Artificial Intelligence Threat Reporting & Incidence report system

Standardization and Policy Development Work within IRIS – SKILLAB

ATLANTIS, EU-CIP, and ECSCI Cluster Joint Webinar

Fortifying the Future: How EU R&D Projects can Shape Standards and Policies in Critical Infrastructure Protection

10th Dec. 2024

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

Senior Research and Innovation Manager – Expert

Netcompany - Intrasoft

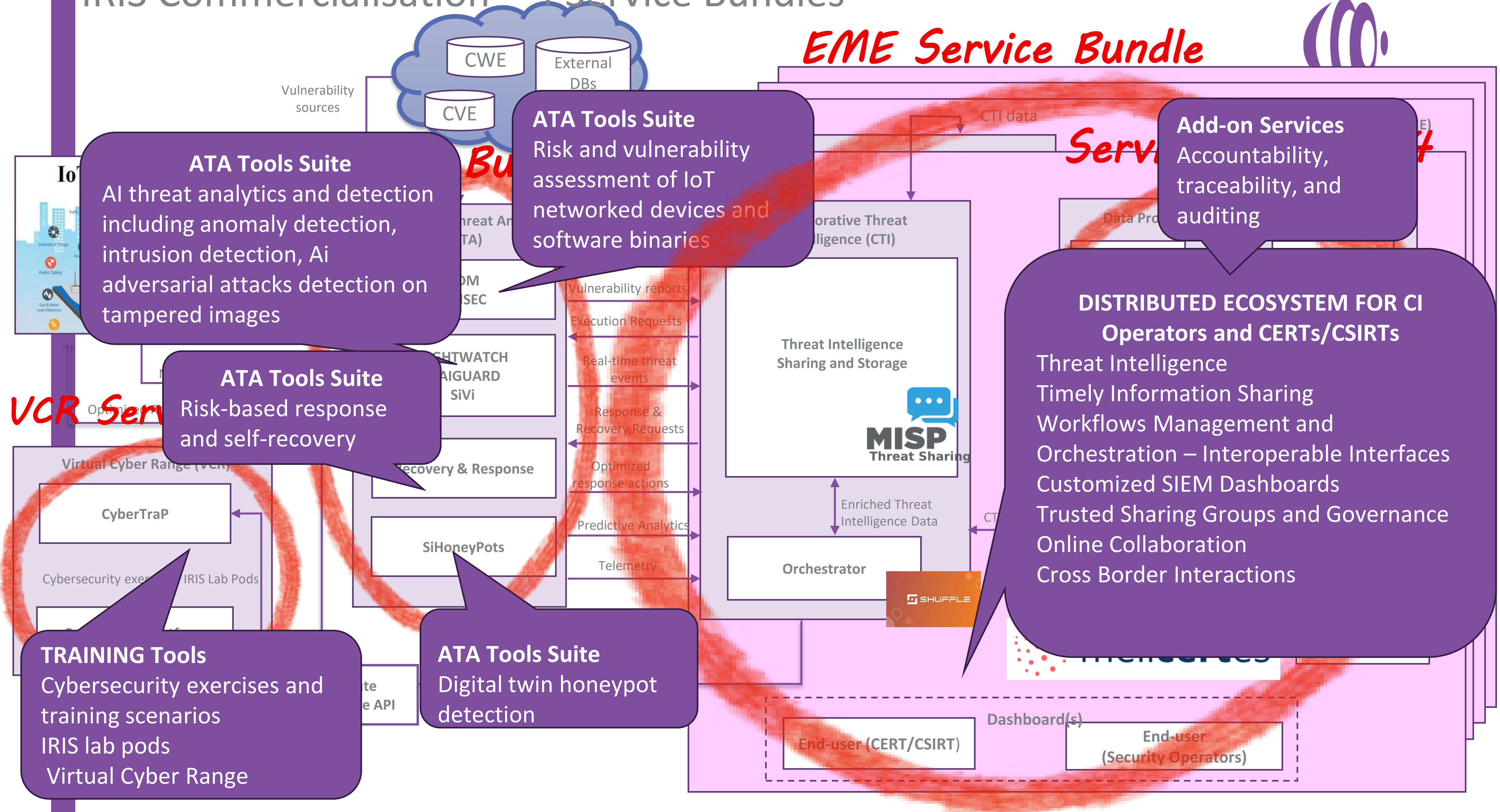
IRIS in a Nutshell

- **H2020 IRIS Project -** A collaborative CERT/CSIRT platform to combat cyber-threats in IoT and AI-driven systems – finished Aug. 2024
- 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

IRIS Platform Innovations

- **An all in one integrated and distributed ecosystem with** loosely coupled architecture, enabling:
  - ✓Automated diverse vulnerabilities and threat/attack detection **on IoT and AI-driven infrastructures** of smart cities (cross CI)
  - ✓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 Situational Awareness and Online Collaboration among **Need to Know Stakeholders** (OES and CERTs/CSIRTs) to manage a threat/incident
  - ✓Closing the loop: Semi-automated response policies execution and acknowledgement of detected vulnerabilities and threats

IRIS Commercialisation – 4 Service Bundles



ATA Tools Suite
AI threat analytics and detection including anomaly detection, intrusion detection, Ai adversarial attacks detection on tampered images

ATA Tools Suite
Risk and vulnerability assessment of IoT networked devices and software binaries

Add-on Services
Accountability, traceability, and auditing

ATA Tools Suite
Risk-based response and self-recovery

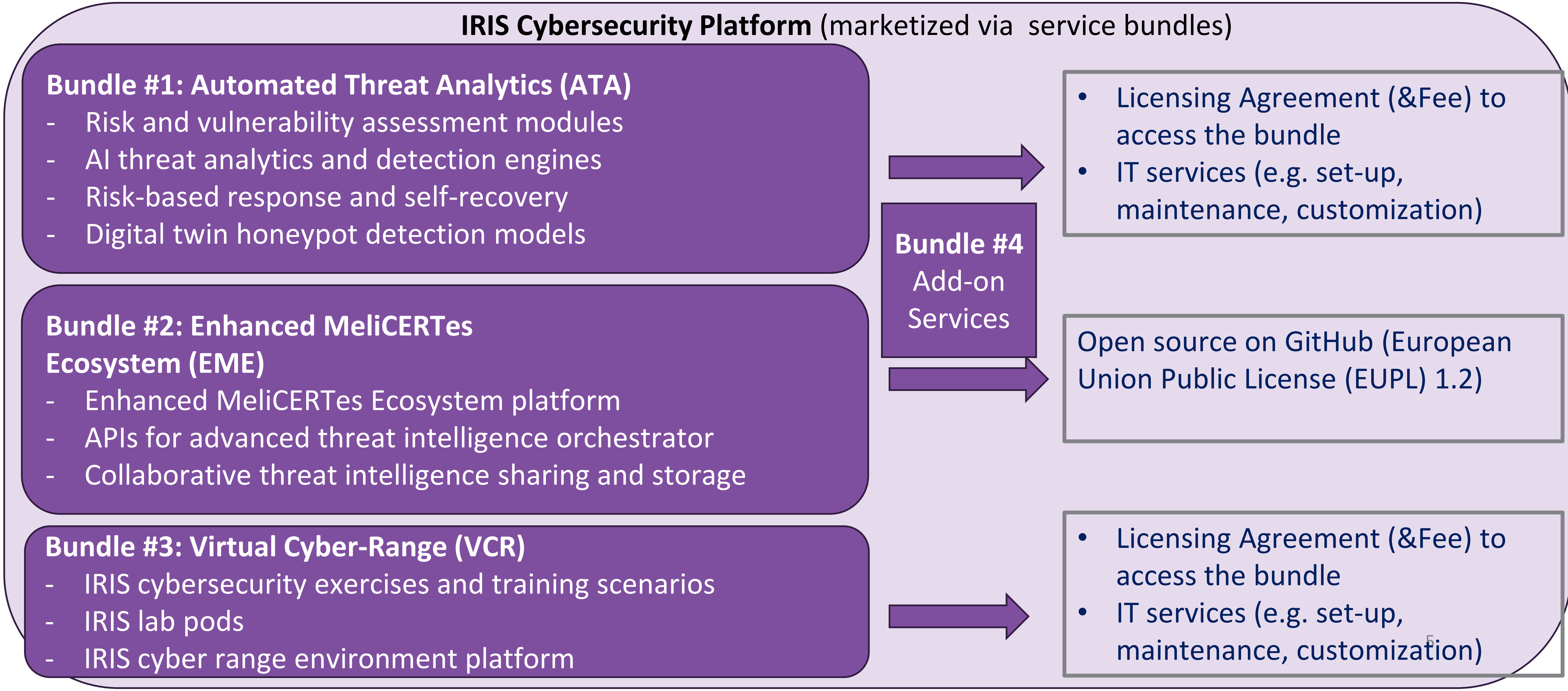
DISTRIBUTED ECOSYSTEM FOR CI Operators and CERTs/CSIRTs
Threat Intelligence
Timely Information Sharing
Workflows Management and Orchestration – Interoperable Interfaces
Customized SIEM Dashboards
Trusted Sharing Groups and Governance
Online Collaboration
Cross Border Interactions

TRAINING Tools
Cybersecurity exercises and training scenarios
IRIS lab pods
Virtual Cyber Range

ATA Tools Suite
Digital twin honeypot detection

Sustainability/ Delivery Model

Deployment details and licensing terms will be discussed with involved partners (service providers)



IRIS Cybersecurity Platform (marketized via service bundles)

Bundle #1: Automated Threat Analytics (ATA)

- Risk and vulnerability assessment modules
- AI threat analytics and detection engines
- Risk-based response and self-recovery
- Digital twin honeypot detection models

Bundle #2: Enhanced MeliCERTes Ecosystem (EME)

- Enhanced MeliCERTes Ecosystem platform
- APIs for advanced threat intelligence orchestrator
- Collaborative threat intelligence sharing and storage

Bundle #3: Virtual Cyber-Range (VCR)

- IRIS cybersecurity exercises and training scenarios
- IRIS lab pods
- IRIS cyber range environment platform

Bundle #4 Add-on Services

- Licensing Agreement (&Fee) to access the bundle
- IT services (e.g. set-up, maintenance, customization)

Open source on GitHub (European Union Public License (EUPL) 1.2)

- Licensing Agreement (&Fee) to access the bundle
- IT services (e.g. set-up, maintenance, customization)

EME capitalizes on widely known and used open source software tools

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.

SHUFFLE

MISP Threat Sharing

Adoption of Relevant Standards

- **IRIS** targets interoperability

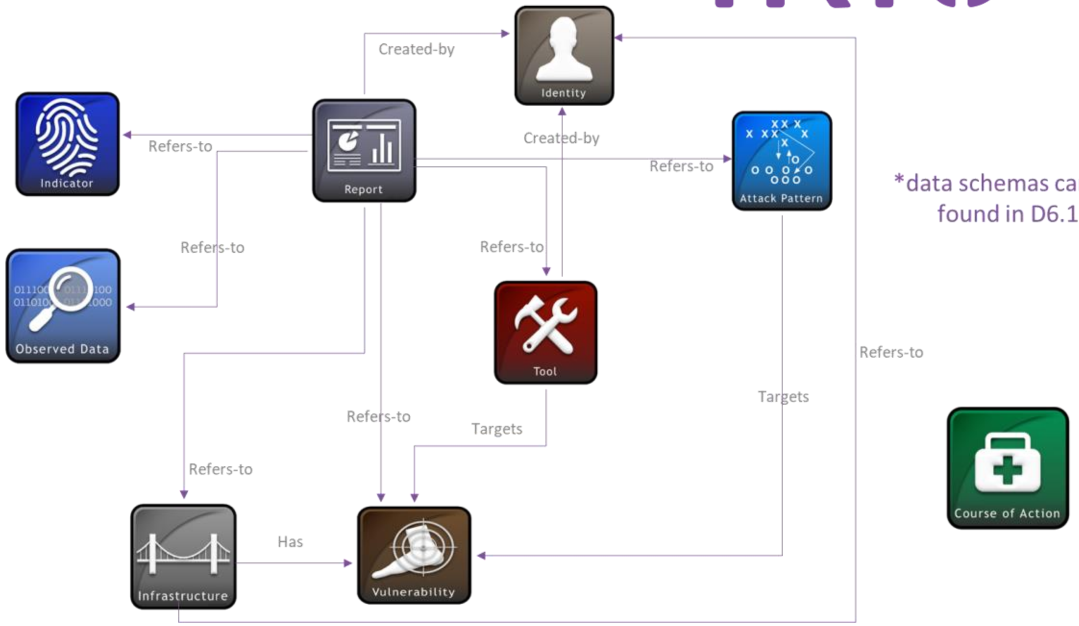
  ✓ **STIX v2.1 is used to describe CTI data enabling their sharing in a consistent way across different systems**, guaranteeing **interoperability (cross-domain and cross-sector)**

  ➢ 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.**

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**

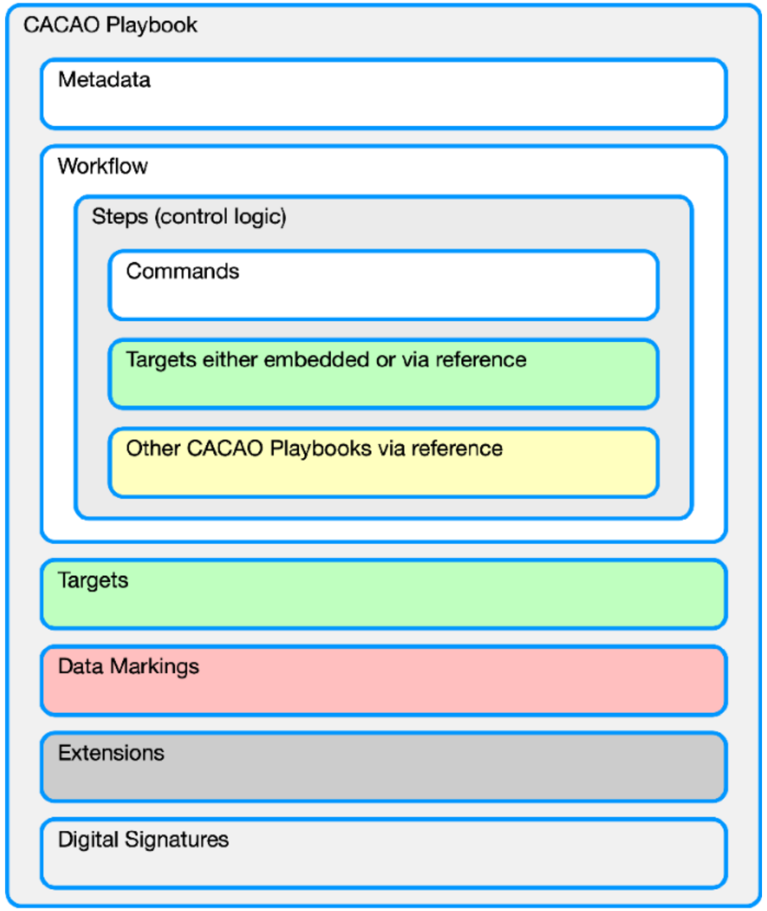


*data schemas can be found in D6.1

STIX v2.1 Data model of IRIS incident report

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

APIs schemas and OpenAPI adoption

Design, Creation of a “Network of APIs” towards Integration

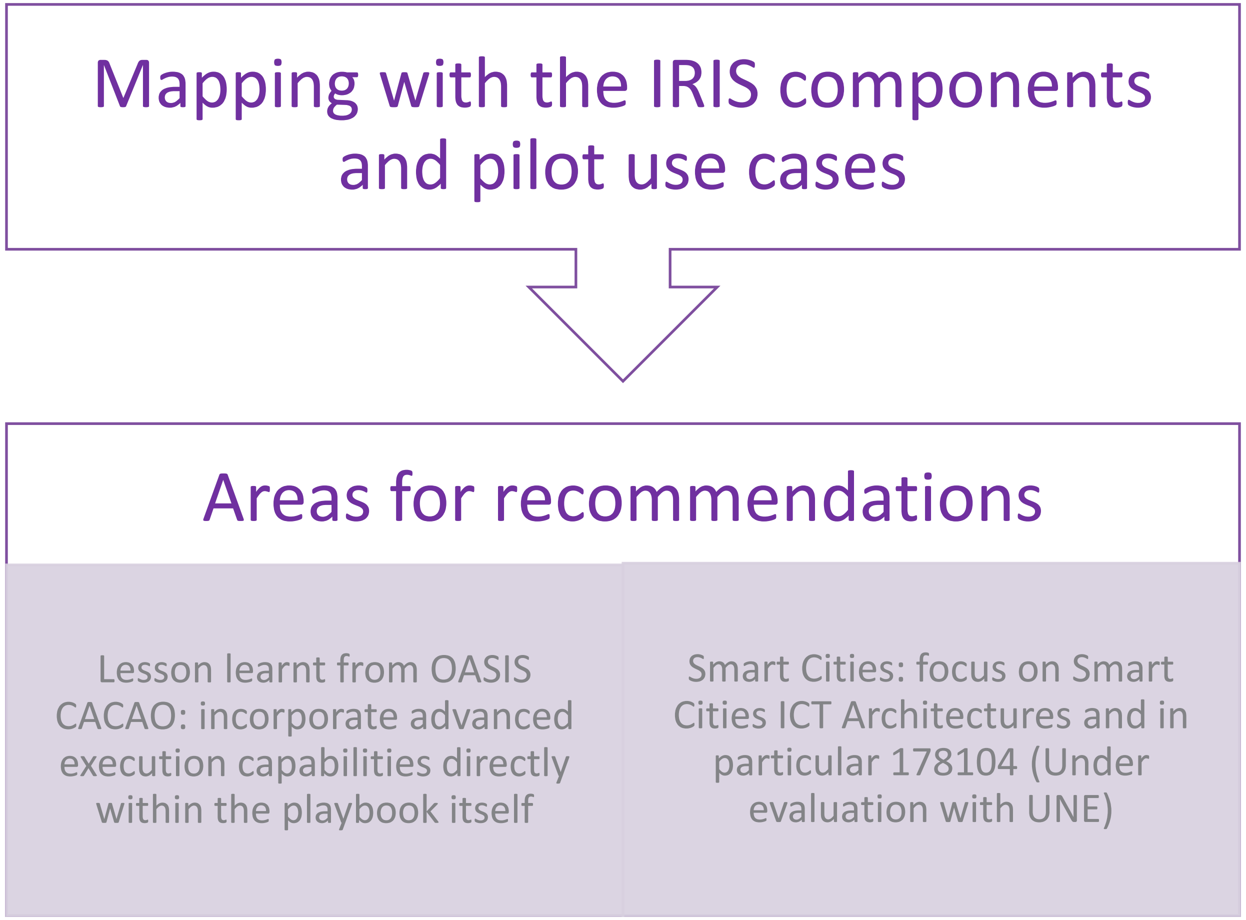
- APIs of vulnerability and threat detection from the infrastructure following STIX2.1 format.
- APIs for SiHoneypots following STIX2.1 format.
- APIs to send responses to the infrastructure following STIX - CACAO format

Also, there are three (3) additional APIs towards external interfaces

- APIs for DPA module following a customised format.
- APIs for MISP, following STIX2.1 format
- APIs for EME, following STIX2.1 format

ATIO APIs definition, the OpenAPI specification was adopted

Contribution to Standardisation



Mapping with the IRIS components and pilot use cases

Areas for recommendations

Lesson learnt from OASIS CACAO: incorporate advanced execution capabilities directly within the playbook itself

Smart Cities: focus on Smart Cities ICT Architectures and in particular 178104 (Under evaluation with UNE)

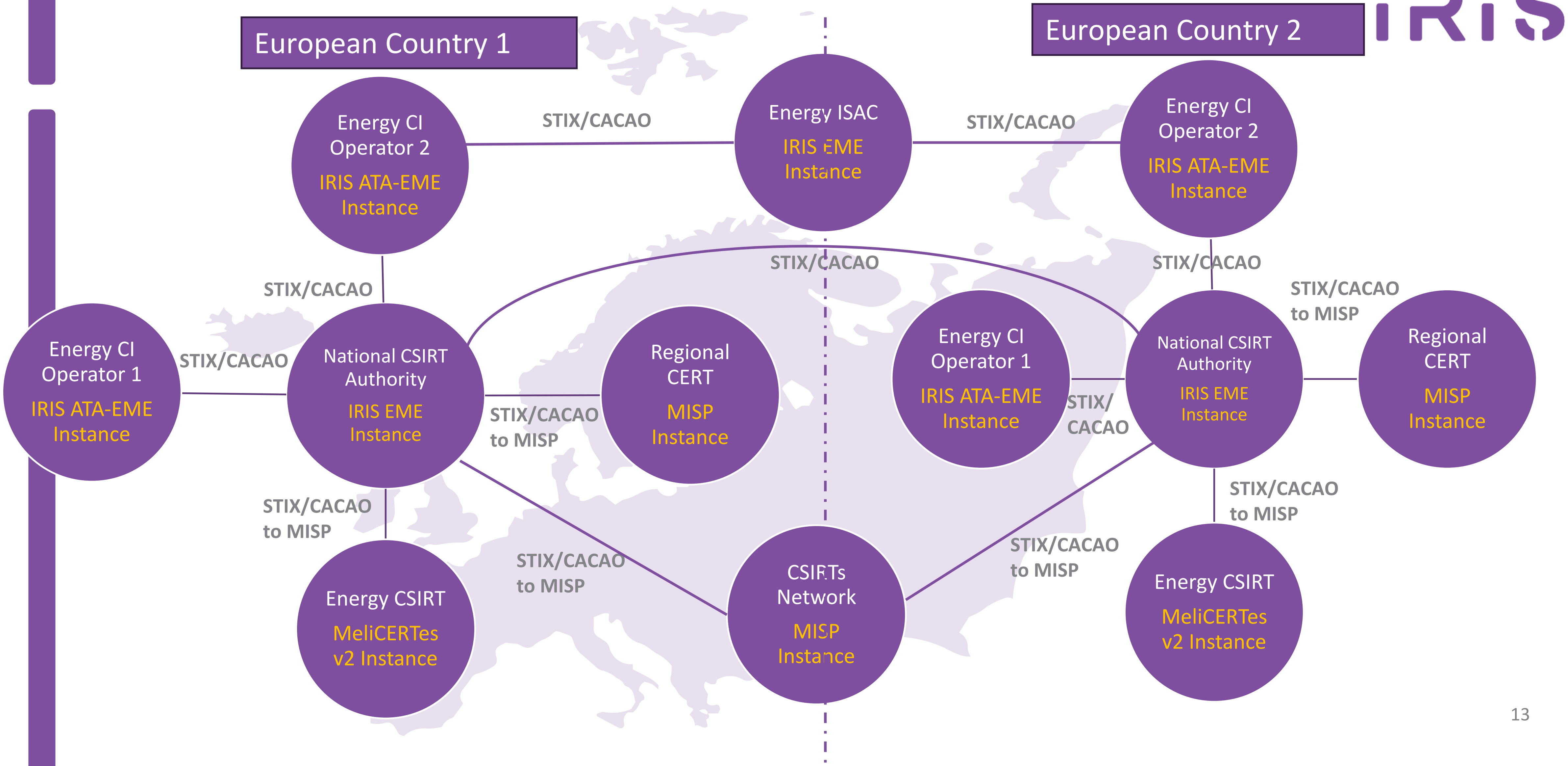
SDOs	TC / WG	Standard	IRIS WP
OASIS	OASIS Cyber Treat Intelligence (CTI) Technical Committee.	Structured Threat Information Expression (STIX™)	Related with WP4 in total and the total scope of the project.
ISO/IEC JTC 1	SC 42	AI standardization.	WP3
ISO/IEC TR 24027 Information technology		Artificial Intelligence (AI) — Bias in AI systems and AI-aided decision making	WP3
ISO/IEC TR 24368:2022		TR Information Technology — Artificial Intelligence — Overview of Ethics and Social Concern	WP3
ISO/IEC/IEEE 29119-11		Software and Systems Engineering — Software Testing — Testing of AI-Based System	WP3
OASIS Open		CACAO: Collaborative Automated Course of Action Operations for Cyber Security	WP3, WP4, WP6
UNE	Spanish agency of normalisation	CTN178	WP7

Compliance to Policies/ Directives

- **NIS2 Directive**: Addressing **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): Addressing 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

Alignment with NIS2 and CER Directives



Support to policies

Network and Information Security (NIS) Directive 2

The NIS2 defines cybersecurity **requirements** for essential and important entities; requirements for the **incident notification**; and rules on enforcement.

Key Provisions

- Risk Assessment
- Security Measures
- Top Management Involvement
- Incident Reporting
- Conformity Assessment
- Enforcement
- National Authorities
- Penalties

IRIS offers valuable suggestions showcasing what end-to-end integrated models are possible to develop or adopt

Compliance to Policies/ Directives

- Cyber Resilience Act (CRA): Adopted **DevSecOps**, incl. **security testing (SAST, DAST) to ensure cybersecurity resilience** of IRIS platform software
  - ✓ Made in Europe, autonomy/sovereignty
- Cyber Solidarity Act: Offer of a **variety of cyber threat detection tools** interoperating with the **distributed Enhanced MeliCERTes ecosystem**, **instances** of which could be used by **cross-border SOCs**, for timely sharing detected threats and incidents among them.

Support to policies

Cyber Solidarity Act Core Pillars

1. European Cybersecurity **Alert System**

Build coordinated detection and common situational awareness capabilities

2. Cybersecurity **Emergency** Mechanism

Support Member States in incident preparedness and management of significant incidents

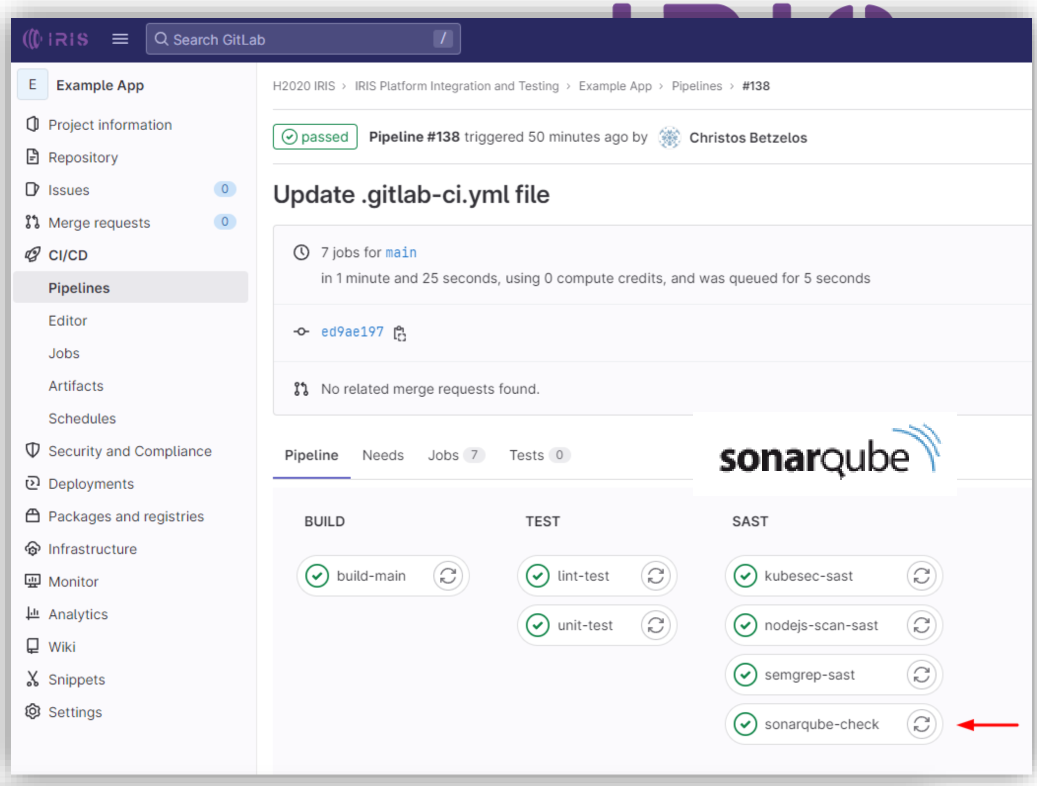
3. Cybersecurity **Incident Review** Mechanism

Review and assess significant or large-scale incidents

IRIS can serve as a proven baseline to demonstrate the existing challenges and the available solutions

IRIS-enhanced MeliCERTes Ecosystem for CRA Compliance

- IRIS adopted 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

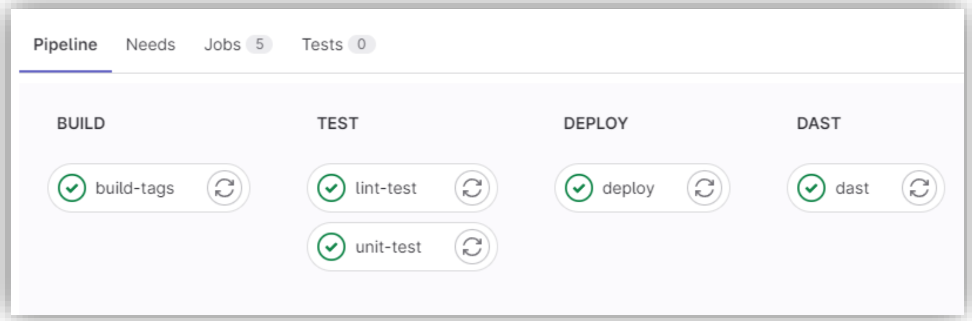
Update .gitlab-ci.yml file

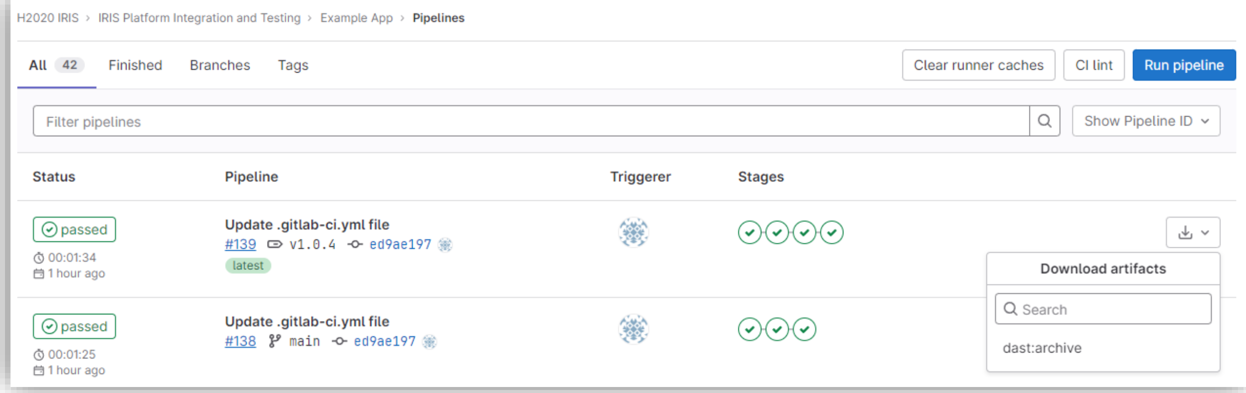
7 jobs for main

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

ed9ae197

No related merge requests found.



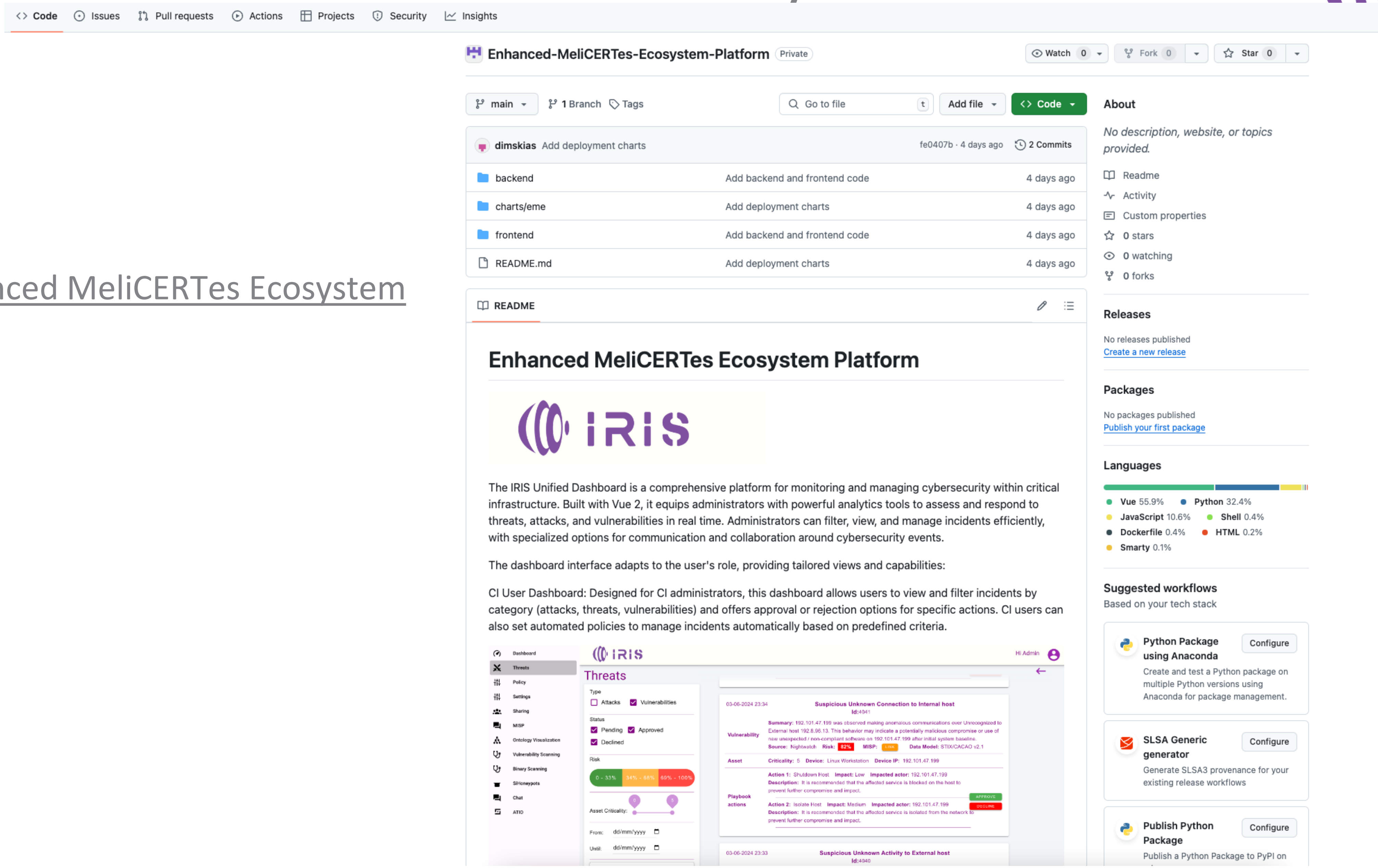


H2020 IRIS › IRIS Platform Integration and Testing › Example App › Pipelines

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 Enhanced MeliCERTes Ecosystem in Github

Enhanced MeliCERTes Ecosystem



Enhanced-MeliCERTes-Ecosystem-Platform Private

dimskias Add deployment charts fe0407b · 4 days ago 2 Commits

backend	Add backend and frontend code	4 days ago
charts/eme	Add deployment charts	4 days ago
frontend	Add backend and frontend code	4 days ago
README.md	Add deployment charts	4 days ago

README

Enhanced MeliCERTes Ecosystem Platform

The IRIS Unified Dashboard is a comprehensive platform for monitoring and managing cybersecurity within critical infrastructure. Built with Vue 2, it equips administrators with powerful analytics tools to assess and respond to threats, attacks, and vulnerabilities in real time. Administrators can filter, view, and manage incidents efficiently, with specialized options for communication and collaboration around cybersecurity events.

The dashboard interface adapts to the user's role, providing tailored views and capabilities:

CI User Dashboard: Designed for CI administrators, this dashboard allows users to view and filter incidents by category (attacks, threats, vulnerabilities) and offers approval or rejection options for specific actions. CI users can also set automated policies to manage incidents automatically based on predefined criteria.

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

03-06-2024 23:34 Suspicious Unknown Connection to Internal host
Id:4041

Vulnerability
Summary: 192.101.47.199 was observed making anomalous communications over Unrecognized to External host 192.8.96.13. This behavior may indicate a potentially malicious compromise or use of new unexpected / non-compliant software on 192.101.47.199 after initial system baseline.
Source: Nightwatch Risk: 82% MISP: LINK Data Model: STIX/CACAO v2.1

Asset
Criticality: 5 Device: Linux Workstation Device IP: 192.101.47.199

Playbook actions
Action 1: Shutdown Host Impact: Low Impacted actor: 192.101.47.199
Description: It is recommended that the affected service is blocked on the host to prevent further compromise and impact.
Action 2: Isolate Host Impact: Medium Impacted actor: 192.101.47.199
Description: It is recommended that the affected service is isolated from the network to prevent further compromise and impact.
APPROVE
DECLINE

03-06-2024 23:33 Suspicious Unknown Activity to External host
Id:4040

About

No description, website, or topics provided.

Readme
Activity
Custom properties
0 stars
0 watching
0 forks

Releases

No releases published
Create a new release

Packages

No packages published
Publish your first package

Languages

Vue 55.9%	Python 32.4%
JavaScript 10.6%	Shell 0.4%
Dockerfile 0.4%	HTML 0.2%
Smarty 0.1%	

Suggested workflows
Based on your tech stack

Python Package using Anaconda — Configure
Create and test a Python package on multiple Python versions using Anaconda for package management.

SLSA Generic generator — Configure
Generate SLSA3 provenance for your existing release workflows

Publish Python Package — Configure
Publish a Python Package to PyPI on

Key Lessons Learnt

- **Alignment with EU legislation and Policies** is time-consuming, requiring the extra mile, but beneficial for results sustainability and adoption by market and stakeholders
- **Monitoring of standards and relevant implementations** among a diverse mix of expertise among partners for standards adoption and interoperability targets is challenging

SKILLAB

SKILLS MATTER

Monitoring the Demand and Supply of Skills in the European Labour Market

https://skillab-project.eu/

Funded by
the European Union

Project duration: Jan 2024 – Dec 2026
Coordinator: Aristotle University of Thessaloniki, Konstantinos Georgiou

This project has received funding from the EU Horizon Europe research and innovation programme under grant agreement No 101132663.

PROJECT AIM

Deliver an **open-source** skill demand/supply identification, analysis and prediction hub for citizens, enterprises, academia, and policy makers.

Funded by
the European Union

A HOLISTIC APPROACH

Develop a skills management and skills shortage identification platform

REGIONAL

Gauge and monitor the European labour market

SECTORAL

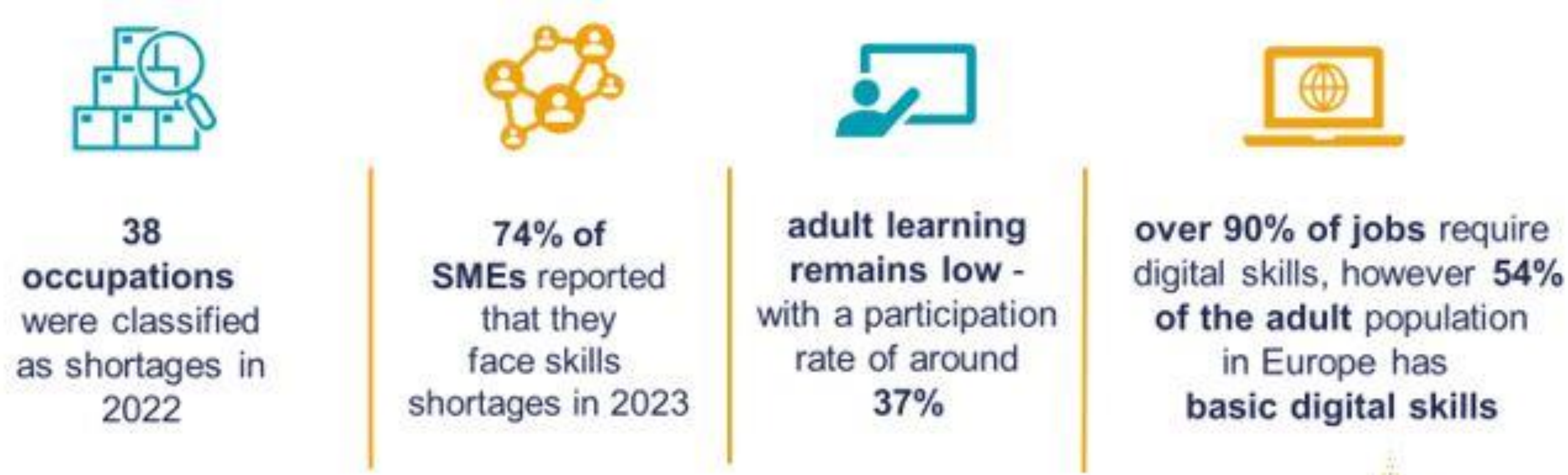
Propose strategies, curricula development, policies

TEMPORAL

Funded by
the European Union

Skills and labour shortages – EYoS

- Skills shortage are a challenge and skilled workforce is an enabler
- 4 objectives: investment, skills relevance, matching skills, attract talent



38 occupations were classified as shortages in 2022

74% of SMEs reported that they face skills shortages in 2023

adult learning remains low - with a participation rate of around **37%**

over 90% of jobs require digital skills, however **54% of the adult** population in Europe has **basic digital skills**

EUROPEAN YEAR OF SKILLS

European Commission

Employment change by sector, EU27, 2022-35

GROWTH

- Information and communication
- Real estate, professional, scientific activities
- Human health and social work
- Accommodation and food services
- Education

SLIGHT GROWTH

- Electricity, gas, stream and air conditioning
- Financial and insurance
- Wholesale and retail
- Administrative and support service activities
- Transport and storage

DECLINE

- Agriculture etc.
- Mining & quarrying
- Construction

SKILLAB KEY FEATURES

Identifying skill shortages and gaps in the labour market.

Recommending personalized reskilling, upskilling, and training plans to EU citizens.

Supporting enterprises in developing their human resources strategy.

Finding ideal candidates for emerging roles and retaining employees.

Providing systematic skill shortages reporting across countries.

Funded by
the European Union

BENEFITS

For Citizens

- Career change opportunities
- Reskilling, upskilling, and personalized training plans
- Monitoring of emerging trends in skills demand

For Enterprises

- Short- and long-term hiring strategies based on skill gaps
- Insights into the company’s skill portfolio and evolution

For Policy Makers

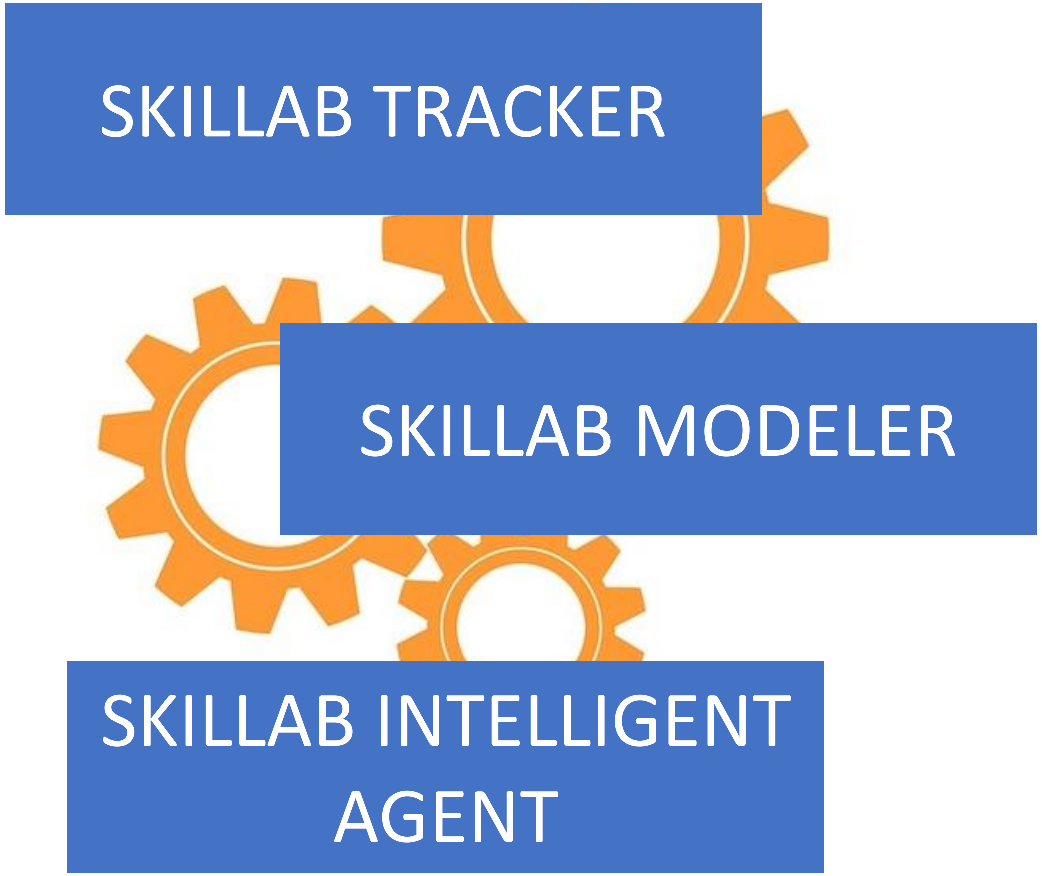
- Identification of blooming and fading market segments
- Systematic reporting on skill shortages across countries

Funded by
the European Union

SKILLAB TECHNOLOGY

Development and deployment of a holistic, open-source skills management and shortage identification platform.

Integrate Advanced **Machine Learning** and **Natural Language Processing** into the analysis of competences.



SKILLAB TRACKER

SKILLAB MODELER

SKILLAB INTELLIGENT AGENT

Funded by
the European Union

ENISA Cybersecurity Skills

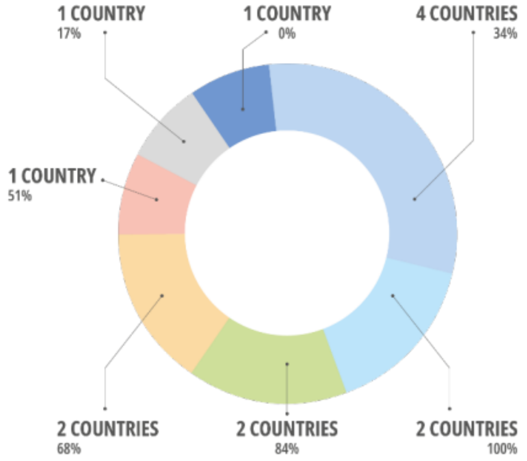
enisa

ENISA is committed to address the **cybersecurity skills gap** through a **comprehensive systemic approach based on education.**

ENISA **supports national authorities by developing initiatives** such as the [Cybersecurity Skills Framework]()

CYBERSECURITY EDUCATION MATURITY ASSESSMENT
May 2024

Figure 9 – Member States' maturity on the inclusion of cybersecurity topics in primary and secondary education curricula

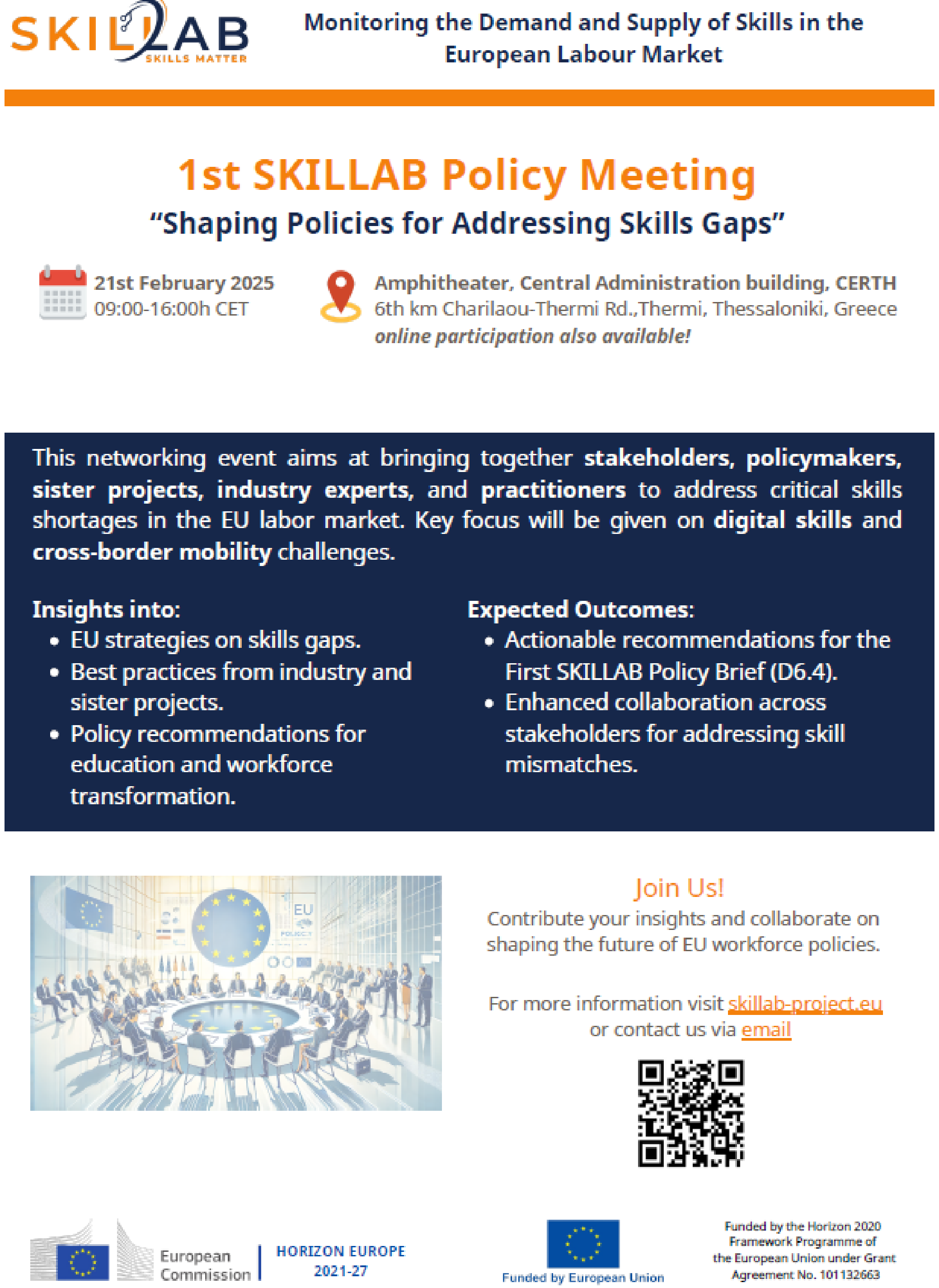


Source: Authors' elaboration (data analysis based on the sampled countries, 13 in total).

Funded by
the European Union

SKILLAB
SKILLS MATTER

SKILLAB 1st Policy Workshop



SKILLAB SKILLS MATTER

Monitoring the Demand and Supply of Skills in the European Labour Market

1st SKILLAB Policy Meeting

"Shaping Policies for Addressing Skills Gaps"

21st February 2025
09:00-16:00h CET

Amphitheater, Central Administration building, CERTH
6th km Charilaou-Thermi Rd.,Thermi, Thessaloniki, Greece
online participation also available!

This networking event aims at bringing together **stakeholders, policymakers, sister projects, industry experts**, and **practitioners** to address critical skills shortages in the EU labor market. Key focus will be given on **digital skills** and **cross-border mobility** challenges.

Insights into:

- EU strategies on skills gaps.
- Best practices from industry and sister projects.
- Policy recommendations for education and workforce transformation.

Expected Outcomes:

- Actionable recommendations for the First SKILLAB Policy Brief (D6.4).
- Enhanced collaboration across stakeholders for addressing skill mismatches.

Join Us!

Contribute your insights and collaborate on shaping the future of EU workforce policies.

For more information visit skillab-project.eu
or contact us via email

European Commission | HORIZON EUROPE 2021-27

Funded by European Union

Funded by the Horizon 2020 Framework Programme of the European Union under Grant Agreement No. 101132663

Funded by the European Union

SKILLAB SKILLS MATTER

Thank you! Questions?

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