IRIS Artificial Intelligence Threat Reporting & Incidence report system

IRIS Innovations for Timely, Semi-automated, Secure and Interoperable CTI and Incidents Information Sharing and Reporting enhancing Awareness and Collaboration among Need to know CI Operators and CERTs/CSIRTs

I-SENSE GROUP ICCS

Ms. Vasiliki-Georgia (Giovana) Bilali, giovana.bilali@iccs.gr

iti Information Technologies Institute

Ms. Eleni Darra, e.darra@iti.gr

netcompany intrasoft

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

SECURE CYBER CLUSTER

Cyber Threat Intelligence: Empowering IoT Security

6 March 2024
Online

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.

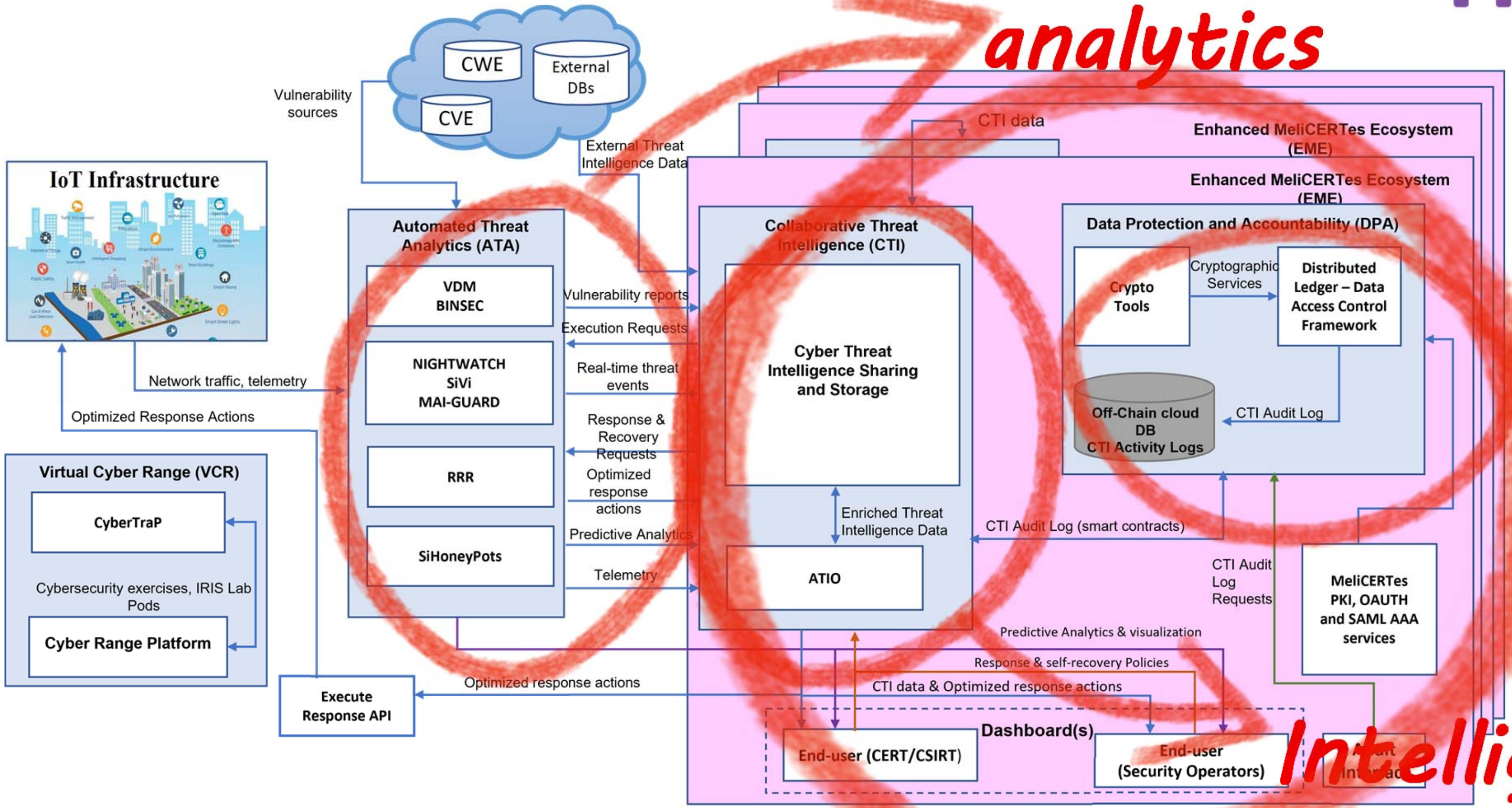
IRIS in a Nutshell

- **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


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)

Privacy

Intelligence

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 Innovations in CTI

- Automated and timely CTI and cyber incidents information collection
- Semi-automated and interoperable CTI workflows management and integration with ATA tools
- Dynamic CTI Information enrichment
- Semi-automated, secure and timely CTI and Incidents Information Sharing and Reporting among Need to Know Stakeholders (OES and CERTs/CSIRTs)
- Enhanced and Timely Cyber Awareness and Collaboration among Need to Know Stakeholders (OES and CERTs/CSIRTs) to manage a threat
- Closing the loop: Semi-automating response policies execution and acknowledgement of detected vulnerabilities and 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 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.

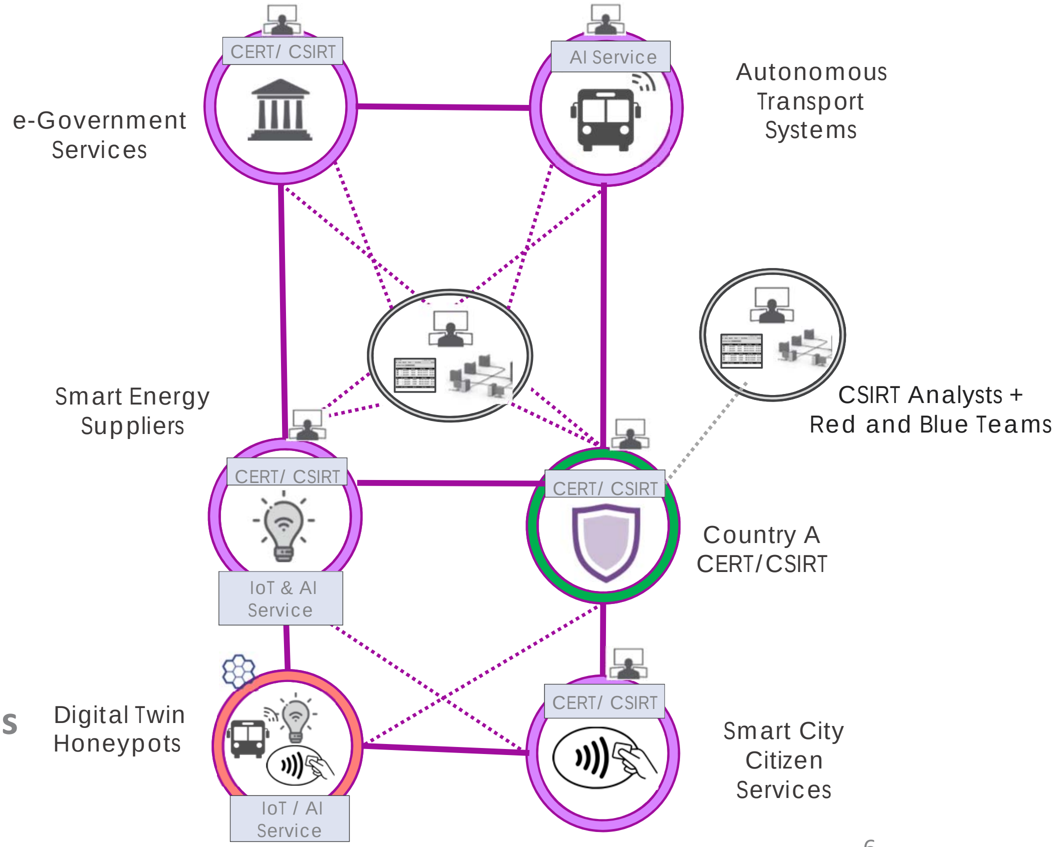
IRIS- Identification of the Problem toward CERT/CSIRT/CI operators daily processes - ICCS

- ✓ Time consuming processes
  - ➢ e.g. monitoring processes, waiting for alerts, Identification of abnormalities
- ✓ Misinterpretation of information by the system for immediate action
- ✓ Decision making processes

Variation of data sources in smart cities

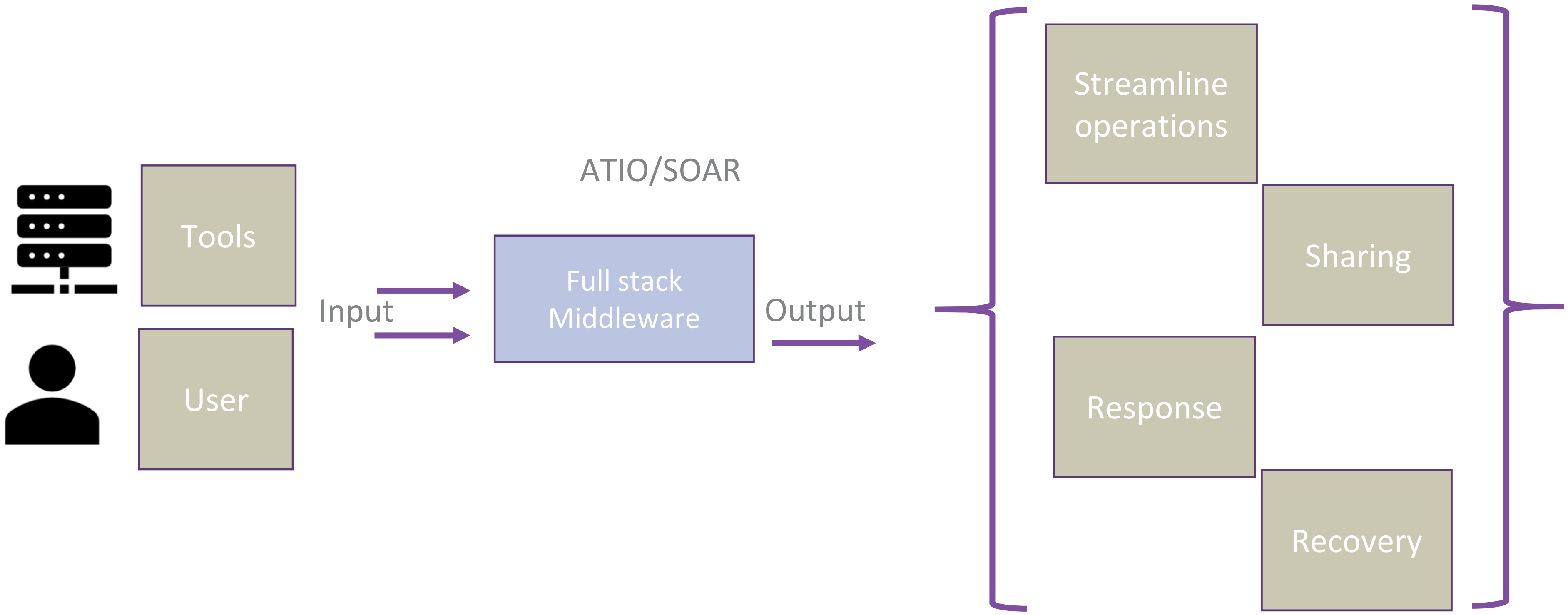
- ✓ Static and Real-time data from sensors adaptors, actuators, IDs, SIEM, CCTV cameras etc.

The vulnerability of the system increases as the smart cities become more variant in data sources.



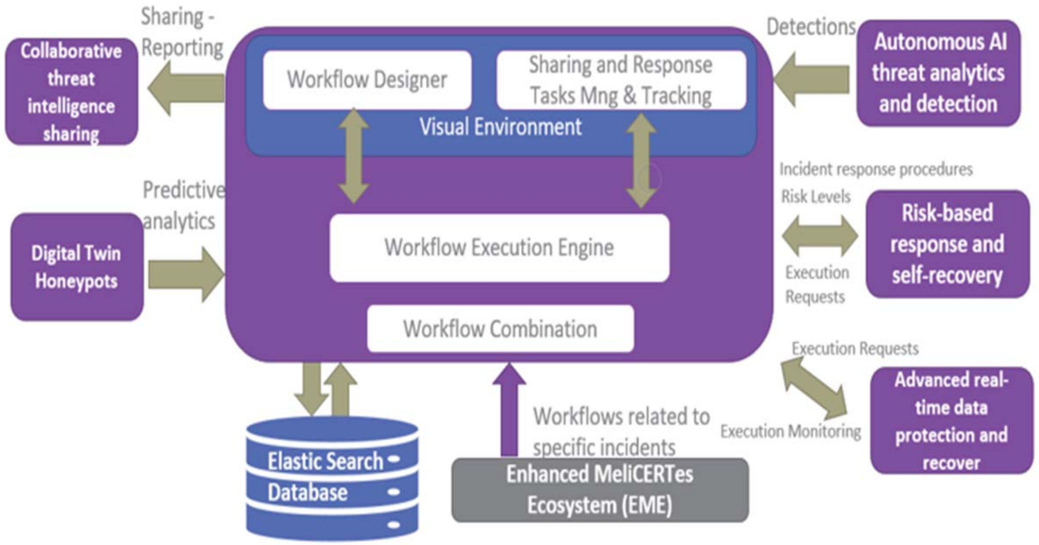
This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors’ view and European Commission is not responsible for any use that may be made of the information it contains.

IRIS supports Security Orchestration Automation and Response (SOAR) service



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.

Advanced Threat Intelligence Orchestrator (ATIO) Structure


Sharing - Reporting
Collaborative threat intelligence sharing
Workflow Designer
Sharing and Response Tasks Mng & Tracking
Visual Environment
Detections
Autonomous AI threat analytics and detection
Predictive analytics
Digital Twin Honeypots
Workflow Execution Engine
Incident response procedures
Risk Levels
Risk-based response and self-recovery
Execution Requests
Workflow Combination
Execution Requests
Advanced real-time data protection and recover
Execution Monitoring
Workflows related to specific incidents
Elastic Search Database
Enhanced MeliCERTes Ecosystem (EME)

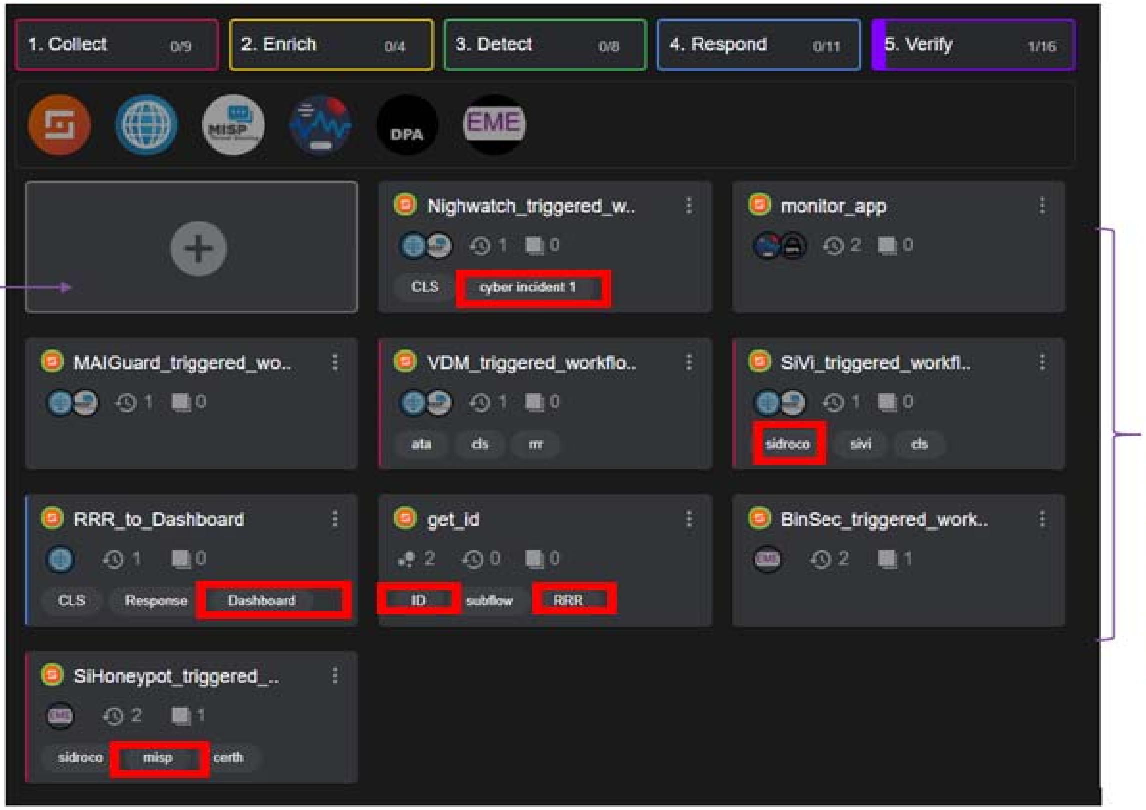
Back end and Front end Services

1. Orchestration Workflow Manager (OWM)
2. Sharing and Response Task Management and Tracking
3. Workflow Execution Engine
4. Workflow Combination
5. Data Exchange Framework
6. Command Execution Requests Framework
7. ATIO database

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.

Orchestrator (ATIO) Workflow Designer (OWM)

1. Creation of customized workflows



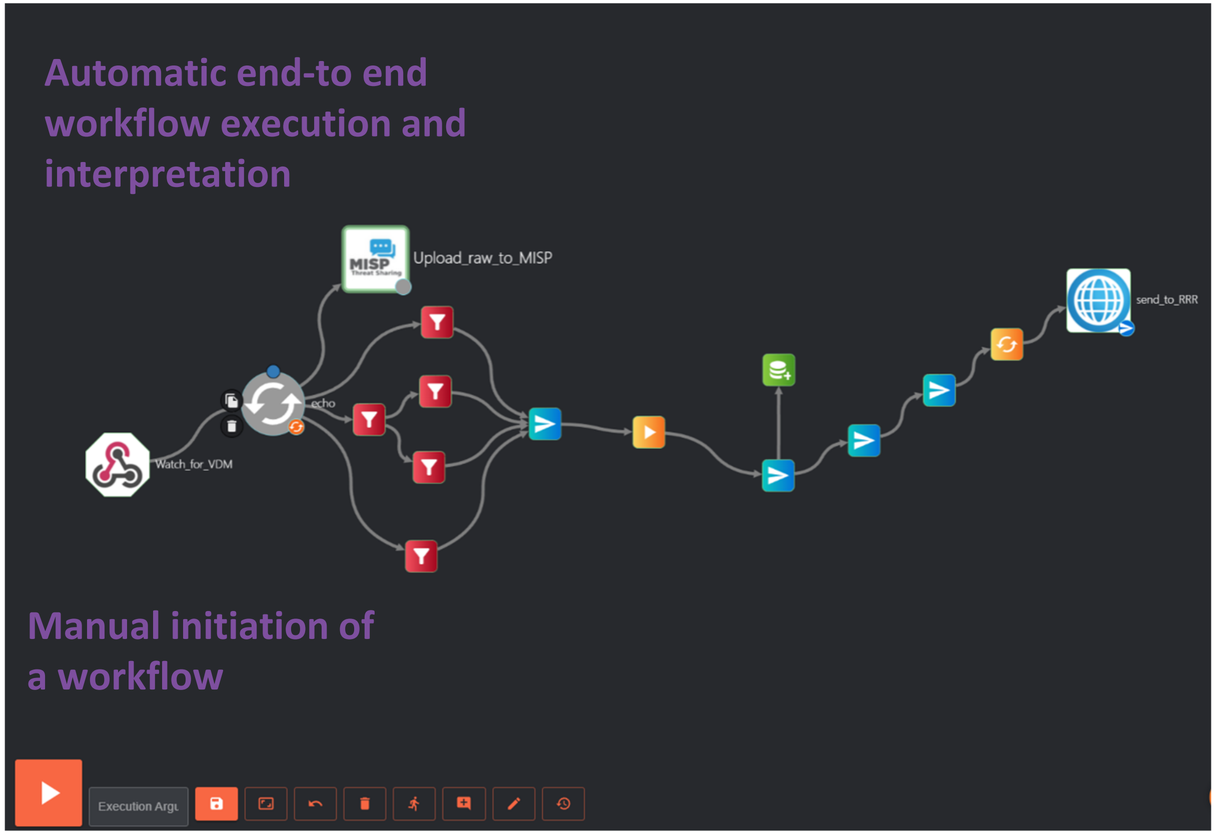
2. Usage of pre-made workflows

3. Capability of changing pre-made Workflows (e.g. end-points, steps, tools)

4. Workflows Tags categorization based on involved tools, cyber-attacks etc.

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.

Terminology of Workflow execution through Shuffle environment



Automatic end-to end workflow execution and interpretation

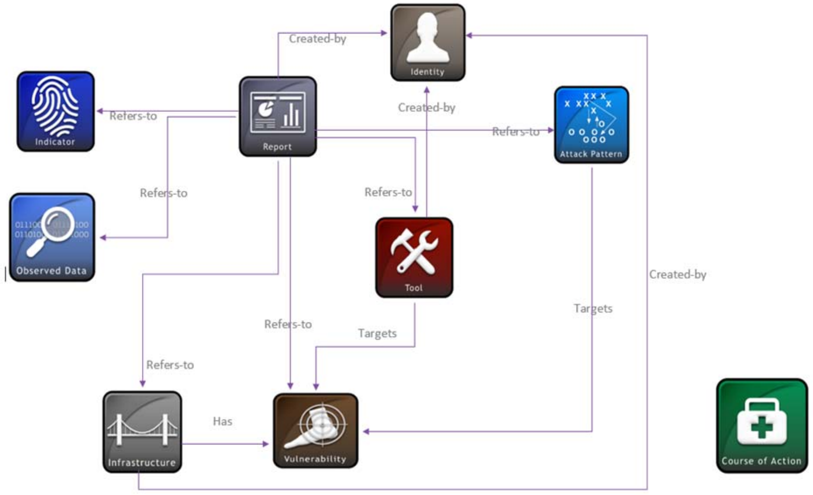
Manual initiation of a workflow

1. Workflow steps
2. Arrows
3. Action steps (processing)
4. Subflows

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

- **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**

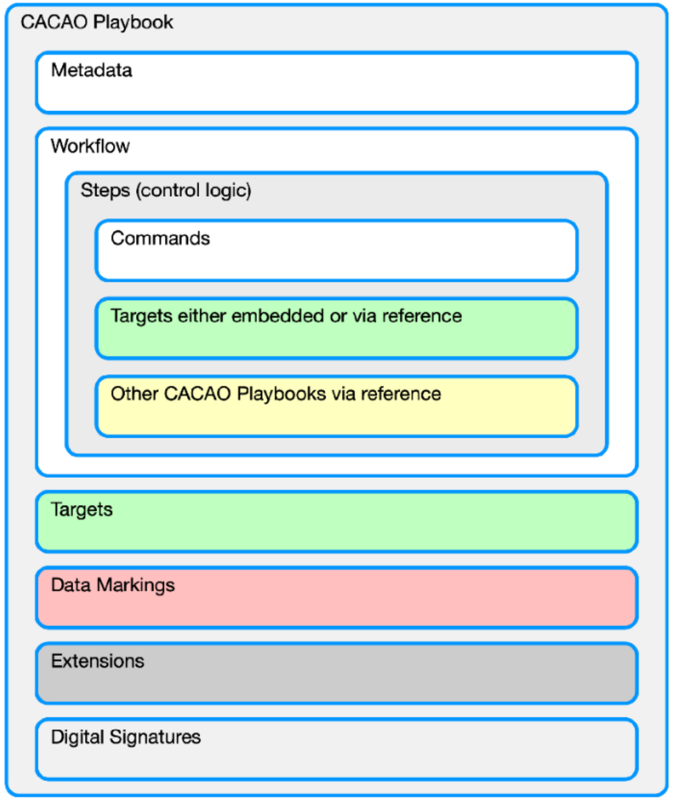


STIX v2.1 Data model of IRIS incident report

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

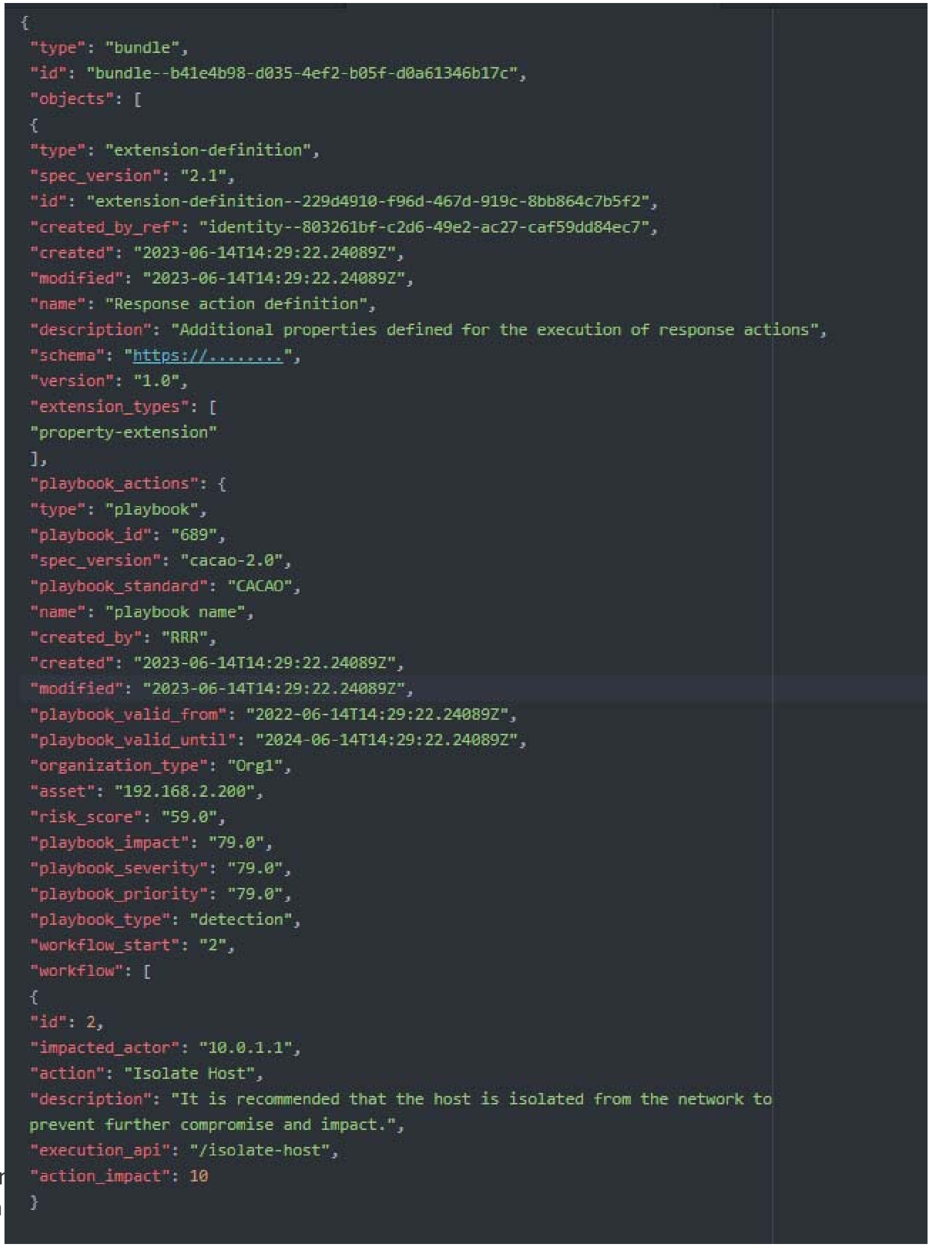
- **CACAO – Collaborative Automated Course of Action Operations playbook**
  - ✓ To **defend against cyber threats**, organizations must **manually identify, create, and document the prevention, mitigation, and remediation steps that, together, form a course of action playbook**. This is performed with **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 ns.

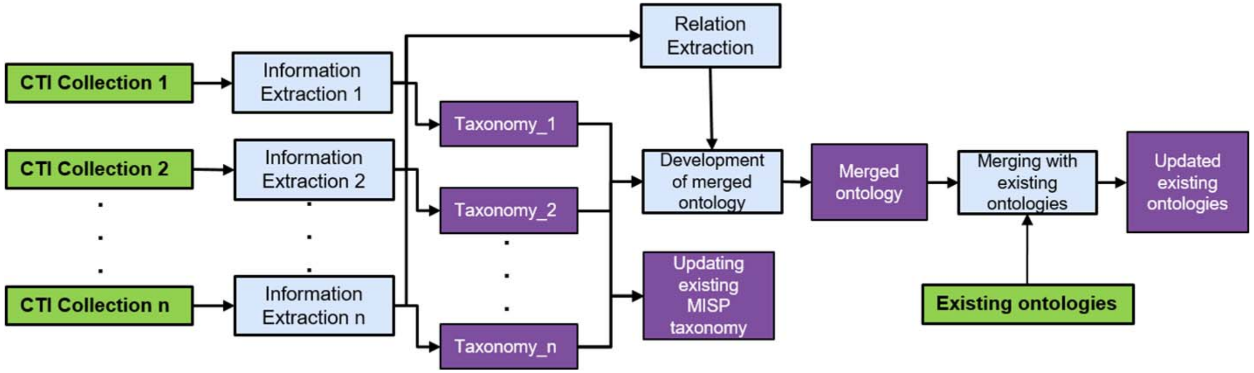
The role of CTI in the IRIS project - CERTH

- **Cyber Threat Intelligence (CTI)** generated from
  - ✓ Indicator of Compromise (IoC) and
  - ✓ Tactics, Techniques and Procedures (TTPs)
- Mitigate the damages caused by attackers
- CTI appears in formats that do not directly provide defence advantages, and more steps are needed to gain all its benefits
- The CTI module allows ICT stakeholders and European CERTs/CSIRTs to create and seamlessly orchestrate and share context-rich information about cyber threats targeting IoT and AI-driven ICT systems
- CTI is complemented by an interoperability layer that allows integration with the smart city's IoT- and AI-enabled infrastructures.
- CTI module aims to collect, share and report threat intelligence to CERTs/CSIRTs SoC teams etc., while building dynamic taxonomies for IoT and AI-related attacks to be used as a basis for building cybersecurity incident response systems.

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.

The role of CTI in the IRIS project

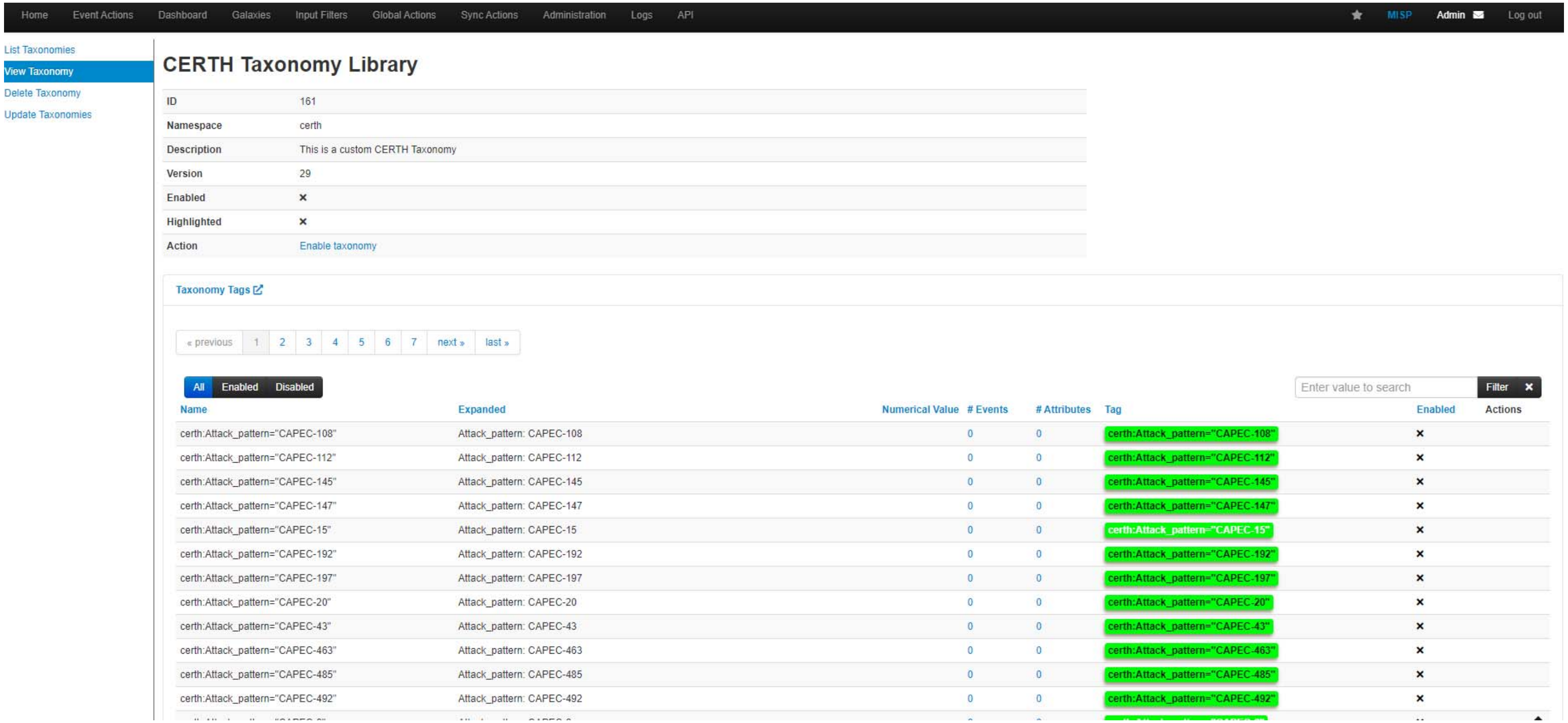
- CTI Collection
- Information Extraction
- Taxonomy generation
  - Update existing MISP taxonomy
- Development of merged ontology
- Merging with existing ontologies
- Updated existing ontologies



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.

Taxonomy generation

Develop a common lexicon with the end goal of setting standards and best practices for managing the cybersecurity of ICT systems against attackers



CERTH Taxonomy Library

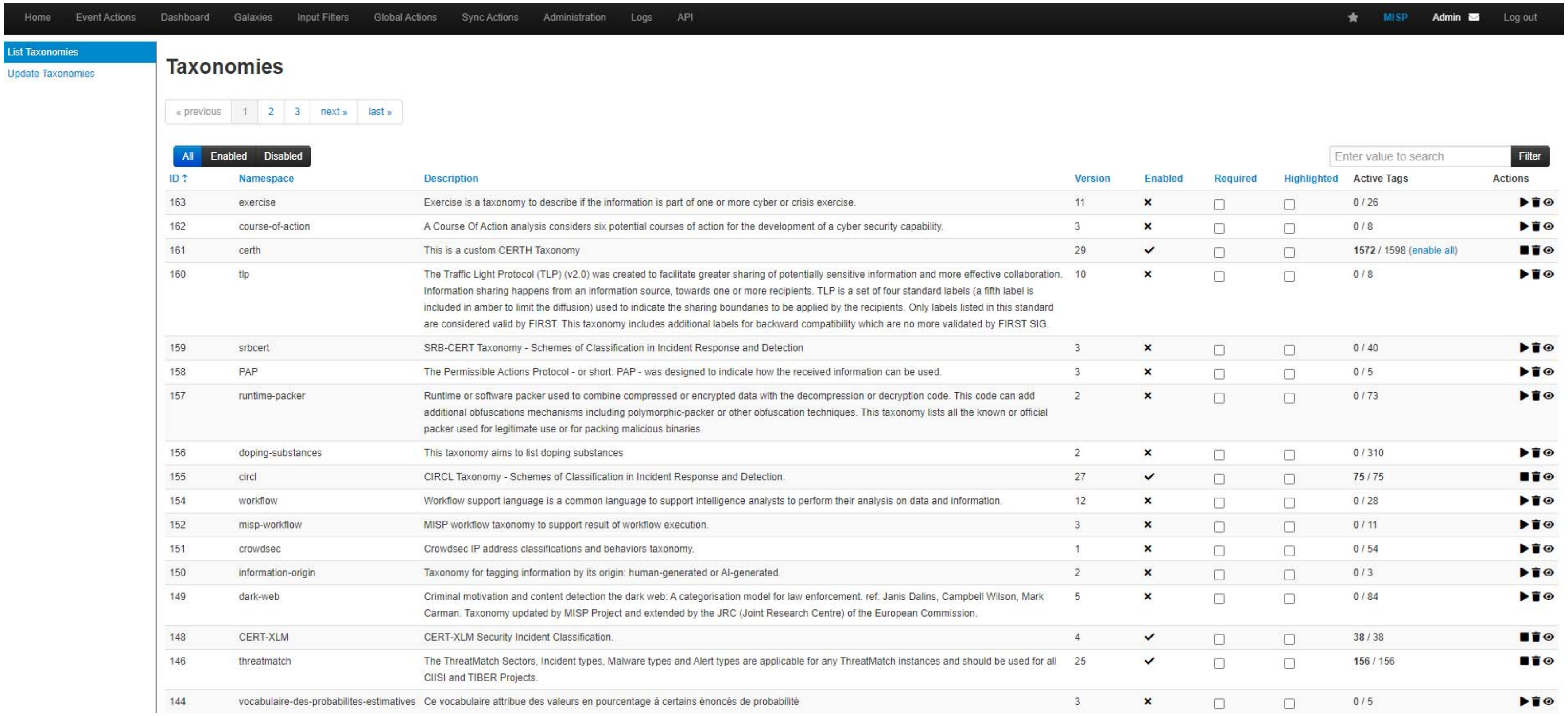
ID	161
Namespace	certh
Description	This is a custom CERTH Taxonomy
Version	29
Enabled	×
Highlighted	×
Action	Enable taxonomy

Taxonomy Tags

Name	Expanded	Numerical Value	# Events	# Attributes	Tag	Enabled	Actions
certh:Attack_pattern="CAPEC-108"	Attack_pattern: CAPEC-108		0	0	certh:Attack_pattern="CAPEC-108"	×	
certh:Attack_pattern="CAPEC-112"	Attack_pattern: CAPEC-112		0	0	certh:Attack_pattern="CAPEC-112"	×	
certh:Attack_pattern="CAPEC-145"	Attack_pattern: CAPEC-145		0	0	certh:Attack_pattern="CAPEC-145"	×	
certh:Attack_pattern="CAPEC-147"	Attack_pattern: CAPEC-147		0	0	certh:Attack_pattern="CAPEC-147"	×	
certh:Attack_pattern="CAPEC-15"	Attack_pattern: CAPEC-15		0	0	certh:Attack_pattern="CAPEC-15"	×	
certh:Attack_pattern="CAPEC-192"	Attack_pattern: CAPEC-192		0	0	certh:Attack_pattern="CAPEC-192"	×	
certh:Attack_pattern="CAPEC-197"	Attack_pattern: CAPEC-197		0	0	certh:Attack_pattern="CAPEC-197"	×	
certh:Attack_pattern="CAPEC-20"	Attack_pattern: CAPEC-20		0	0	certh:Attack_pattern="CAPEC-20"	×	
certh:Attack_pattern="CAPEC-43"	Attack_pattern: CAPEC-43		0	0	certh:Attack_pattern="CAPEC-43"	×	
certh:Attack_pattern="CAPEC-463"	Attack_pattern: CAPEC-463		0	0	certh:Attack_pattern="CAPEC-463"	×	
certh:Attack_pattern="CAPEC-485"	Attack_pattern: CAPEC-485		0	0	certh:Attack_pattern="CAPEC-485"	×	
certh:Attack_pattern="CAPEC-492"	Attack_pattern: CAPEC-492		0	0	certh:Attack_pattern="CAPEC-492"	×	

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.

List of taxonomies in MISP

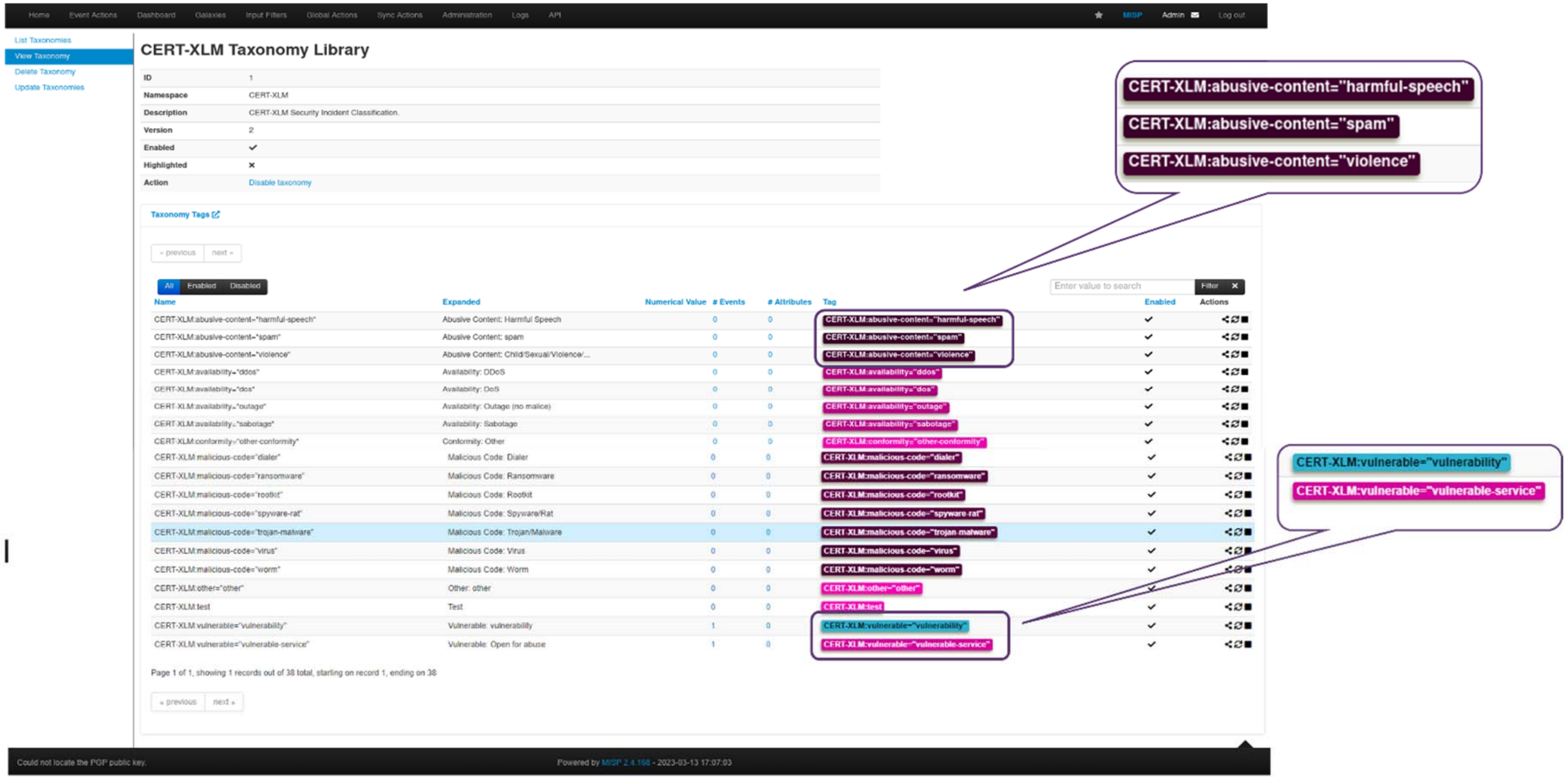


Taxonomies

ID ↑	Namespace	Description	Version	Enabled	Required	Highlighted	Active Tags	Actions
163	exercise	Exercise is a taxonomy to describe if the information is part of one or more cyber or crisis exercise.	11	✗	□	□	0 / 26	▶ 🗑 👁
162	course-of-action	A Course Of Action analysis considers six potential courses of action for the development of a cyber security capability.	3	✗	□	□	0 / 8	▶ 🗑 👁
161	certh	This is a custom CERTH Taxonomy	29	✓	□	□	1572 / 1598 (enable all)	■ 🗑 👁
160	tlp	The Traffic Light Protocol (TLP) (v2.0) was created to facilitate greater sharing of potentially sensitive information and more effective collaboration. Information sharing happens from an information source, towards one or more recipients. TLP is a set of four standard labels (a fifth label is included in amber to limit the diffusion) used to indicate the sharing boundaries to be applied by the recipients. Only labels listed in this standard are considered valid by FIRST. This taxonomy includes additional labels for backward compatibility which are no more validated by FIRST SIG.	10	✗	□	□	0 / 8	▶ 🗑 👁
159	srbcert	SRB-CERT Taxonomy - Schemes of Classification in Incident Response and Detection	3	✗	□	□	0 / 40	▶ 🗑 👁
158	PAP	The Permissible Actions Protocol - or short: PAP - was designed to indicate how the received information can be used.	3	✗	□	□	0 / 5	▶ 🗑 👁
157	runtime-packer	Runtime or software packer used to combine compressed or encrypted data with the decompression or decryption code. This code can add additional obfuscations mechanisms including polymorphic-packer or other obfuscation techniques. This taxonomy lists all the known or official packer used for legitimate use or for packing malicious binaries.	2	✗	□	□	0 / 73	▶ 🗑 👁
156	doping-substances	This taxonomy aims to list doping substances	2	✗	□	□	0 / 310	▶ 🗑 👁
155	circl	CIRCL Taxonomy - Schemes of Classification in Incident Response and Detection.	27	✓	□	□	75 / 75	■ 🗑 👁
154	workflow	Workflow support language is a common language to support intelligence analysts to perform their analysis on data and information.	12	✗	□	□	0 / 28	▶ 🗑 👁
152	misp-workflow	MISP workflow taxonomy to support result of workflow execution.	3	✗	□	□	0 / 11	▶ 🗑 👁
151	crowdsec	Crowdsec IP address classifications and behaviors taxonomy.	1	✗	□	□	0 / 54	▶ 🗑 👁
150	information-origin	Taxonomy for tagging information by its origin: human-generated or AI-generated.	2	✗	□	□	0 / 3	▶ 🗑 👁
149	dark-web	Criminal motivation and content detection the dark web: A categorisation model for law enforcement. ref: Janis Dalins, Campbell Wilson, Mark Carman. Taxonomy updated by MISP Project and extended by the JRC (Joint Research Centre) of the European Commission.	5	✗	□	□	0 / 84	▶ 🗑 👁
148	CERT-XLM	CERT-XLM Security Incident Classification.	4	✓	□	□	38 / 38	■ 🗑 👁
146	threatmatch	The ThreatMatch Sectors, Incident types, Malware types and Alert types are applicable for any ThreatMatch instances and should be used for all CIISI and TIBER Projects.	25	✓	□	□	156 / 156	■ 🗑 👁
144	vocabulaire-des-probabilites-estimatives	Ce vocabulaire attribue des valeurs en pourcentage à certains énoncés de probabilité	3	✗	□	□	0 / 5	▶ 🗑 👁

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.

MISP update



CERT-XLM Taxonomy Library

ID	1
Namespace	CERT-XLM
Description	CERT-XLM Security Incident Classification.
Version	2
Enabled	✓
Highlighted	✕
Action	Disable taxonomy

Taxonomy Tags

Name	Expanded	Numerical Value	# Events	# Attributes	Tag	Enabled	Actions
CERT-XLM:abusive-content="harmful-speech"	Abusive Content: Harmful Speech		0	0	CERT-XLM:abusive-content="harmful-speech"	✓	< ⟳ ■
CERT-XLM:abusive-content="spam"	Abusive Content: spam		0	0	CERT-XLM:abusive-content="spam"	✓	< ⟳ ■
CERT-XLM:abusive-content="violence"	Abusive Content: Child/Sexual/Violence/...		0	0	CERT-XLM:abusive-content="violence"	✓	< ⟳ ■
CERT-XLM:availability="ddos"	Availability: DDoS		0	0	CERT-XLM:availability="ddos"	✓	< ⟳ ■
CERT-XLM:availability="dos"	Availability: DoS		0	0	CERT-XLM:availability="dos"	✓	< ⟳ ■
CERT-XLM:availability="outage"	Availability: Outage (no malice)		0	0	CERT-XLM:availability="outage"	✓	< ⟳ ■
CERT-XLM:availability="sabotage"	Availability: Sabotage		0	0	CERT-XLM:availability="sabotage"	✓	< ⟳ ■
CERT-XLM:conformity="other-conformity"	Conformity: Other		0	0	CERT-XLM:conformity="other-conformity"	✓	< ⟳ ■
CERT-XLM:malicious-code="dialer"	Malicious Code: Dialer		0	0	CERT-XLM:malicious-code="dialer"	✓	< ⟳ ■
CERT-XLM:malicious-code="ransomware"	Malicious Code: Ransomware		0	0	CERT-XLM:malicious-code="ransomware"	✓	< ⟳ ■
CERT-XLM:malicious-code="rootkit"	Malicious Code: Rootkit		0	0	CERT-XLM:malicious-code="rootkit"	✓	< ⟳ ■
CERT-XLM:malicious-code="spyware-rat"	Malicious Code: Spyware/Rat		0	0	CERT-XLM:malicious-code="spyware-rat"	✓	< ⟳ ■
CERT-XLM:malicious-code="trojan-malware"	Malicious Code: Trojan/Malware		0	0	CERT-XLM:malicious-code="trojan-malware"	✓	< ⟳ ■
CERT-XLM:malicious-code="virus"	Malicious Code: Virus		0	0	CERT-XLM:malicious-code="virus"	✓	< ⟳ ■
CERT-XLM:malicious-code="worm"	Malicious Code: Worm		0	0	CERT-XLM:malicious-code="worm"	✓	< ⟳ ■
CERT-XLM:other="other"	Other: other		0	0	CERT-XLM:other="other"	✓	< ⟳ ■
CERT-XLM:test	Test		0	0	CERT-XLM:test	✓	< ⟳ ■
CERT-XLM:vulnerable="vulnerability"	Vulnerable: vulnerability		1	0	CERT-XLM:vulnerable="vulnerability"	✓	< ⟳ ■
CERT-XLM:vulnerable="vulnerable-service"	Vulnerable: Open for abuse		1	0	CERT-XLM:vulnerable="vulnerable-service"	✓	< ⟳ ■

Page 1 of 1, showing 1 records out of 38 total, starting on record 1, ending on 38

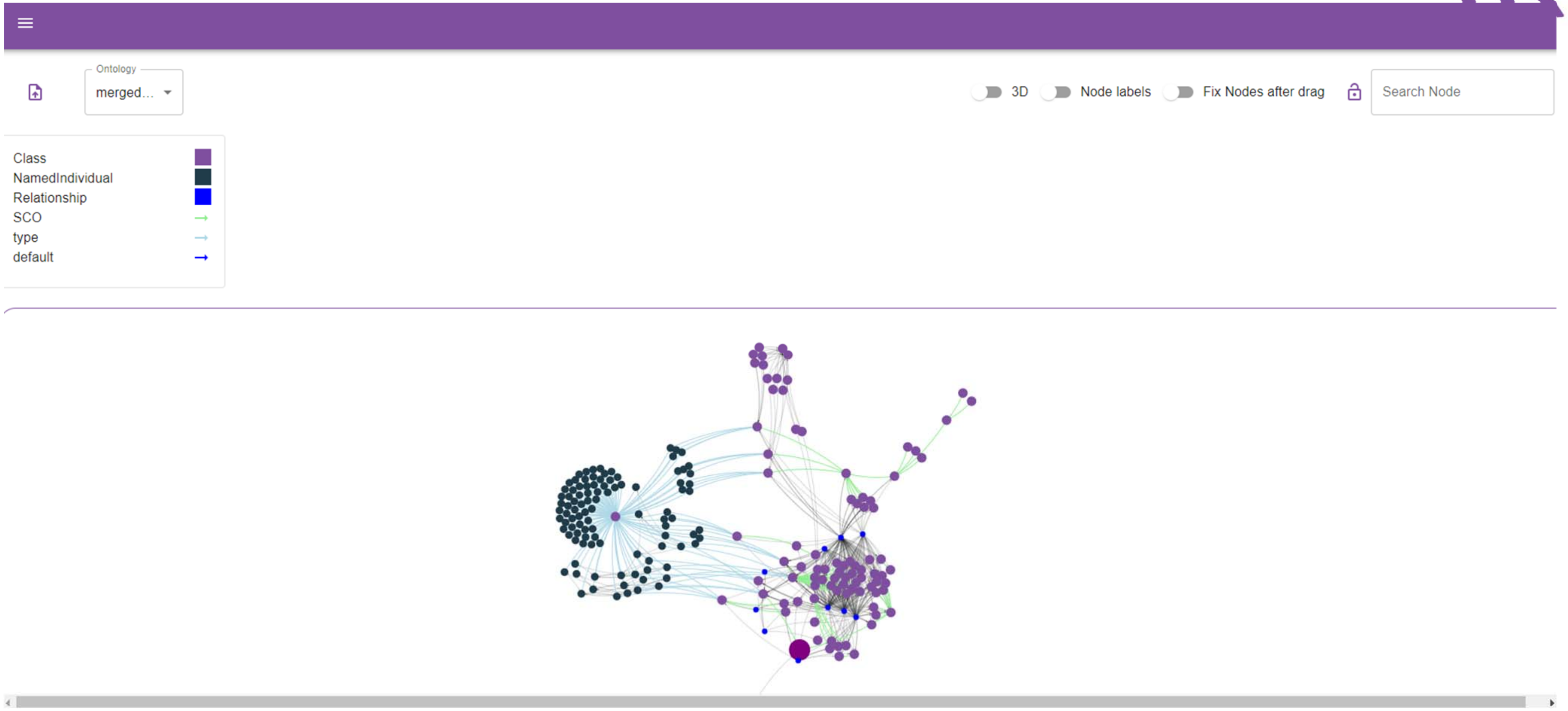
Could not locate the PGP public key.

Powered by MISP 2.4.168 - 2023-03-13 17:07:03

CERT-XLM:abusive-content="harmful-speech"
CERT-XLM:abusive-content="spam"
CERT-XLM:abusive-content="violence"
CERT-XLM:vulnerable="vulnerability"
CERT-XLM:vulnerable="vulnerable-service"

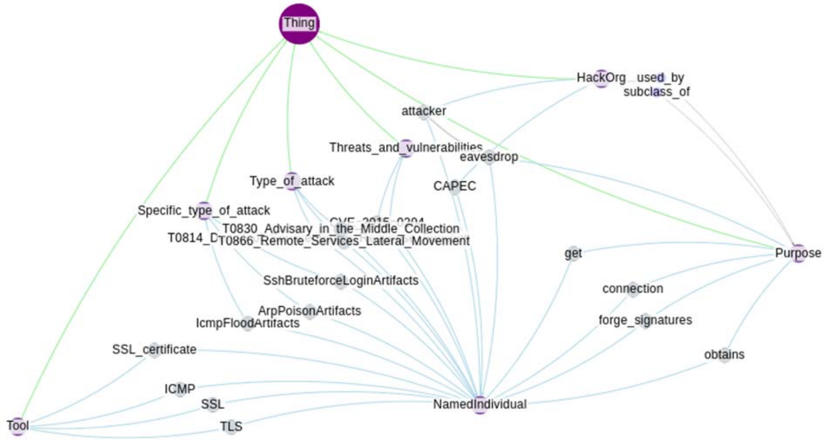
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

Ontology visualization environment

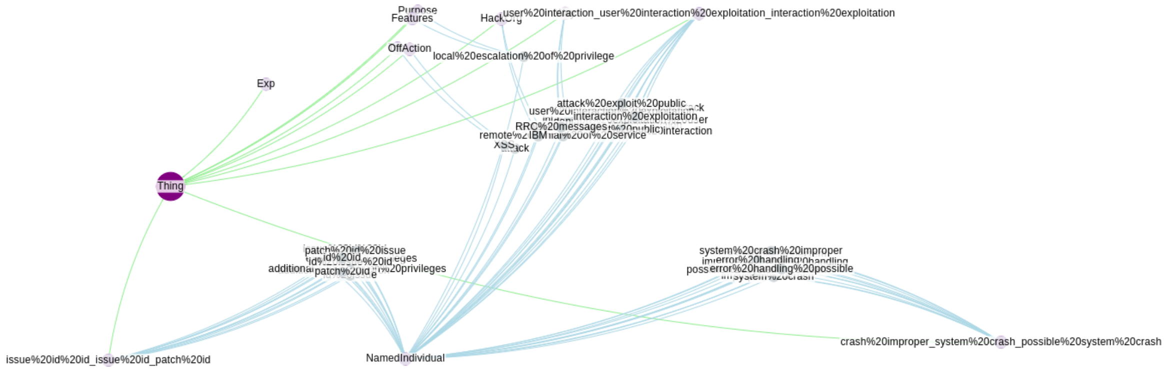


This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

Ontology generation



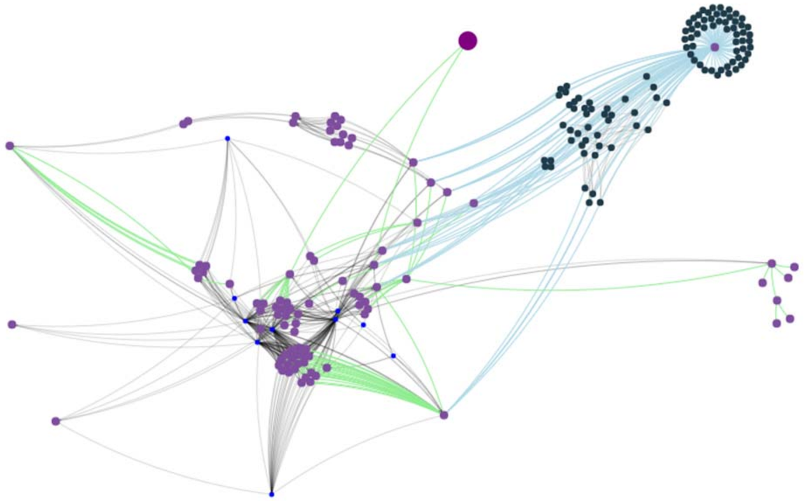
Ontology generation from internal sources


Purpose
Features
HackOrg
user%20interaction_user%20interaction%20exploitation_interaction%20exploitation
OffAction
local%20escalation%20of%20privilege
Exp
attack%20exploit%20public
interaction%20exploitation
RRC%20messages
interaction
remote
IBM
XSS
attack
Thing
patch%20id%20issue
id%20id
additional
patch%20id
privileges
system%20crash%20improper
error%20handling
error%20handling%20possible
system%20crash
issue%20id%20id_issue%20id_patch%20id
NamedIndividual
crash%20improper_system%20crash_possible%20system%20crash

Ontology generated from different external sources

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.

Ontologies' update



MALOnt update

IoTSec updated

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 - INTRA

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.

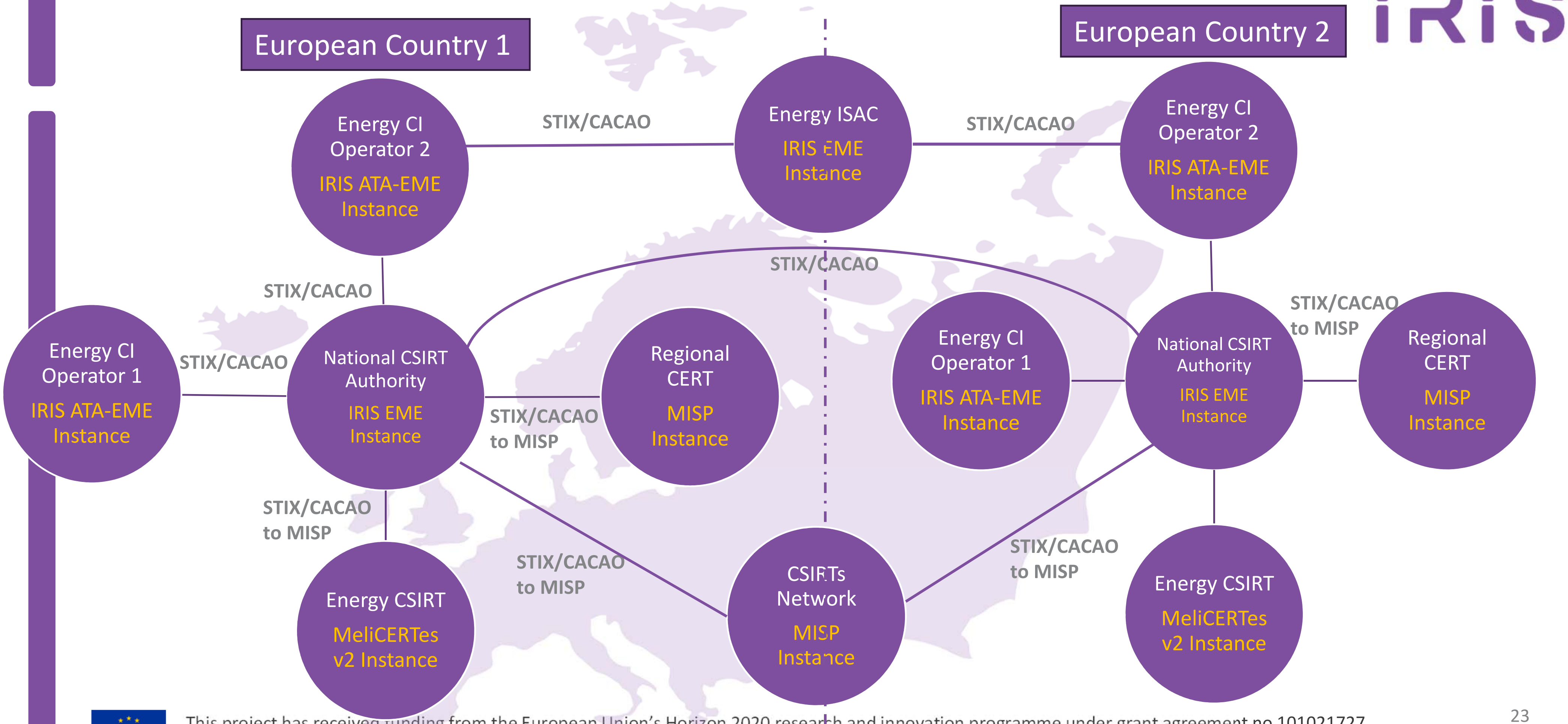
Key objectives: Extend MeliCERTes v2 open-source platform incorporating IRIS CTI developments to enable:

- **Secure and efficient security information representation** in **standardized** formats (STIX v2.1 / CACAO / MISP) → interoperability within and across IRIS Platform
- **Secure disclosable AI- & IoT-relevant CTI information sharing and collaboration among need to know stakeholders**
  - ✓ 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**
- Provision of **advanced and unified dashboard for incident reporting, situational awareness, response actions configuration and recommendation (EME UI)**
- Offering Authentication and Authorization **AAA** services
- **Distributed architecture – ecosystem**
  - ✓ **Instances** deployed at **stakeholders' premises (CI Operators/OESs & CERTs/CSIRTs authorities)**

MISP
Threat Sharing

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



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

- 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

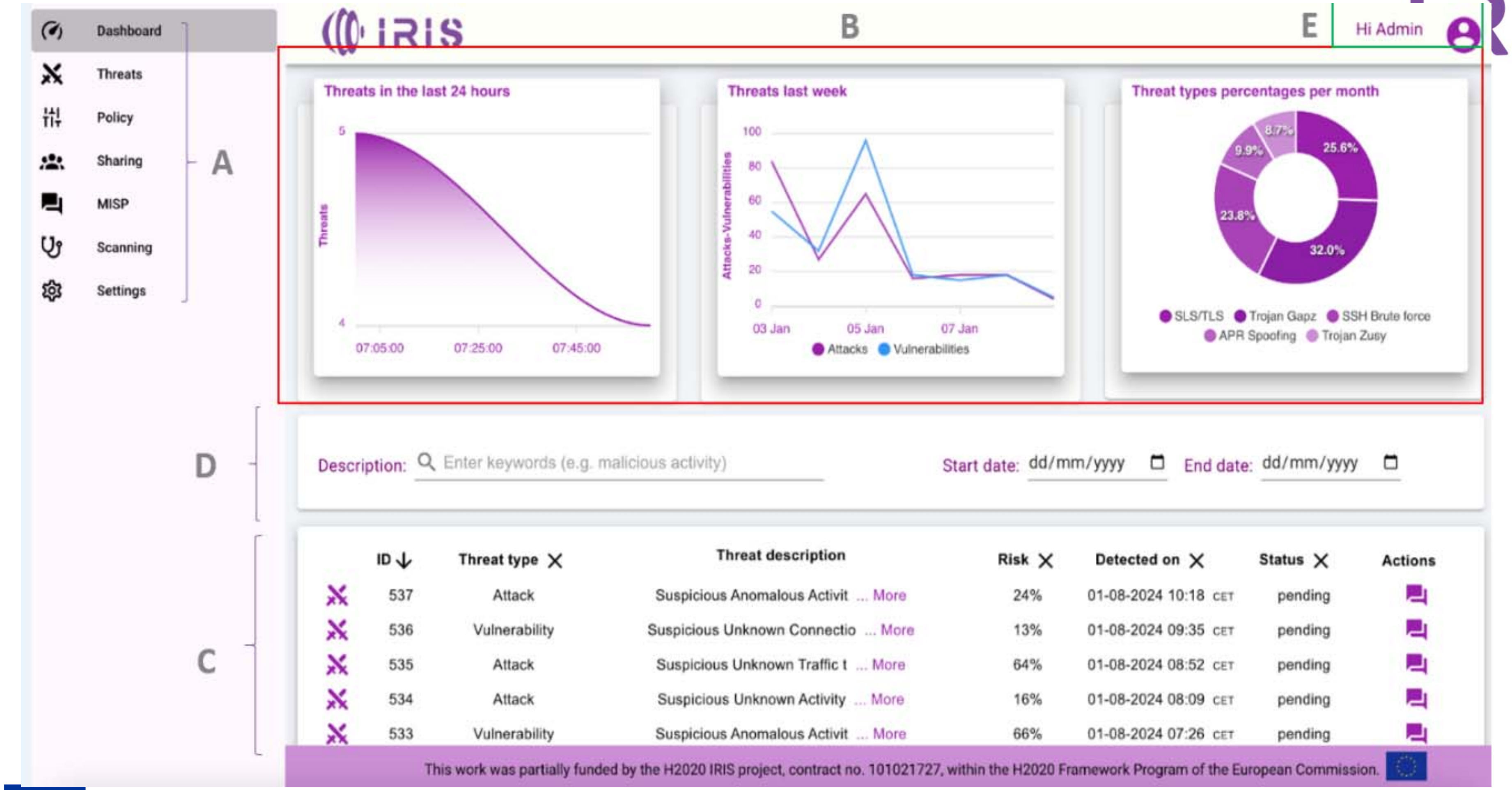
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

IRIS-EME Cerebrate for Trust Communities

- 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.

EME – CI operator view



Description: Enter keywords (e.g. malicious activity)

Start date: dd/mm/yyyy

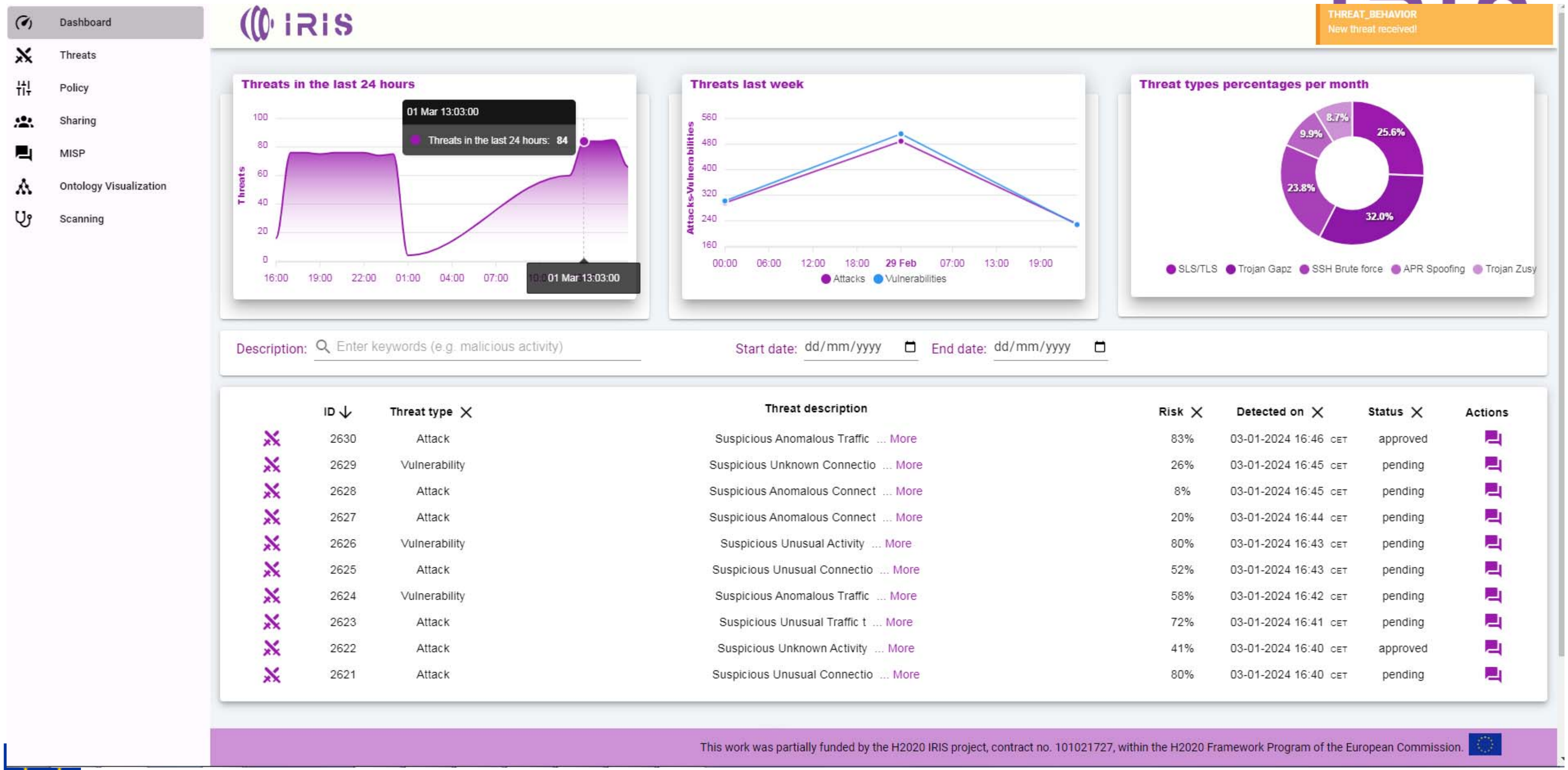
End date: dd/mm/yyyy

	ID ↓	Threat type ✕	Threat description	Risk ✕	Detected on ✕	Status ✕	Actions
✕	537	Attack	Suspicious Anomalous Activit ... More	24%	01-08-2024 10:18 CET	pending	
✕	536	Vulnerability	Suspicious Unknown Connectio ... More	13%	01-08-2024 09:35 CET	pending	
✕	535	Attack	Suspicious Unknown Traffic t ... More	64%	01-08-2024 08:52 CET	pending	
✕	534	Attack	Suspicious Unknown Activity ... More	16%	01-08-2024 08:09 CET	pending	
✕	533	Vulnerability	Suspicious Anomalous Activit ... More	66%	01-08-2024 07:26 CET	pending	

This work was partially funded by the H2020 IRIS project, contract no. 101021727, within the H2020 Framework Program of the European Commission.

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



THREAT_BEHAVIOR
New threat received!

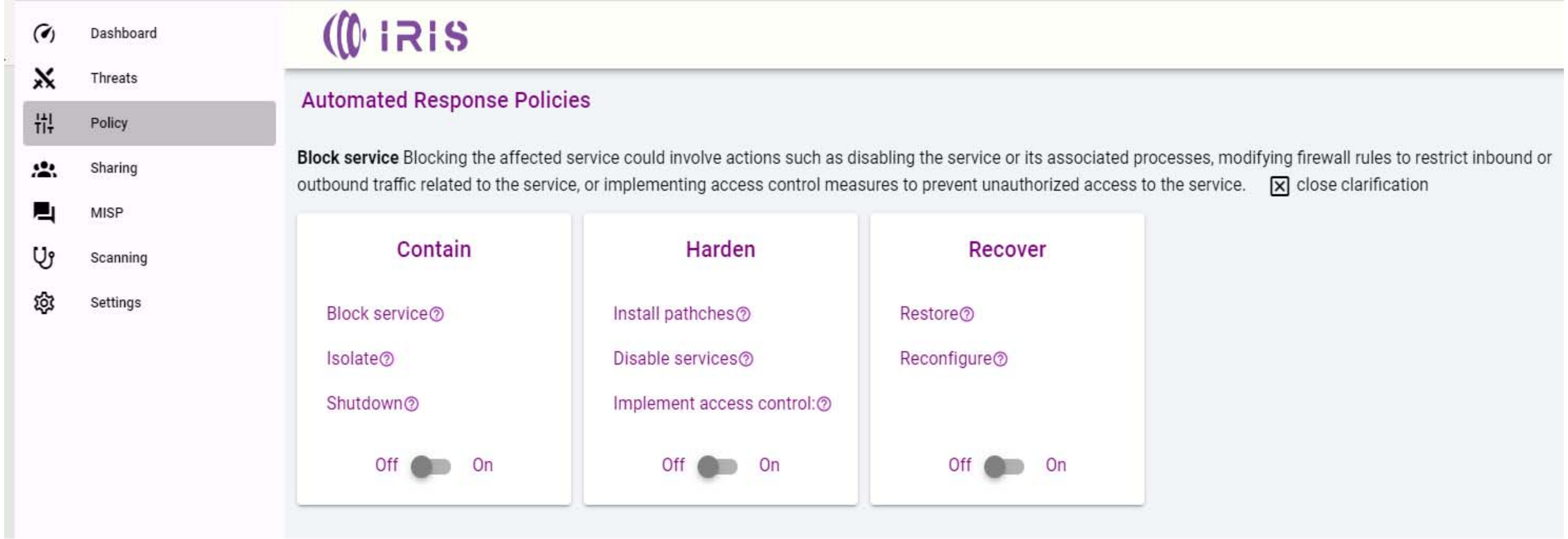
Description: Enter keywords (e.g. malicious activity) Start date: dd/mm/yyyy End date: dd/mm/yyyy

	ID ↓	Threat type ✕	Threat description	Risk ✕	Detected on ✕	Status ✕	Actions
	2630	Attack	Suspicious Anomalous Traffic ... More	83%	03-01-2024 16:46 CET	approved	
	2629	Vulnerability	Suspicious Unknown Connectio ... More	26%	03-01-2024 16:45 CET	pending	
	2628	Attack	Suspicious Anomalous Connect ... More	8%	03-01-2024 16:45 CET	pending	
	2627	Attack	Suspicious Anomalous Connect ... More	20%	03-01-2024 16:44 CET	pending	
	2626	Vulnerability	Suspicious Unusual Activity ... More	80%	03-01-2024 16:43 CET	pending	
	2625	Attack	Suspicious Unusual Connectio ... More	52%	03-01-2024 16:43 CET	pending	
	2624	Vulnerability	Suspicious Anomalous Traffic ... More	58%	03-01-2024 16:42 CET	pending	
	2623	Attack	Suspicious Unusual Traffic t ... More	72%	03-01-2024 16:41 CET	pending	
	2622	Attack	Suspicious Unknown Activity ... More	41%	03-01-2024 16:40 CET	approved	
	2621	Attack	Suspicious Unusual Connectio ... More	80%	03-01-2024 16:40 CET	pending	

This work was partially funded by the H2020 IRIS project, contract no. 101021727, within the H2020 Framework Program of the European Commission.

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



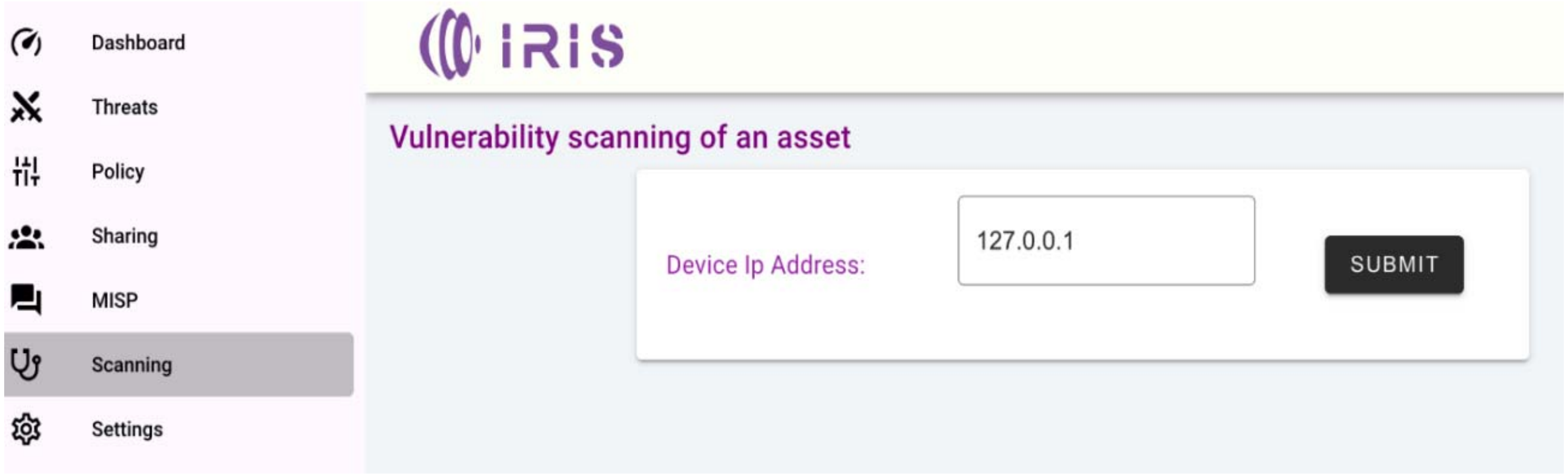
Automated Response Policies

Block service Blocking the affected service could involve actions such as disabling the service or its associated processes, modifying firewall rules to restrict inbound or outbound traffic related to the service, or implementing access control measures to prevent unauthorized access to the service. ☒ close clarification

Contain	Harden	Recover
Block service⍰	Install pathches⍰	Restore⍰
Isolate⍰	Disable services⍰	Reconfigure⍰
Shutdown⍰	Implement access control:⍰	
Off ● On	Off ● On	Off ● On

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 – Vulnerability Scanning

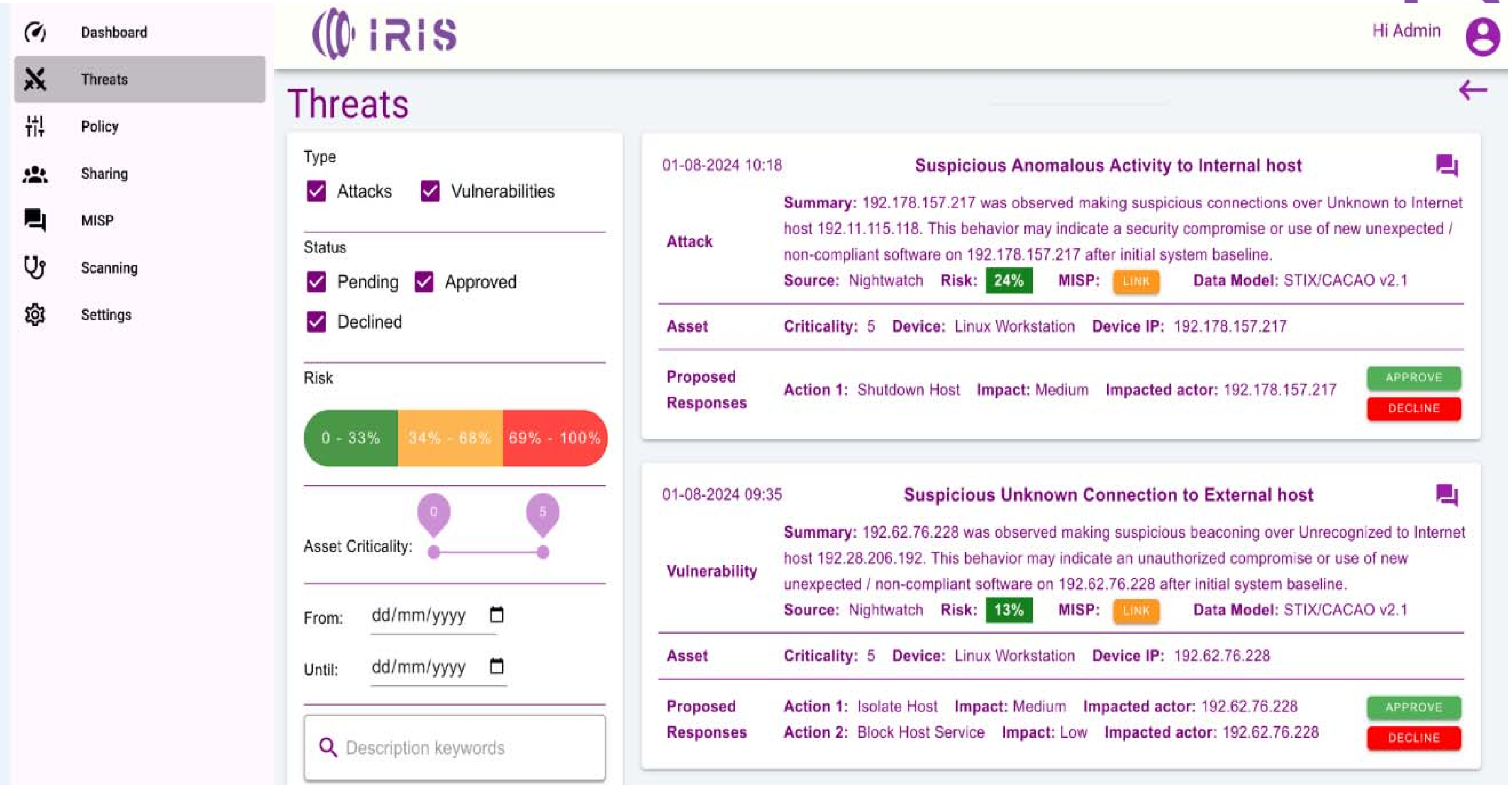


Vulnerability scanning of an asset

Device Ip Address: 127.0.0.1

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 Attacks view



Threats

Type
☑ Attacks ☑ Vulnerabilities

Status
☑ Pending ☑ Approved
☑ Declined

Risk
0 - 33% | 34% - 68% | 69% - 100%

Asset Criticality: 0 – 5

From: dd/mm/yyyy
Until: dd/mm/yyyy

Description keywords

01-08-2024 10:18 **Suspicious Anomalous Activity to Internal host**

Attack
Summary: 192.178.157.217 was observed making suspicious connections over Unknown to Internet host 192.11.115.118. This behavior may indicate a security compromise or use of new unexpected / non-compliant software on 192.178.157.217 after initial system baseline.
Source: Nightwatch **Risk:** 24% **MISP:** LINK **Data Model:** STIX/CACAO v2.1

Asset **Criticality:** 5 **Device:** Linux Workstation **Device IP:** 192.178.157.217

Proposed Responses **Action 1:** Shutdown Host **Impact:** Medium **Impacted actor:** 192.178.157.217

01-08-2024 09:35 **Suspicious Unknown Connection to External host**

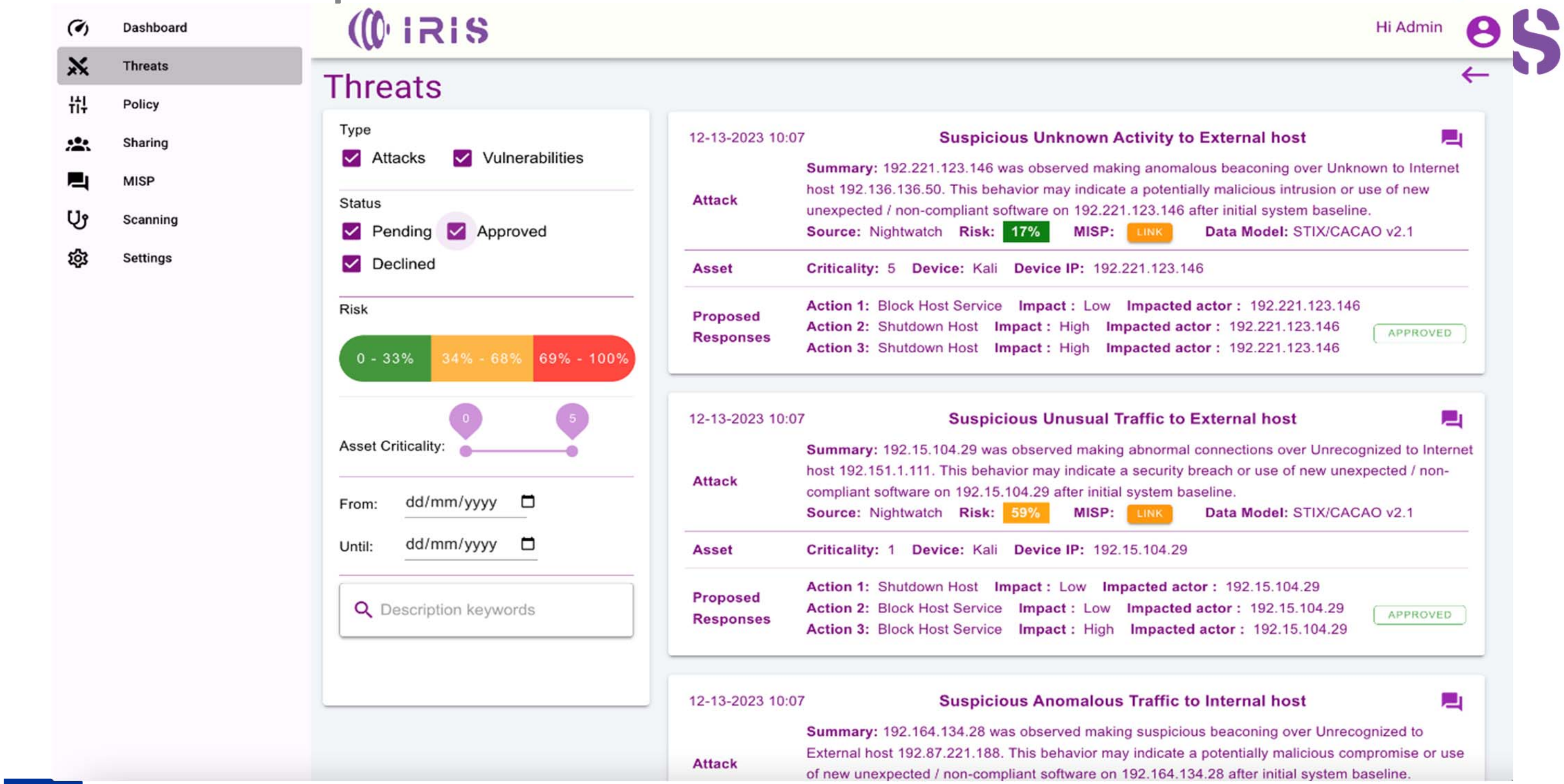
Vulnerability
Summary: 192.62.76.228 was observed making suspicious beaconing over Unrecognized to Internet host 192.28.206.192. This behavior may indicate an unauthorized compromise or use of new unexpected / non-compliant software on 192.62.76.228 after initial system baseline.
Source: Nightwatch **Risk:** 13% **MISP:** LINK **Data Model:** STIX/CACAO v2.1

Asset **Criticality:** 5 **Device:** Linux Workstation **Device IP:** 192.62.76.228

Proposed Responses
Action 1: Isolate Host **Impact:** Medium **Impacted actor:** 192.62.76.228
Action 2: Block Host Service **Impact:** Low **Impacted actor:** 192.62.76.228

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



Threats

Type
☑ Attacks ☑ Vulnerabilities

Status
☑ Pending ☑ Approved
☑ Declined

Risk
0 - 33% | 34% - 68% | 69% - 100%

Asset Criticality: 0 – 5

From: dd/mm/yyyy
Until: dd/mm/yyyy

Description keywords

12-13-2023 10:07 **Suspicious Unknown Activity to External host**

Attack
Summary: 192.221.123.146 was observed making anomalous beaconing over Unknown to Internet host 192.136.136.50. This behavior may indicate a potentially malicious intrusion or use of new unexpected / non-compliant software on 192.221.123.146 after initial system baseline.
Source: Nightwatch **Risk:** 17% **MISP:** LINK **Data Model:** STIX/CACAO v2.1

Asset **Criticality:** 5 **Device:** Kali **Device IP:** 192.221.123.146

Proposed Responses
Action 1: Block Host Service **Impact :** Low **Impacted actor :** 192.221.123.146
Action 2: Shutdown Host **Impact :** High **Impacted actor :** 192.221.123.146
Action 3: Shutdown Host **Impact :** High **Impacted actor :** 192.221.123.146
APPROVED

12-13-2023 10:07 **Suspicious Unusual Traffic to External host**

Attack
Summary: 192.15.104.29 was observed making abnormal connections over Unrecognized to Internet host 192.151.1.111. This behavior may indicate a security breach or use of new unexpected / non-compliant software on 192.15.104.29 after initial system baseline.
Source: Nightwatch **Risk:** 59% **MISP:** LINK **Data Model:** STIX/CACAO v2.1

Asset **Criticality:** 1 **Device:** Kali **Device IP:** 192.15.104.29

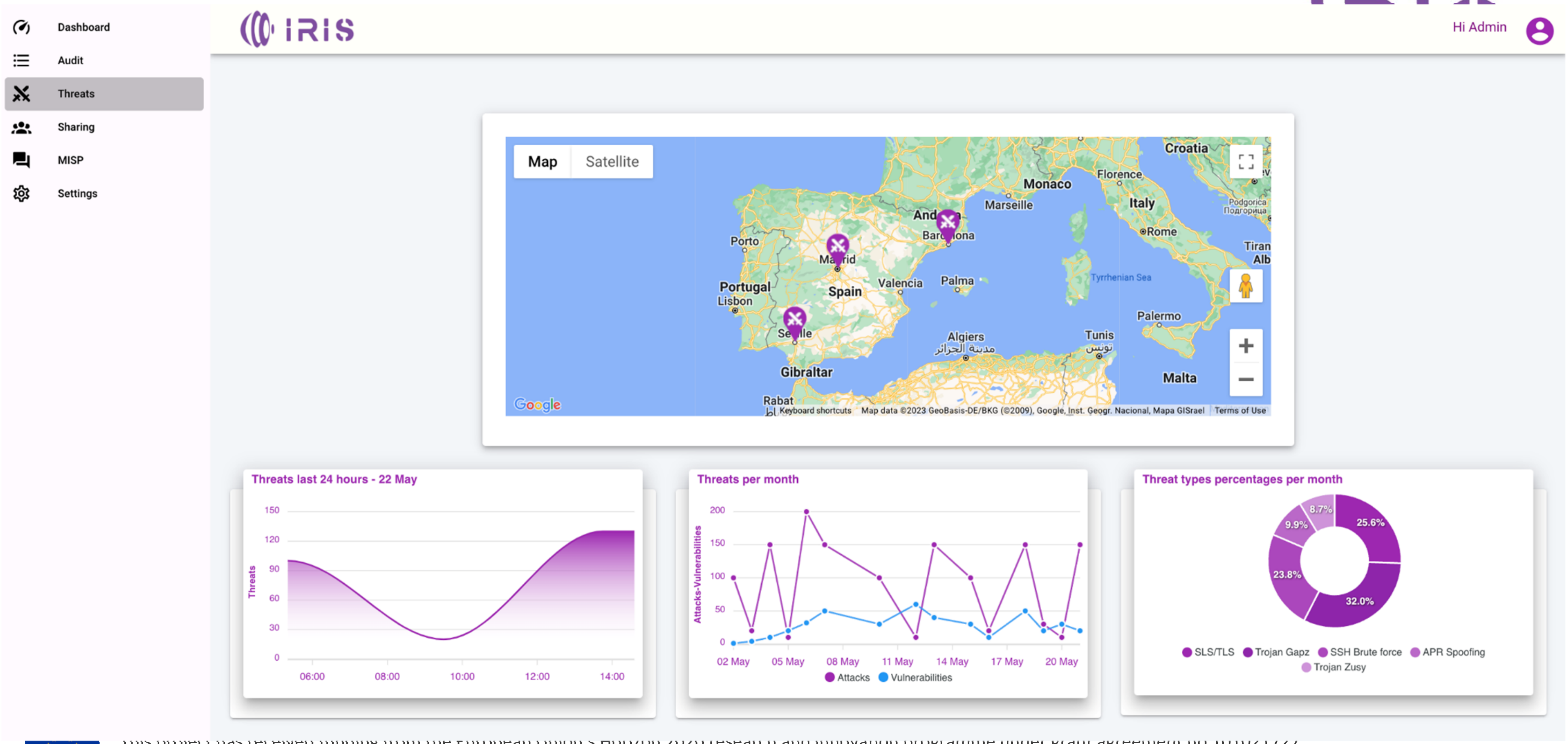
Proposed Responses
Action 1: Shutdown Host **Impact :** Low **Impacted actor :** 192.15.104.29
Action 2: Block Host Service **Impact :** Low **Impacted actor :** 192.15.104.29
Action 3: Block Host Service **Impact :** High **Impacted actor :** 192.15.104.29
APPROVED

12-13-2023 10:07 **Suspicious Anomalous Traffic to Internal host**

Attack
Summary: 192.164.134.28 was observed making suspicious beaconing over Unrecognized to External host 192.87.221.188. This behavior may indicate a potentially malicious compromise or use of new unexpected / non-compliant software on 192.164.134.28 after initial system baseline.

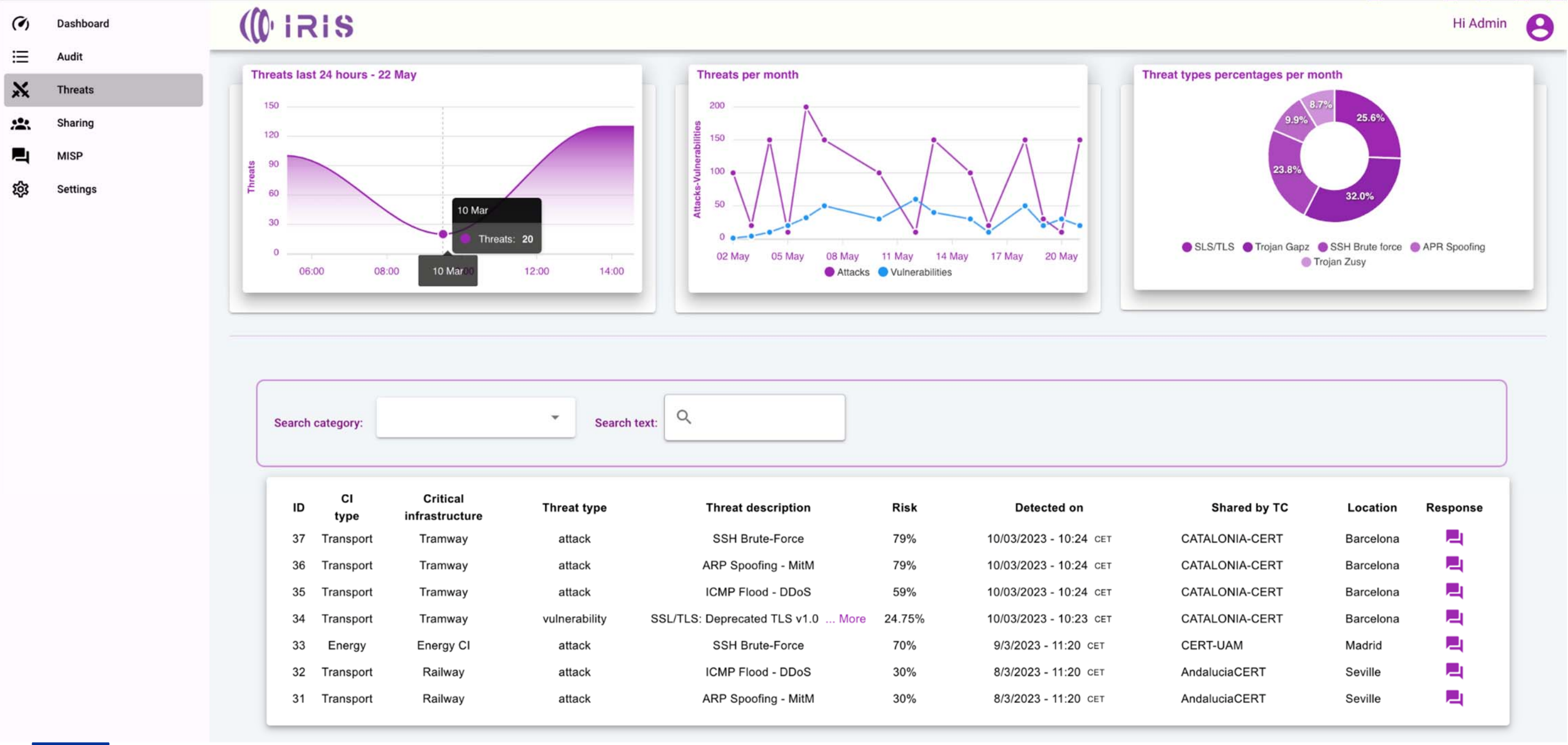
This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors’ view and European Commission is not responsible for any use that may be made of the information it contains.

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.

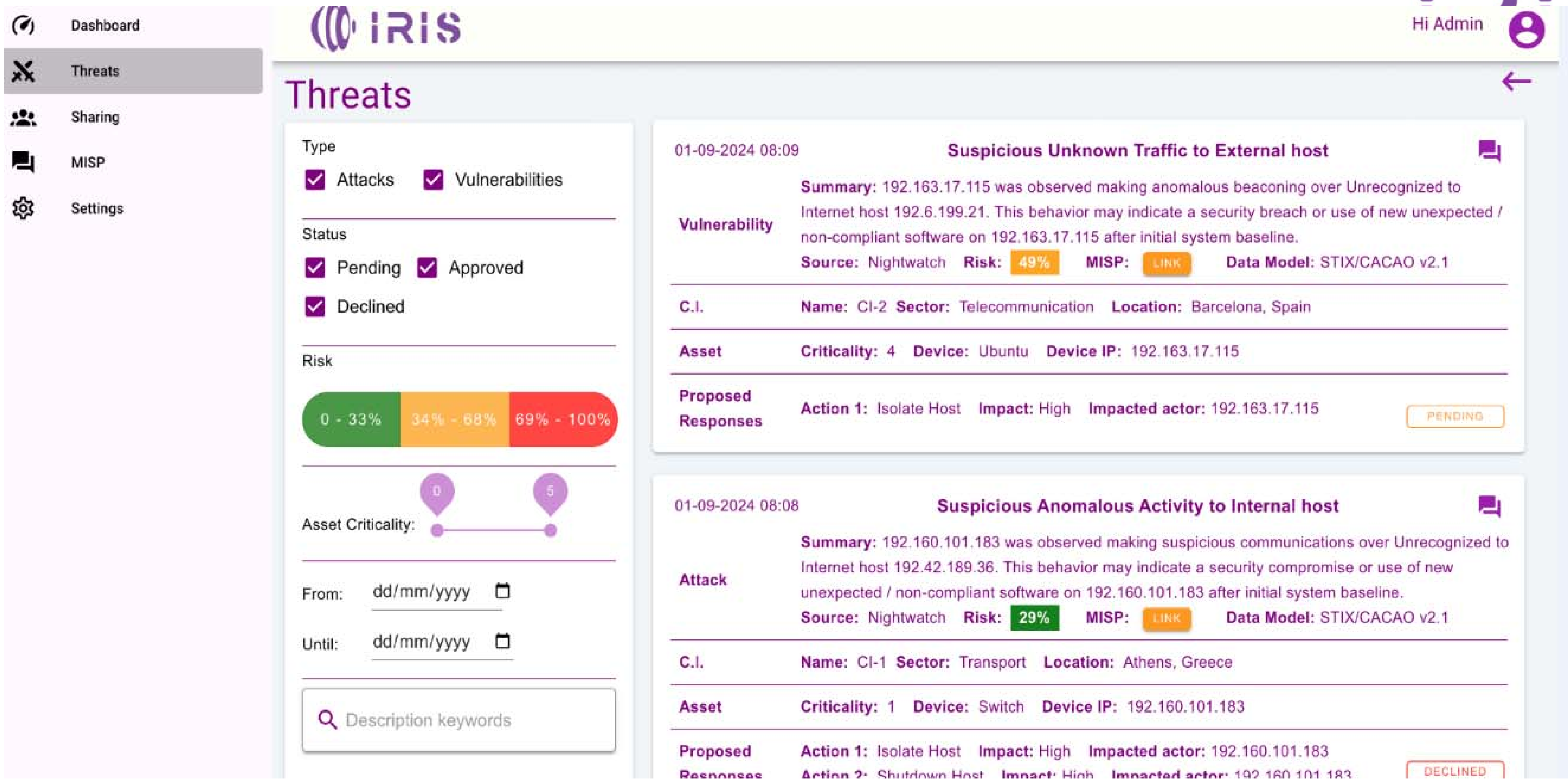
EME – CERT/CSIRT authority view



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.

EME – CERT/CSIRT authority view



Threats

Type
☑ Attacks ☑ Vulnerabilities

Status
☑ Pending ☑ Approved
☑ Declined

Risk
0 - 33% | 34% - 68% | 69% - 100%

Asset Criticality: 0 – 5

From: dd/mm/yyyy

Until: dd/mm/yyyy

Description keywords

01-09-2024 08:09 **Suspicious Unknown Traffic to External host**

Vulnerability	**Summary:** 192.163.17.115 was observed making anomalous beaconing over Unrecognized to Internet host 192.6.199.21. This behavior may indicate a security breach or use of new unexpected / non-compliant software on 192.163.17.115 after initial system baseline. **Source:** Nightwatch **Risk:** 49% **MISP:** LINK **Data Model:** STIX/CACAO v2.1
C.I.	**Name:** CI-2 **Sector:** Telecommunication **Location:** Barcelona, Spain
Asset	**Criticality:** 4 **Device:** Ubuntu **Device IP:** 192.163.17.115
Proposed Responses	**Action 1:** Isolate Host **Impact:** High **Impacted actor:** 192.163.17.115 PENDING

01-09-2024 08:08 **Suspicious Anomalous Activity to Internal host**

Attack	**Summary:** 192.160.101.183 was observed making suspicious communications over Unrecognized to Internet host 192.42.189.36. This behavior may indicate a security compromise or use of new unexpected / non-compliant software on 192.160.101.183 after initial system baseline. **Source:** Nightwatch **Risk:** 29% **MISP:** LINK **Data Model:** STIX/CACAO v2.1
C.I.	**Name:** CI-1 **Sector:** Transport **Location:** Athens, Greece
Asset	**Criticality:** 1 **Device:** Switch **Device IP:** 192.160.101.183
Proposed Responses	**Action 1:** Isolate Host **Impact:** High **Impacted actor:** 192.160.101.183 **Action 2:** Shutdown Host **Impact:** High **Impacted actor:** 192.160.101.183 DECLINED

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

Thank you! Questions?

SECURE CYBER CLUSTER

Cyber Threat Intelligence: Empowering IoT Security

6 March 2024
Online

iris-h2020.eu

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.