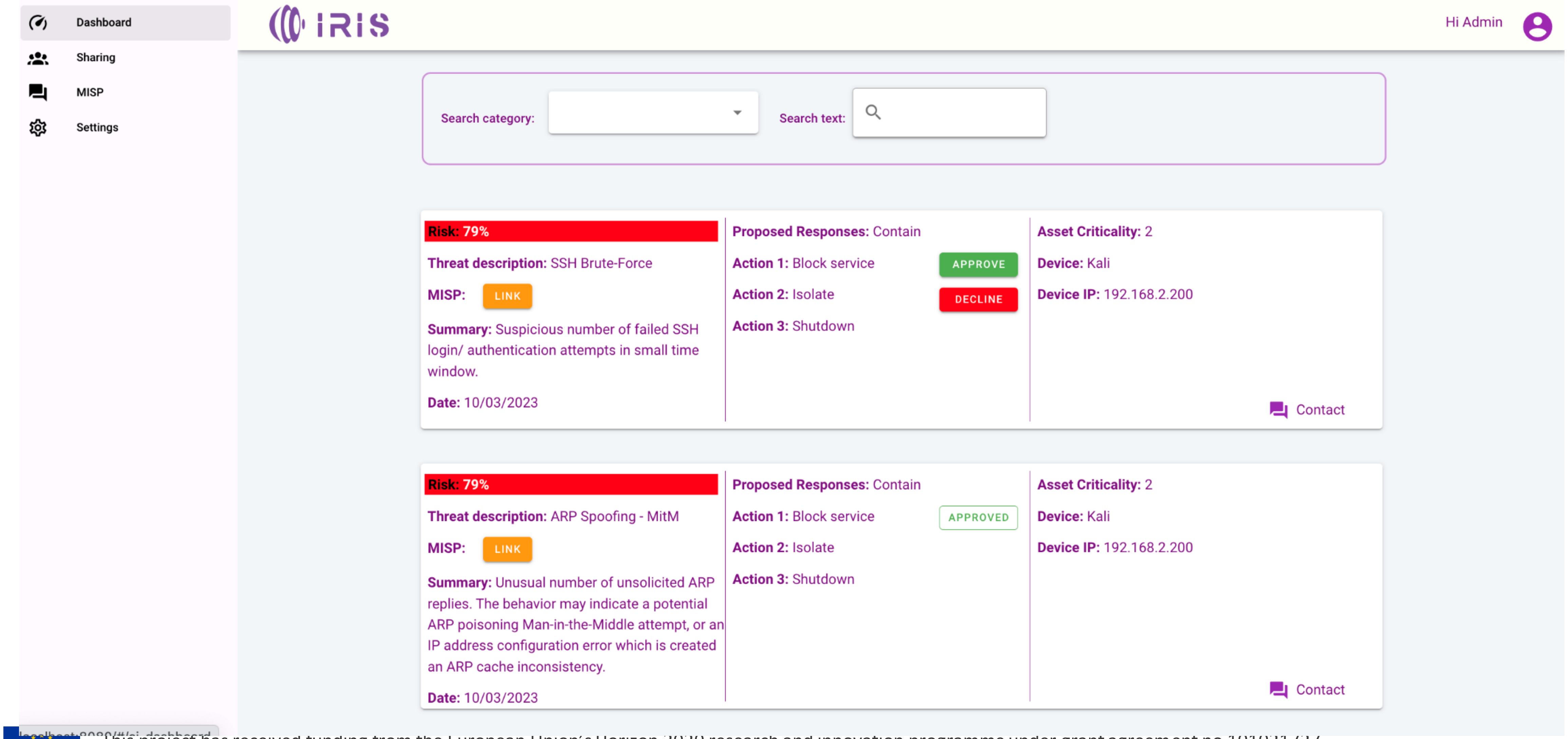
- Install Patches: off
- Disable service: off
- Implement Access Control: off

Recover

- Restore: off
- Reconfigure: off

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

Contact

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

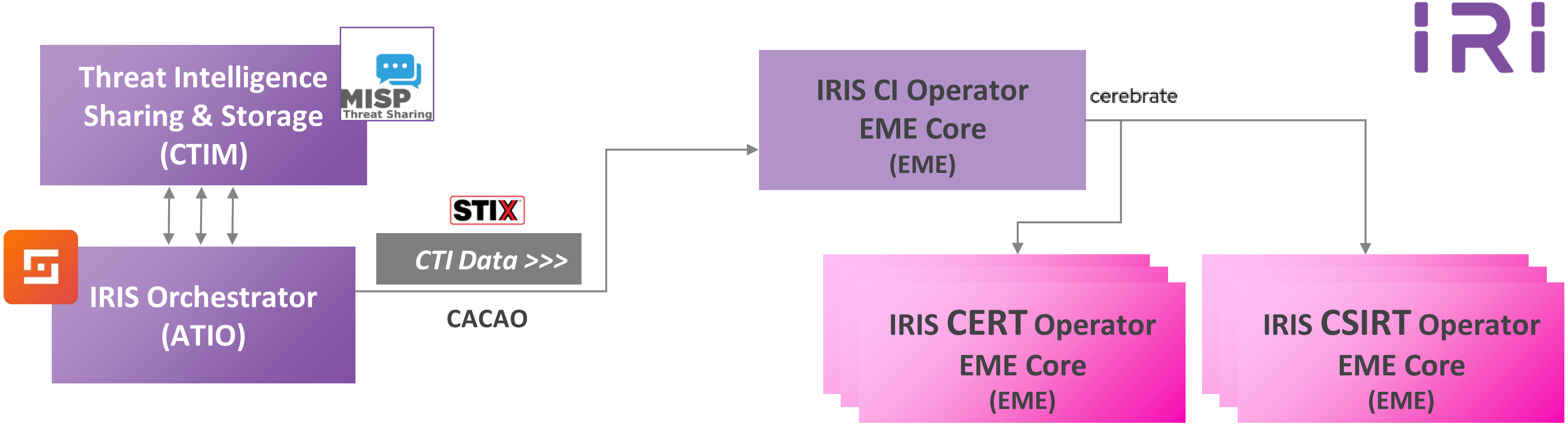
Device: Kali

Device IP: 192.168.2.200

Contact

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.

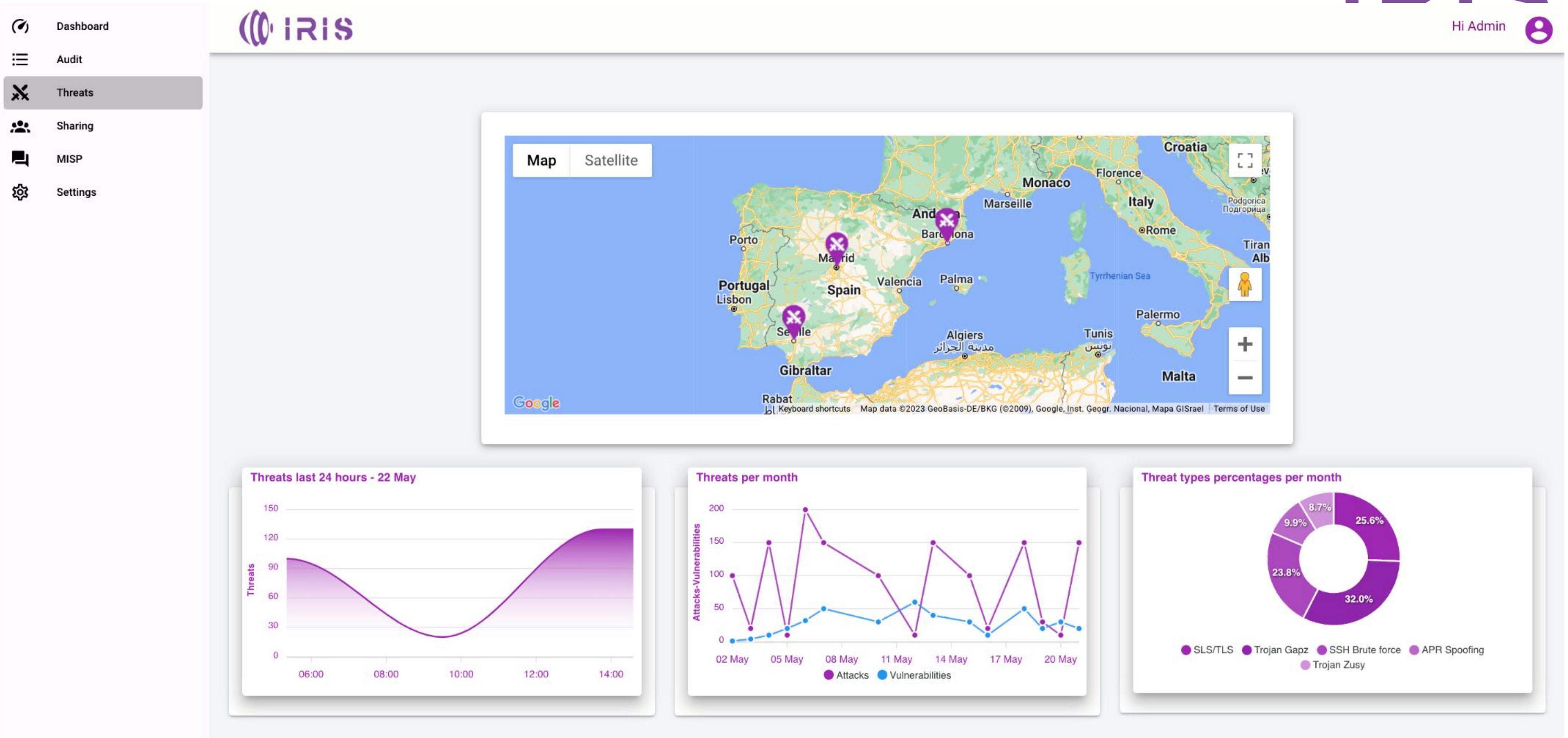
EME – CIs & CERTs/CSIRTs coordination and collaboration


Threat Intelligence Sharing & Storage (CTIM)
MISP Threat Sharing
IRIS Orchestrator (ATIO)
STIX
CTI Data >>>
CACAO
IRIS CI Operator EME Core (EME)
cerebrate
IRIS CERT Operator EME Core (EME)
IRIS CSIRT Operator EME Core (EME)

- IRIS Enhanced MeliCERTes Ecosystem follows a **distributed architecture** schema
- IRIS detected CTI Data **are shared among the IRIS stakeholders**
  - ✓ CI Operators
  - ✓ CERTs/CSIRTs cybersecurity authorities
    - ➢ Regional
    - ➢ National
    - ➢ Pan-European level

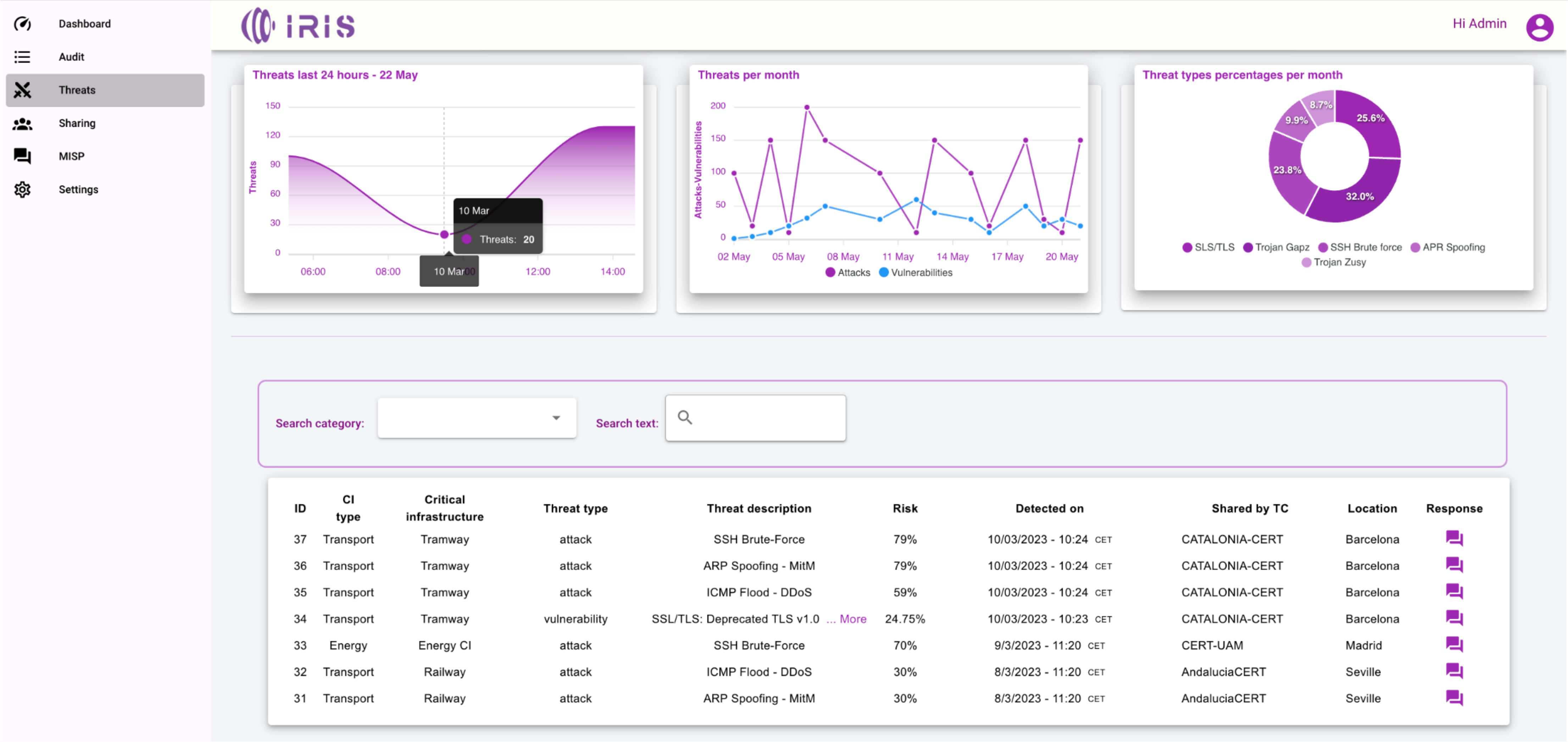
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

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.

Potential Contributions & Support Needed

- Towards Standards
  - ✓ Interaction support with the relevant Standardization Bodies in an easy and fast pacing manner
  - ✓ Feedback provision on description needs potentially not currently covered by adopted standards
  - ✓ Extend current standardized data models and link them to relevant standards for physical security of a CI and for hybrid, cyber-physical threats and attacks
- Towards Policies and Regulations
  - ✓ Provide insights on the approach chosen to meet fundamental requirements from the policy and legal landscape
  - ✓ Support to easily approach and interact with the target community (CERTs/CSIRTs, CI Operators, etc.) on a frequent basis in order to:
    - ➢ present results
    - ➢ gather needs
    - ➢ contribute and give applied tangible feedback as to feasibility/applicability within and across sectors
    - ➢ share knowledge – lessons learnt
    - ➢ develop acceptable and usable approaches and technologies

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! Questions?

Dr. Sofia Tsekeridou, sofia.tsekeridou@netcompany.com

iris-h2020.eu

IRIS H2020 Project

iris_h2020

ECSCI SPM Workshop| 5th Dec 2023

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.