Artificial Intelligence Threat Reporting and Incident Response System

D8.4 Interim report on dissemination, communication, standardisation and exploitation

Project Title:	Artificial Intelligence Threat Reporting and Incident Response System
Project Acronym:	IRIS
Deliverable Identifier:	Document number
Deliverable Due Date:	31/8/2023
Deliverable Submission Date:	12/9/2023
Deliverable Version:	1.0
Main author(s) and Organisation:	Maria Tsirigoti, ICCS Konstantinos Chrisiridis, INTRA Sebastijan Cutura, ECSO Roberto Cascella, ECSO
Work Package:	WP8 Dissemination, Communication and Exploitation of Results
Task:	Task 8.1 Dissemination and communication outreach
Dissemination Level:	PU: Public

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

Quality Control

	Name	Organisation	Date
Editor	Maria Tsirigoti	ICCS	07/09/2023
Peer Review 1	Nina Olesen	ECSO	11/08/2023
Peer Review 2	Michaël Marcozzi Sébastien Bardin	CEA	06/09/2023
Submitted by (Project Coordinator)	Gonçalo Cadete	INOV	12/09/2023

Contributors

Organisation
ICCS
INTRA
ECSO

Document History

Version	Date	Modification	Partner
V.01	06/06/2023	ToC	Maria Tsirigoti
V.02	29/06/2023	1st draft	Maria Tsirigoti
V.03	5/07/2023	Input from INTRA, ECSO (exploitation activities- draft version, community building activities)	Konstantinos Chrisiridis, Sebastijan Cutura
V.04	28/07/2023	Input from ECSO (standardisation activities)	Roberto Cascella
V.05	02/08/2023	Final input from INTRA (exploitation activities-final version)	Konstantinos Chrisiridis
V.06	29/089/2023	Implementation of the reviewers' comments (ECSO)	Maria Tsirigoti
V0.7	11/09/2023	Implementation of the reviewers' comments (CEA)	Maria Tsirigoti
V1.0	12/09/2023	Final editing	Gonçalo Cadete

Legal Disclaimer

Contents

1 INTRODUCTION 9

1.1 Project Introduction 9

1.2 Deliverable Purpose 9

1.3 Intended Readership 9

1.4 Relationship with other deliverables and tasks 9

2 DISSEMINATION AND COMMUNICATION CHANNELS AND ACTIVITIES FROM M12 UNTIL M24 AND FUTURE STEPS 11

2.1 Website 11

2.2 Social Media 11

2.2.1 Twitter 12
2.2.2 LinkedIn 12
2.2.3 YouTube 13
2.2.4 Mastodon 14

2.3 Online Platforms 15

2.3.1 Cyberwatching.eu 15
2.3.2 Zenodo Community 15

2.4 Newsletters 16

2.5 Press Releases & Press Activities 17

2.6 Events 17

2.7 Organisation of Workshops 20

2.7.1 Ethics Advisory Board Workshop 20
2.7.2 Stakeholders and Industrial Workshops (SIW) 20
2.7.3 Validation Workshop 21

2.8 Publications 21

2.9 Future steps in Dissemination and Communication (M24-36) 23

3 KEY PERFORMANCE INDICATORS 24

4 EXPLOITATION ACTIVITIES FROM M12 UNTIL M24 AND FUTURE STEPS 25

4.1 Section summary - Market analysis, business models and exploitation 25

4.2 Updated exploitation strategy of IRIS 25

4.3 Key exploitable results and IRIS service bundles 27

4.4 Cybersecurity market size, trends and analysis 37

4.5 Initial business models for the IRIS service bundles 38

4.6 Future steps in exploitation 44

5 CLUSTERING ACTIVITIES FROM M12 UNTIL M24 AND FUTURE STEPS 45

5.1 Stakeholders and Industrial Workshops 45

5.2 H2020 Synergies 46
5.2.1 Communication Task Force (CTF) 46
5.2.2 ELECTRON International event 46
5.2.3 EU-made cybersecurity for safe, resilient and trustworthy applications and services Workshop 46
5.2.4 Horizon Booster 47
5.2.5 Meetings with PALANTIR project 47
5.2.6 ERATOSTHENES "Trust and Identity Management for IoT '' Workshop 48

5.3 European Cluster of Securing Critical Infrastructures (ECSCI) 49

5.4 Future steps 49

6 POLICY AND STANDARDISATION ACTIVITIES FROM M12 UNTIL M24 AND FUTURE STEPS 50

6.1 Policy landscape 50
6.1.1 Information sharing in EU Policy 53

6.2 Standardisation landscape 53

7 COMMUNITY BUILDING AND LIASON ACTIVITIES WITH RELEVANT STAKEHOLDERS FROM M12 UNTIL M24 AND FUTURE STEPS 61

8 CONCLUSION 63

9 ANNEXES 64

List of Figures

Figure 1: IRIS website statistics 11
Figure 2: IRIS Twitter page 12
Figure 3: IRIS LinkedIn page 13
Figure 4: IRIS YouTube Channel 13
Figure 5: IRIS Mastodon account 14
Figure 6: IRIS Launch Event promotion through Cyberwatching.eu 15
Figure 7: IRIS Zenodo Community 16
Figure 8: IRIS Newsletter, 3rd & 4th issue 16
Figure 9: Interview about IRIS in Cybersecurity Magazine 17
Figure 10: Picture from the Ethics Advisory Board Meeting 20
Figure 11: Social Media Banners for the SIWs 20
Figure 12: Picture from the IRIS Validation Workshop 21
Figure 13: IRIS updated exploitation strategy 26
Figure 14 : IRIS Roadmap to Commercialisation 34
Figure 15: Picture from the 2nd SIW 45
Figure 16: ELECTRON event social media banner 46
Figure 17: Social media banner created for the joint workshop 47
Figure 18: Horizon Booster logo 47
Figure 19: Screenshot from the meeting with PALANTIR project 48
Figure 20: Screenshot from ERATOSTHENES Workshop 48
Figure 21: ECSCI Cluster 49
Figure 22: List of relevant events and journals 64

List of Tables

Table 1: Expected and Current Performance: IRIS Website 11
Table 2: Expected and Current Performance: Twitter 12
Table 3: Expected and Current Performance: LinkedIn 13
Table 4: Expected and Current Performance: YouTube 13
Table 5: Expected and Current Performance: Mastodon 14
Table 6: Expected and Current Performance: E-newsletters 17
Table 7: Expected and Current Performance: Press releases & Press activities 17
Table 8: Conferences and other events 19
Table 9: Expected and Current Performance: Presentations in conferences, Project presentations, Booths 19
Table 10: Expected and Current Performance: Workshops & Webinars 21
Table 11: List of the scientific papers 22
Table 12: Expected and Current Performance: Scientific publications 23
Table 13: Key Performance Indicators 24
Table 14 Updated List of the IRIS KER, Potential Licenses, and Time-to-Market 30
Table 15: IRIS KER Exploitation Type and Paths 33
Table 16: IRIS Service Bundles (Merged offerings of KER) 36
Table 17: Potential Exploitation Paths per IRIS Service Bundle 39
Table 18 :Tailored business models for the first three service bundles 43
Table 19: Standards and the relevance for IRIS 58
Table 20: well established, used or under development standards 60
Table 21:IRIS CISO Stakeholder Community 62
Table 22: Updated IRIS KERs 73

LIST OF ABBREVIATIONS AND ACRONYMS

Abbreviation/ Acronym	Meaning
AI	Artificial Intelligence
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
D	Deliverable
DoA	Document of Action
DG	Directorate-General
EC	European Commission
ECSO	European Cyber Security Organisation
EU	European Union
ICCS	Institute of Communication & Computer Systems
ICT	Information and Communication Technology
IoT	Internet of Things
INTRA	Netcompany-Intrasoft
KERs	Key Exploitable Results
KPI	Key Performance Indicator
Q&As	Questions & Answers
R&D	Research & Development
REA	European Research Executive Agency
SMEs	Small and Medium Enterprises
T	Task
WP	Work Package

EXECUTIVE SUMMARY

The purpose of this deliverable entitled D8.4 Interim report on dissemination, communication, standardisation and exploitation is to provide a report of the activities performed in the IRIS project in the second project year (M12-24), regarding the dissemination, communication, standardisation and exploitation of the project. Deliverable D8.4 Interim report on dissemination, communication, standardisation and exploitation, is the continuation of the D8.3 Initial report on dissemination, communication, standardisation and exploitation and sets out the activities and impact of actions undertaken by the IRIS project partners.

The document begins with an overview of our activities relating dissemination and communication, presented per channel and tool used. The document presents, in detail, all the progress that has been made in dissemination and communication of the project's results and in engaging the target audiences and stakeholders, through tables presenting their expected and current performance. Then, there is a dedicated chapter which presents in detail the exploitation and business modelling activities of IRIS project implemented during the second year of the project (from M12 until M24) along with the planned future steps. The next chapter showcases all the clustering and liaising activities held with relevant stakeholders and similar H2020 projects in the past 12 months and the ones scheduled to start in the third project year. Next, there is an overview of the work performed regarding the standardisation activities in the second project year and those that are about to performed in the next months. Finally, there is chapter dedicated to the activities and effort made to create links with stakeholders from Industry, SMEs, CERTs/CSIRTs and policy makers at the EU and national level.

This deliverable is the output of task T8.1 Dissemination and communication outreach and is also associated with task T8.2 Market analysis, business models and exploitation, task T8.3 Clustering Activities, task T8.4 Policy recommendation and standardisation, and task T8.5 Community building and liaison with relevant stakeholders.

1 INTRODUCTION

1.1 Project Introduction

As existing and emerging smart cities continue to expand their IoT and AI-enabled platforms, this introduces novel and complex dimensions to the threat intelligence landscape linked with identifying, responding and sharing data related to attack vectors, based on emerging IoT and AI technologies.

IRIS's vision is to integrate and demonstrate a single platform addressed to CERTs/CSIRTs for assessing, detecting, responding to and sharing information regarding threats & vulnerabilities of IoT and AI-driven ICT systems. To achieve this, IRIS brings together experts in cybersecurity, IoT, AI explainability, automated threat detection, response, and recovery.

IRIS aims to help European CERTs/CSIRTs minimise the impact of cybersecurity and privacy risks as well as threats introduced by cyber-physical vulnerabilities in IoT platforms and adversarial attacks on AI-provisions and their learning/decision-making algorithms.

The IRIS platform will be demonstrated and validated on 3 highly realistic environments with the engagement of 3 smart cities in Helsinki, Tallinn and Barcelona, along with the involvement of national CERTs/CSIRTs, and cybersecurity authorities.

1.2 Deliverable Purpose

The document includes all the activities on dissemination, communication, standardisation and exploitation that have been undertaken by the consortium partners during the second year of the project (M12-24) as well as those still planned for the third and last year.

1.3 Intended Readership

This deliverable is public and therefore is mainly addressed to the IRIS Consortium partners, the European Commission (funding authority), as well as other audiences who are interested in learning more about the project. The deliverable will be made available on the IRIS website once approved by the European Commission.

1.4 Relationship with other deliverables and tasks

This deliverable D8.4 "Interim report on dissemination, communication, standardisation and exploitation" is an output of task T8.1 "Dissemination and communication outreach" and is also linked to task T8.2 "Market analysis, business models and exploitation", task T8.3 "Clustering Activities', task T8.4 "Policy recommendation and standardisation", and task T8.5 "Community building and liaison with relevant stakeholders".

D8.1: Project website, which presents in detail the structure of the official project's website.

D8.2: Plans for dissemination, communication, and exploitation, which presents the coordinated dissemination and communication plan that is followed by IRIS and describes how the project will establish and follow highly effective dissemination and communication activities to promote the project. It also records how the results are being exploited.

D8.3: Initial report on dissemination, communication, standardisation and exploitation, which includes include all dissemination and communication activities that have been undertaken, during the first twelve (12) months of the project, and those still planned. The deliverable will also

include the analysis of the standardization landscape and policies relevant to IRIS. The deliverable 8.3 also serves as a guiding document for the deliverables 8.4 and 8.5.

D8.5: Final report on dissemination, communication, standardisation and exploitation, which will document all dissemination, communication and standardisation activities that have been undertaken during the second half of the project duration. It will also summarize the most important dissemination, communication, and standardisation achievements of IRIS during the project's lifetime.

In addition to the above-mentioned tasks and deliverables, the document has a close indirect relation to all project achievements that need to be disseminated and communicated.

2 DISSEMINATION AND COMMUNICATION CHANNELS AND ACTIVITIES FROM M12 UNTIL M24 AND FUTURE STEPS

All the dissemination and communication activities were created based on the IRIS dissemination and communication strategy that is included in the deliverable D8.2 Plans for Dissemination, Communication and Exploitation. The activities performed in the second year of the project have been focused on the effective communication of the available project results and findings and have tried to raise further awareness on project related issues, in a collaborative engaging way.

2.1 Website

The IRIS website www.iris-h2020.eu went live in November 2021 (M2 of the project life span). Its concept, objectives, design, and many more details are presented in the deliverable D8.1 "Project Website" submitted in M3 and D8.3 Initial report on dissemination, communication, standardisation and exploitation.

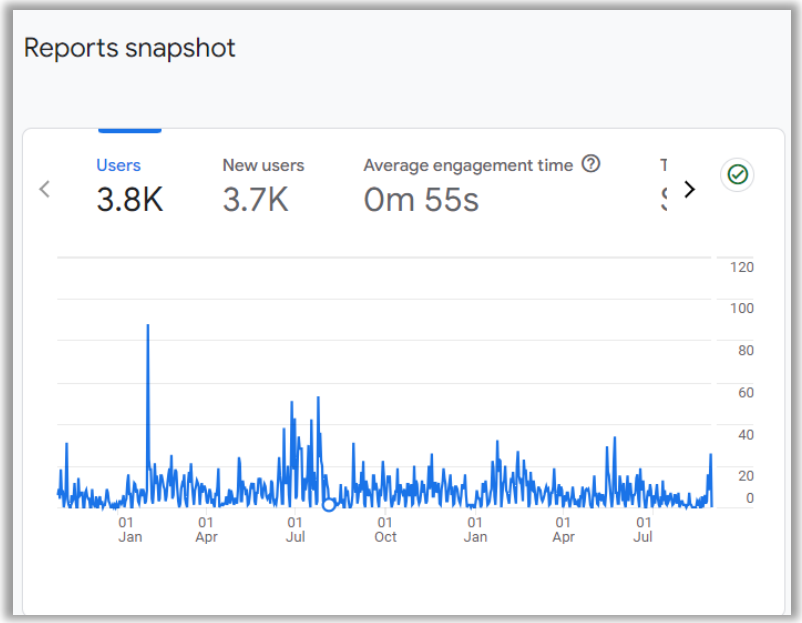


Figure 1: IRIS website statistics

Activity	Expected KPI	Current Status M24
www.iris.eu	5000 per year	3,8 K
	Ready by M2	accomplished

Table 1: Expected and Current Performance: IRIS Website

2.2 Social Media

Social media play an important role in making our stakeholders aware of the IRIS project and highlighting the project's progress and accomplishments. Beside Twitter and LinkedIn, IRIS has also created and maintain a dedicated YouTube channel and a Mastodon profile.

2.2.1 Twitter

@iris_h2020 is mostly used to raise awareness about the project's progress, interact with key stakeholders, and build relationships with other H2020 projects as well as to disseminate the project's news and current results. It is by far the most popular social media account of the project, having currently 643 followers and almost 300 tweets. It's worth mentioning that the account has gained 350 followers the last year.

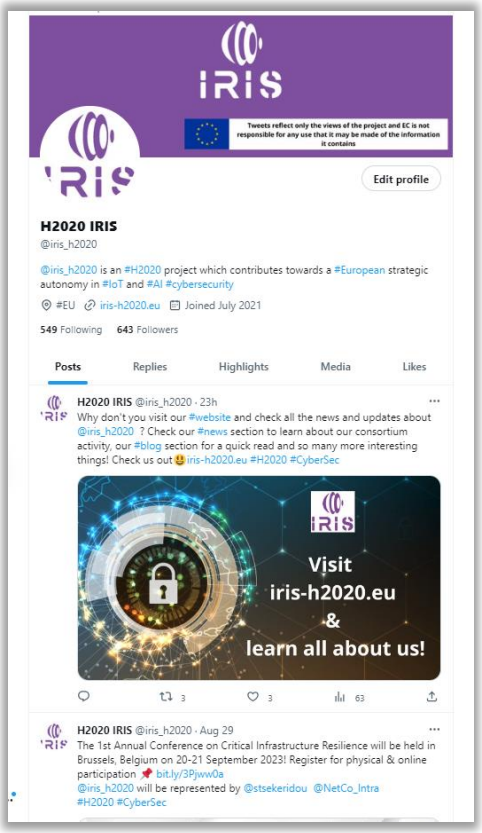


Figure 2: IRIS Twitter page

Activity	Expected KPI	Current Status M24
Twitter Followers	300	643

Table 2: Expected and Current Performance: Twitter

2.2.2 LinkedIn

The IRIS H2020 Project LinkedIn account has 252 followers, 76 more than the 1st year, coming from multiple professional fields and various European locations. Most of our followers come from the fields of Research and Academia, Project and Programme Management and Engineering and the three top countries from which our followers come are Greece, Portugal, and Spain.

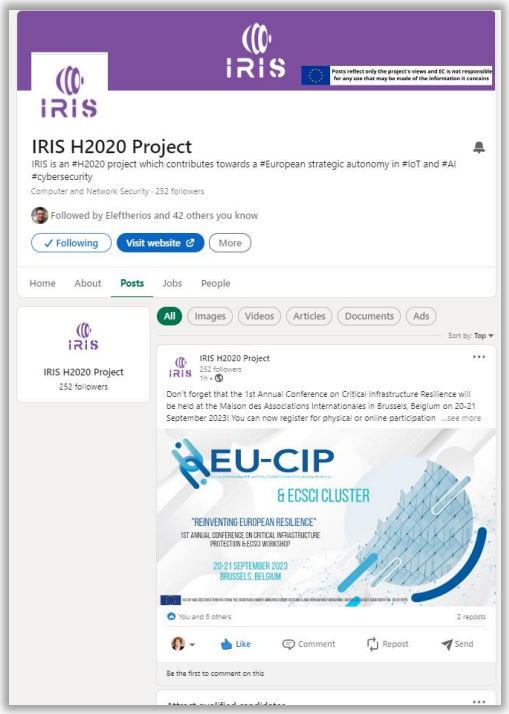


Figure 3: IRIS LinkedIn page

Activity	Expected KPI	Current Status M24
LinkedIn Followers	300	252

Table 3: Expected and Current Performance: LinkedIn

2.2.3 YouTube

The project's YouTube channel currently hosts three videos from workshops and events so far and will host the project's general videos, among others.

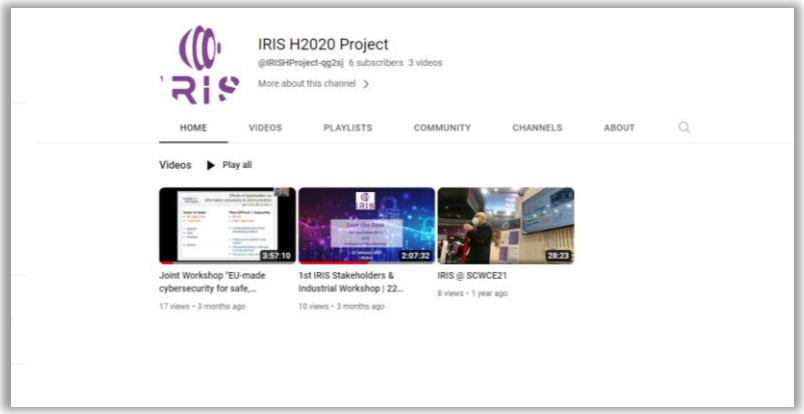


Figure 4: IRIS YouTube Channel

Activity	Expected KPI	Current Status M24
YouTube channel	N/A	3 videos

Table 4: Expected and Current Performance: YouTube

2.2.4 Mastodon

Mastodon is an up and coming, free and open-source software for running self-hosted social networking services, very popular among scientists. IRIS has created an account after being encouraged by one of the reviewers during the project's first review meeting. The account was created in April 2023 and it is quite active, sharing the project's updates.

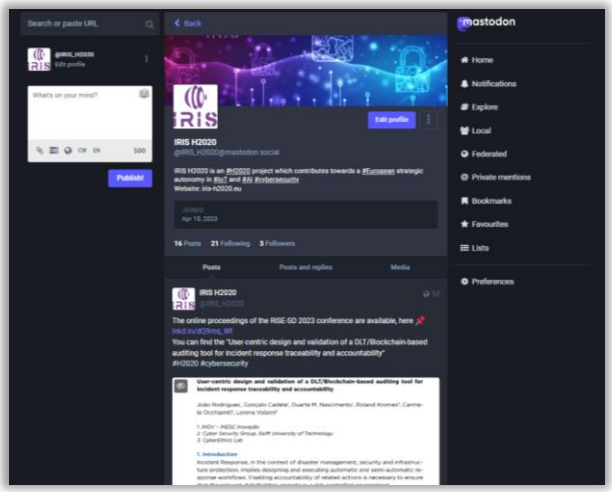


Figure 5: IRIS Mastodon account

Activity	Expected KPI	Current Status M24
Mastodon	N/A	N/A

Table 5: Expected and Current Performance: Mastodon

2.3 Online Platforms

2.3.1 Cyberwatching.eu

The IRIS profile on the Cyberwatching.eu project hub was created in the beginning of the project and it's been updated as needed. One of IRIS' events was also promoted through the platform.

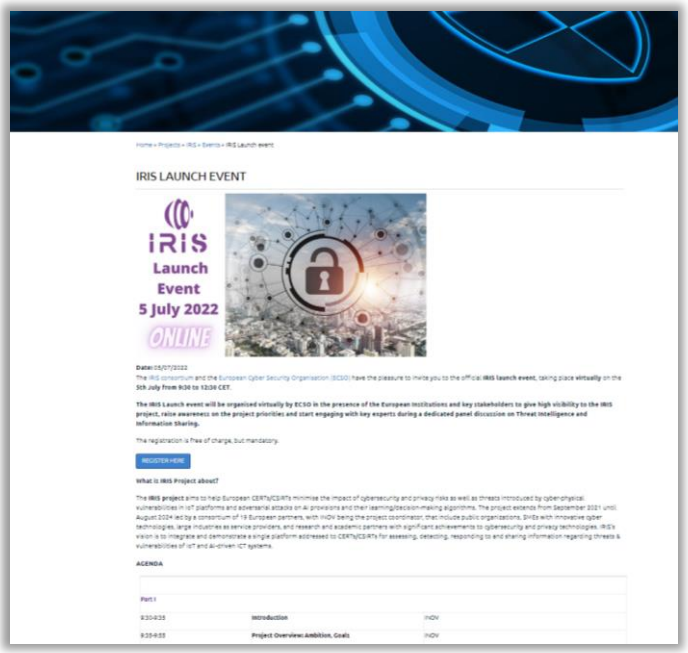


Figure 6: IRIS Launch Event promotion through Cyberwatching.eu

2.3.2 Zenodo Community

The IRIS Zenodo Community includes all the public information regarding the project such as the dissemination material (brochure, poster, banner, brand book, colour palette, logo), the e-newsletters, all the public deliverables approved by the EC along with the scientific papers that were submitted by the consortium partners in different conferences and workshops. The community is constantly updated.

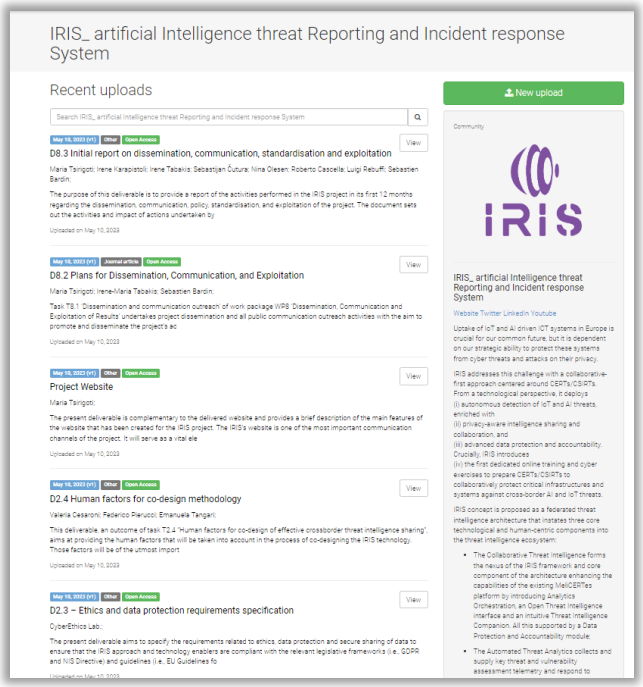


Figure 7: IRIS Zenodo Community

2.4 Newsletters

Within the second year of the project (M12-24), another two issues of the IRIS newsletter have been published. The newsletters are sent to the people that have registered through the website, they are circulated through the social media and they are available both on the website and the Zenodo community.

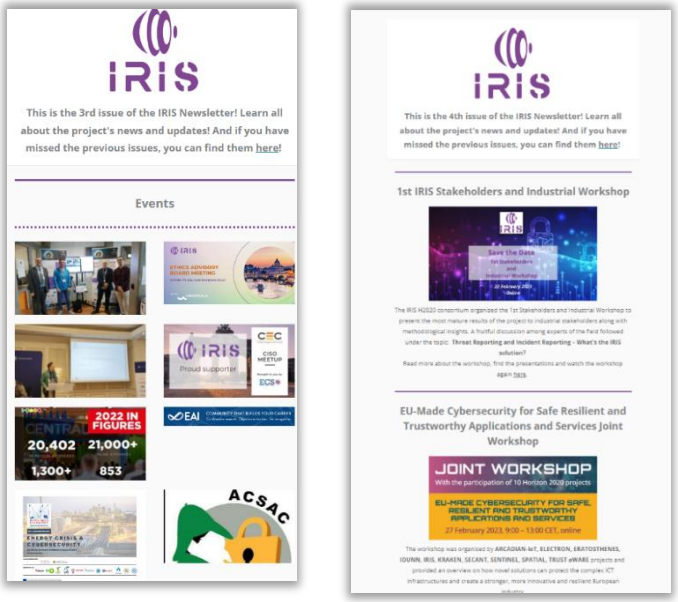


Figure 8: IRIS Newsletter, 3rd & 4th issue

Activity	Expected KPI	Current Status M24
Newsletters	6 e-newsletters	4 e-newsletters published

Table 6: Expected and Current Performance: E-newsletters

2.5 Press Releases & Press Activities

All the press activities and press releases are available on the IRIS website and those occurred until M12 of the project (August 2022) were presented in detail in the deliverable D8.3 Initial report on dissemination, communication, standardisation and exploitation. The latest press activity is the interview performed by our partners in UPC at the Cybersecurity Magazine after their participation in ETSI Security Conference in October 2022. You can watch the interview here.

Figure 9: Interview about IRIS in Cybersecurity Magazine

Activity	Expected KPI	Current Status M24
Press releases	6 press releases	3 press releases + 4 republications
Press activities	3 media appearances	4 media appearances

Table 7: Expected and Current Performance: Press releases & Press activities

2.6 Events

IRIS participated in several events and conferences in the 2nd year of the project lifespan. Consortium representatives have networked and engaged with relevant stakeholders, as well as presented some of the core objectives of the project. The events concerning the 1st year of the project are available in the deliverable D8.3 Initial report on dissemination, communication, standardisation and exploitation and those of the 2nd year are presented in the table below and are also available on the IRIS website in details:

Partner	Date	Activity	Website
TUD	26-30 September 2022	**paper presentation (4 papers)**	https://esorics2022.compute.dtu.dk/
UPC, ATOS, IMI, CISCO	3-5 October 2022	**project presentation, demo**	https://www.etsi.org/events/2068-etsi-security-conference#pane-6/
DNSC	27 & 28 October 2023	**project presentation**	https://dnsc.ro/bucharest-cybersecurity-conference/
INOV	28 October 2022	**project presentation**	https://ecs-org.eu/events/register-for-ecsos-first-ever-ciso-meetup-and-discover-the-sponsorship-opportunities/
UPC, CISCO, IMI, ATOS	15-17 November 2022	**project presentation, demo**	https://www.smartcityexpo.com/
TUD	21-22 November 22	**paper presentation (2 papers)**	https://blocktea.eai-conferences.org/2022/
ICCS	5-7 December 2022	**Project presentation**	ELECTRON International event
TUD	5-9 December 2022	**paper presentation**	https://www.acsac.org/
TUD	12-14 December 2022	**paper presentation**	https://www.acml-conf.org/2022/

IMI, UPC, CISCO	31 January 2023	**project presentation**	https://www.st.com/content/st_com/en/iot-solution-world-congress-23.html
ATOS	27 February 2023	**project presentation**	https://www.iris-h2020.eu/iris-eu-made-cybersecurity-for-safe-resilient-and-trustworthy-applications-and-services-workshop-2/
ECSO	24-26 May 2023	**project presentation**	CyberTek Tech Festival
INOV, ICCS, CEL	29-31 May 2023	**booth, paper presentation**	https://rise-sd2023.eu/
CISCO	4-7 June 2023	**project presentation, booth**	UITP Global Public Transport Summit
ATOS	16 June 2023	**project presentation**	https://eratosthenes-project.eu/2nd-workshop-trust-and-identity-management-for-iot-friday-june-16-online/
SID	31 July 2023	**paper Presentation**	https://www.ieee-csr.org/epes-spr/

Table 8: Conferences and other events

Activity	Expected KPI	Current Status M24
Presentations in conferences	18 oral presentations	15 oral presentations (1 keynote presentation, 14 paper presentations)
Project presentations	7 project presentations	20 project presentations
Booths	3 booths or demos	3 booths, demos

Table 9: Expected and Current Performance: Presentations in conferences, Project presentations, Booths

2.7 Organisation of Workshops

The IRIS consortium has organised several workshops for different reasons either online or physical. You can find details for these workshops below:

2.7.1 Ethics Advisory Board Workshop

The workshop organised by CEL took place in October 2022 in Rome, Italy, with the participation of IRS partners and the Ethics Advisory Board (EAB) members.

Figure 10: Picture from the Ethics Advisory Board Meeting

2.7.2 Stakeholders and Industrial Workshops (SIW)

IRIS has organised two SIW so far and will organise another one by the end of the project with the aim of getting feedback from target stakeholders. Both of the SIW are presented in detail in chapter five of this document.

Figure 11: Social Media Banners for the SIWs

2.7.3 Validation Workshop

A dedicated Validation workshop was held on 31 May in conjunction with the RISE-SD 2023 conference in Rhodes, Greece. The workshop was organised by INOV and CEL and was open only to the invited external experts and end users who provided informal feedback regarding the IRIS pilots and requirements.

Figure 12: Picture from the IRIS Validation Workshop

Activity	Expected KPI	Current Status M24
Workshops & Webinars	3 workshops & 3 webinars	5 workshops/webinars

Table 10: Expected and Current Performance: Workshops & Webinars

2.8 Publications

IRIS partners have made a major effort in publishing peer-reviewed scientific papers in high-impact factor peer-reviewed journals and conference proceedings. To assist partners in planning their dissemination activities, a list, including prestigious journals and renown conferences, has been updated every 6 months and is available in the IRIS repository as well as it is presented in Annex 1. The table below presents a list of the scientific papers of the second project year, which can also be found on the IRIS website and the Zenodo Community.

Scientific paper	*Conference / event / journal*	*Partner*	*Status*
DEKS: A Secure Cloud-Based Searchable Service Can Make Attackers Pay	ESORICS 2022	TUD	published
Lighter is Better: A Lighter Multi-client Verifiable Outsourced Computation with Hybrid Homomorphic Encryption			

No-Directional and Backward-Leak Uni-Directional Updatable Encryption Are Equivalent			
Volume and Access Pattern Leakage-Abuse Attack with Leaked Documents			
ID-based self-encryption via Hyperledger Fabric based smart contract	EAI BlockTEA 2022	TUD	published
Combining ID's, Attributes, and Policies in Hyperledger Fabric			
More is Better (Mostly): On the Backdoor Attacks in Federated Graph Neural Networks	ACSAC 2022	TUD	published
FLVoogd: Robust And Privacy Preserving Federated Learning	ACLM 2022	TUD	published
Threat intelligence using Digital Twin Honeypots in Cybersecurity".	IEEE CSR Workshop on Electrical Power and Energy Systems Security, Privacy and Resilience (EPES-SPR)	SID	presented
Fine-Grained Coverage-Based Fuzzing	ACM Transactions on Software Engineering and Methodology Journal	CEA	published
User-centric design and validation of a DLT/Blockchain-based auditing tool for incident response traceability and accountability	RISE 2023	INOV,CEL	presented

Table 11: List of the scientific papers

Activity	Expected KPI	Current Status M24
Journal Publications/ Conferences Proceedings	3 scientific papers	• 11 papers **published** in conference proceedings • 1 paper **published** in a scientific journal

Table 12: Expected and Current Performance: Scientific publications

2.9 Future steps in Dissemination and Communication (M24-36)

All the dissemination and communication activities that were conducted in the second phase of the project focused on the IRIS key audiences, as these have been defined in an earlier stage of the project. These activities concentrated on the effective communication of the available project results and findings and will try to raise further awareness on project related issues, in a collaborative engaging way. The detailed communication and dissemination strategy followed is described in detail within the deliverable D8.2 “Plans for Dissemination, Communication and Exploitation”, submitted in M6.

Website: The IRIS website will continue to be the backbone of the project’s communication. The website will be regularly updated with the project’s news and updates as it has been so far. The different website sections will be promoted through the social media to gain more visitors.

Brochure and Roll up banner: Both the brochure and the roll up banner will be updated focusing more on the IRIS solutions.

Video: A general video will be created depicting the project’s aim and the solutions it will provide to the EU citizens.

Social Media: The project’s social media accounts will keep being active and will give emphasis to the communication of the project’s results, engaging even more t

Online Platforms: The IRIS results will be uploaded on the Horizon Result Platform and we will create an IRIS profile.

Newsletters: Two more issues of the IRIS newsletter are going to be published.

Press Releases: There will be the publication of at least three more press releases.

Events: Consortium partners will continue on giving oral presentations in conferences and workshops. The list of the relevant events which is already available on the IRIS repository is updated regularly.

Partners Individual Plans: The IRIS consortium partners fill in the document about their individual plans regarding the dissemination and communication of the projects once a year, engaging them this way to do their best in raising awareness and disseminating the project’s results.

3 KEY PERFORMANCE INDICATORS

Within the IRIS DoA, a specific set of KPIs exists, used to measure the effectiveness of communication and dissemination activities within the project. In this section, each KPI will be addressed individually and given a rating based on a colour-based rating system.

For this rating system, red is used to show performance is off track, black for performance which is generally on track but should be improved, blue to highlight that performance is on track, brown is used for an action which has yet to be started and green to show that the expected performance has been met or/and exceeded.

Off track ○ On track but needs improvement ○ On track ○

KPI met or/and surpassed ○ Brown is used for an action which has yet to be started ○

Action	Expected KPI	Current Status M24
Website	5000 visitors per year	3,8 K visitors ○
Social media	Twitter: 300 followers in total LinkedIn: 100 followers in total	643 followers ○ 255 followers ○
Dissemination material	2 brochures 3 roll up banners	1 brochure ○ 4 roll up banners ○
Video	1 general video	○
Press Activities	6 press releases 3 media appearances	3 press releases ○ 4 media appearances ○
E-newsletters	6 e-newsletters	4 published ○
Journal Publications/ Conferences Proceedings	3 scientific papers	11 papers **published** in conference proceedings and 1 paper in a scientific journal ○
Conferences/Events	• 18 oral presentations in conferences • 7 project presentations • 3 booth demonstrations	• 15 oral presentations (1 keynote speech, 14 paper presentations) ○ • 20 project presentations ○ • 3 booths ○
Training	• 3 training sessions for students • 2 MSc & 4 PhD students supervision	○ 1 PhD student ○
Project code repository	2 contributions to open source projects	○
International Standards	2 standards contributions	○
Workshops/Webinars	3 workshops 3 seminars/webinars	5 workshops/webinars (2 Stakeholders and Industrial Workshops, 1 Advisory board Workshop, 1 Validation Workshop, 1 Launch event) ○

Table 13: Key Performance Indicators

4 EXPLOITATION ACTIVITIES FROM M12 UNTIL M24 AND FUTURE STEPS

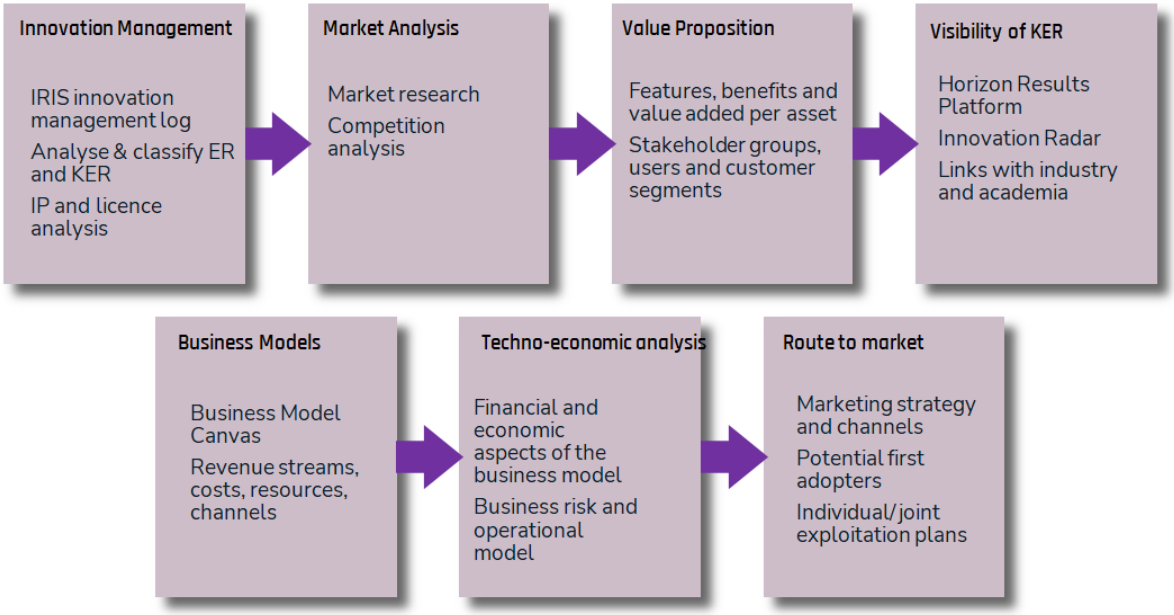
4.1 Section summary - Market analysis, business models and exploitation

This section presents the exploitation and business modelling activities of IRIS, which implemented during the 2nd year of the project (from M12 until M24). The **exploitation strategy** of the project **has been updated** in alignment with the project particularities – addressing the concept of cybersecurity resilience in IoT and AI driven applications – and the technical developments so far. In parallel, **the list of exploitable results has been updated and 4 new service bundles of the IRIS platform** are introduced – 17 exploitable results updated from the previous version (merged one KER based on technical developments and partners consultations) and 4 service bundles introduced, updated version with 21 updated KER in total. These bundles are comprised of a subset of the KER and constitute standalone customized service offerings of the project, for the integrated IRIS Platform, that could be exploited by various stakeholders as identified and presented in this Section. An **in-depth market analysis** has also been conducted and presented to identify trends, gaps, and opportunities in the cybersecurity market to effectively grasp market openings and prospects for the IRIS innovations. The section concludes with the presentation of **tailored exploitation and route to market paths for each of the KER and services bundles**. Notably, **initial business models for each of the service bundles** are also presented, offering among others, potential customer segments for each bundle, target market, positioning, value propositions, revenue streams and pricing models that could be applied. Moreover, during the 2nd year of the project, the IRIS consortium has also applied and communicated the list of KER to the Horizon Results Booster for dissemination support, in order to increase their outreach and potential impact.

The exploitation activities of the 1st year of the project's implementation have already been reported in D8.3.

4.2 Updated exploitation strategy of IRIS

We present hereby the updated methodological approach we have used (and will continue to be using) to effectively implement the IRIS exploitation activities and ensure the proper utilisation of the IRIS innovations in further commercial and/or research activities after the end of the project. The updated exploitation strategy of IRIS is illustrated in the figure below.



:

Figure 13: IRIS updated exploitation strategy

Phase 1 - Innovation Management: In this phase, we identify and update the Key Exploitable Results (KER) of IRIS. The exploitation team analyses the features, TRL, target market, and other business-related characteristics of the KERs. This phase also includes an analysis of intellectual property (IP) and licensing options. To facilitate the business and exploitation activities of this phase, in the frame of T8.2, INTRA has created and continuously manages the IRIS **Innovation Management Log**, an .xlsx template that will be used to track and manage KERs along with their features, TRL, target markets, licenses, and other several exploitation-related aspects. Given the dynamic nature of the project's technical activities, the Innovation Management Log will be a living document that will be adjusted by the WPLs regularly (every 2 months – via emails as well as during dedicated telcos) to capture the most up to date progress of the project's KERs.

The initial version of the IRIS innovation management log was created by INTRA as of M17 of the project and it was shared with partners along with tailored guidelines on how to complete it. It is a living document uploaded on the project's cloud repository. With the contribution of each partner and especially the Work Package Leaders, an initial version of the innovation management log was consolidated and fuelled the development of the current deliverable. Based on the project developments and partners' views, the next set of inputs will be reported in D8.5.

Phase 2 - Market Analysis: We conduct market research using various sources such as market reports, databases, surveys, and technology papers. The market is segmented, and target audiences are defined for the IRIS innovations, also analysing the competitive landscape, identifying market trends, challenges, and opportunities. The exploitation team will also assess the potential demand for the IRIS innovations in the market.

Phase 3 - Value Proposition: The exploitation team defines the value proposition for each KER and each market segment, identifies and analyses the benefits of the IRIS KER for each market segment, and evaluates the pricing strategy for the KERs and service bundles.

Phase 4 - Visibility of results: The project partners will select means for dissemination of results and utilise EC services to maximise project impact. Key results will be proposed for submission

to Horizon Results Booster and Innovation Radar. These platforms will increase visibility of innovations to potential customers/investors and search for synergies related to the project.

Phase 5 - Business Models: In this phase, we define the business model(s) that best fits the IRIS product and market, as well as it will evaluate and compare different business models, such as subscription-based, pay-per-use, or freemium, identify the revenue streams and cost structure for each business model. By the end of the project, we will have determined the most prominent business model for the IRIS service bundles.

Phase 6 - Techno-Economic Analysis: In this phase, we assess the feasibility of the potential business models and the revenue streams, define the market size and market potential for the KER, analyse the financial and economic aspects of the business model of each service bundle, such as revenue, costs, and profits.

Phase 7 - Route to Market: By the end of the project, the exploitation team will identify the most effective and efficient routes to market for the IRIS KER and develop a go-to-market plan that includes target markets, channels, and messaging. At this phase, the exploitation team will also design tailored individual and/or joint exploitation paths per KER and per IRIS service bundles.

4.3 Key exploitable results and IRIS service bundles

During the 2nd year of the project's implementation, the **IRIS innovation management log** (an .xlsx template) was shared with project partners along with tailored guidelines, with a view to **(i) updating the list of KERs** along with their core features, customers segments, target market and potential exploitation paths, **(ii) design the 4 IRIS service bundles**, and **(iii) elaborate on IP aspects including results' ownership** and **license analysis** of the various software modules. This exploitation activity resulted in updating the business features of the already identified KERs, as well as in developing a concrete business offering of services bundles, comprised by subsets of KERs, in order to enhance the IRIS business and economic impact on stakeholders. For each of the KER and service bundles, an analysis has been conducted to investigate potential exploitation paths, value propositions, target groups and indicative go-to-market routes based on their licenses and IP. Based on the features of the identified IRIS KER, and on the results of the market analysis conducted, the exploitable innovations developed by IRIS can provide benefits to each of these main **target groups**:

- **National CSIRT/CERT teams** can benefit from IRIS via enhanced threat intelligence sharing, online communication and collaboration, and an incident management platform. These KERs can help improve the timely cyber situational awareness, preparedness, detection and response capabilities of CSIRT/CERT teams, provide them with actionable insights for threat mitigation, and facilitate collaboration between different teams and organisations, at regional, national, cross-border and European contexts, as well as with critical infrastructure operators and operators of essential services.
- **National public authorities**, especially cybersecurity authorities and critical infrastructure operators, can use IRIS innovations to improve cyber situational awareness, for faster and more effective incident response, for increased operational efficiency, and for the ability to collaborate with other stakeholders in the cybersecurity ecosystem.
- **Companies providing cybersecurity products**, services and/or processes (**supply side**) can benefit from IRIS innovations by offering new or enhanced cybersecurity products and services, accessing to real-time threat intelligence, and improving their product's incident

response capabilities. The European Council has estimated that there are 60,000 such companies in Europe (ENISA market research report).

- **Companies needing cybersecurity products**, services and/or processes (**demand side**) can benefit from IRIS innovations by receiving services for enhanced cyber resilience, improved incident management, and access to real-time threat intelligence.
- **Large corporations and cybersecurity associations** (e.g., ENISA) can use IRIS to help raise awareness about cybersecurity threats and provide consulting services and guidance to their members on how to protect themselves.
- **Research institutions and universities** can use IRIS innovations as a means to conduct research on cyber threats and trends and contribute to the development of more effective cybersecurity solutions, especially in the evolving domain of cyber threats and attacks on IoT and AI-driven applications.

During the 2nd year of the project, partners (under the management of the exploitation manager, INTRA) have made a collaborative exercise (based also on the inputs of the innovation management log) to update the list of KERs and, their descriptions based on the latest technical developments (this list can be further found in a dedicated table in the Annexes), their potential target groups (initial adopters and potential customers), their indicative licenses (important for exploitation purposes - either proprietary (owned by specific organisations within the consortium), or open source, and their expected time-to-market. The time-to-market estimations have been revised accordingly to pursue more concrete and closer to the market exploitation paths for each KER. The **updated list of the 21 IRIS KER (17 initial updated KERs and 4 Service Bundles)** is presented in the table below.

ID	Name	TRL	Target Group(s)	License	Time to market
KER #1	**Social acceptance framework**	7	CSIRT/CERT teams, Companies needing incident management solutions	Proprietary	Less than 1 year
KER #2	**Risk and vulnerability assessment module**	7	National public authorities, Critical infrastructure operators, Companies needing cybersecurity products	Proprietary	1 to 2 years
KER #3	**AI threat analytics and detection engine**	7	IoT/AI infrastructure providers, large enterprises across various industries, MSSPs, SOCs, IT service providers, cybersecurity consultants	Proprietary	Less than 1 year
KER #4	**Risk-based response and self-recovery**	7	Large enterprises across various industries, MSSPs, SOCs, IT service providers, Cybersecurity consultants	Proprietary	More than 1 year
KER #5	**Digital twin honeypot detection models**	7	Organizations seeking enhanced threat detection capabilities	Proprietary	More than 1 year

ID	Name	TRL	Target Group(s)	License	Time to market
KER #6	**IRIS-enhanced MeliCERTes platform**	7	CSIRT/CERT teams, Companies requiring incident management and response solutions including Critical Infrastructure Operators/OESs	Open Source (like MeliCERTes)	Less than 1 year
KER #7	**APIs for advanced threat intelligence orchestration**	7	SOC teams, CERT/CSIRTs, IT & OT operators	agpl license	Less than 1 year
KER #8	**Collaborative threat intelligence sharing and storage**	7	CERTs, CSIRTs, SOC teams, Companies providing cybersecurity products.	CC-BY-NC-ND	2 years
KER #9	**DLT-based control services for accountability, traceability and auditing**	7	Organizations seeking blockchain-based security solutions	Proprietary	Less than 1 year
KER #10	**IRIS secure crypto functions for data management**	7	Organizations requiring secure data management solutions	Proprietary	Less than 1 year
KER #11	**IRIS cybersecurity exercises and training scenarios**	7	CSIRT/CERT teams, Research institutions and universities, Cybersecurity associations	Proprietary	Less than 1 year
KER #12	**IRIS lab pods**	7	CSIRT/CERT teams, Large corporations, Cybersecurity associations	Proprietary	Less than 1 year
KER #13	**IRIS cyber range environment platform**	7	Organizations requiring practical cybersecurity training	Proprietary	Less than 1 year
KER #14	**Smart city IoT and control system pilot**	7	Smart city operators, IoT solution providers	-	3 years (requires public procurement)
KER #15	**Smart city autonomous transport system pilot**	7	Smart city operators, Autonomous vehicle manufacturers	Proprietary	Less than 1 year

ID	Name	TRL	Target Group(s)	License	Time to market
KER #16	**Cross-border smart grid pilot**	7	Smart grid operators, Energy companies	Proprietary	1-2 years
KER #17	**Integrated IRIS Platform**	7	CSIRT/CERT teams, National public authorities, Critical Infrastructure Operators / OESs, Cybersecurity companies	Proprietary, Open Source	1-2 years
KER#18	**Autonomous Threat Analytics (ATA) Service Bundle**	7	Cybersecurity providers (supply side) /Industrial players and SMEs (demand side)/ National authorities / Critical Infrastructure Operators / Operators of Essential Services	Proprietary	1-2 years
KER#19	**Enhanced MeliCERTes Ecosystem (EME) Service Bundle**	7	CERTs/CSIRT teams/ National authorities/ / Critical Infrastructure Operators / Operators of Essential Services / Cybersecurity providers/ Academia/Policymakers/Open-source software community/ ENISA	Open Source (like MeliCERTes)	1 year
KER#20	**Virtual Cyber Range training (VCR) Service Bundle**	7	CERTs/CSIRT teams/ National authorities/Large corporations and SMEs interested in Cybersecurity training/Research/Academia	Proprietary	1-2 years
KER#21	**Add-ons Services Bundle**	7	CERTs/CSIRT teams/ National authorities/ Cybersecurity providers/ Academia/Policymakers/Open-source software community/ ENISA	Proprietary, Open Source	1-2 years

Table 14 Updated List of the IRIS KER, Potential Licenses, and Time-to-Market

Moreover, during the 2nd year of the project, partners have made an analysis to identify how each of the KER could practically be exploited (either for commercial or research purposes) after the end of the project. This information is summarised in the table that follows along with the envisioned (joint or individual) exploitation path for each KER.

ID	Name	Exploitation Type
KER #1	**Social acceptance framework**	**Individual - CEL**
How are we going to exploit the result?	Collaborate with industry stakeholders, organise workshops and training sessions to promote the framework, and actively engage with	

ID	Name	Exploitation Type
	relevant communities and organisations to raise awareness and encourage adoption.	
KER #2	**Risk and vulnerability assessment module**	**Joint – ATOS, CEA**
How are we going to exploit the result?	Develop joint marketing materials, create case studies highlighting the benefits of the module, offer consulting services to assist organisations in implementing and utilising the module effectively, participate in industry conferences and events to showcase the module's capabilities.	
KER #3	**AI threat analytics and detection engine**	**Joint – CLS, SID, CEA**
How are we going to exploit the result?	(Potentially new product) Collaborate with partner organisations to create a comprehensive marketing plan, provide proof-of-concept demonstrations, and establish partnerships with cybersecurity vendors to integrate the engine into their existing solutions. Subscription licensing business model.	
KER #4	**Risk-based response and self-recovery**	**Individual – CLS**
How are we going to exploit the result?	(Potentially new product) Develop a comprehensive marketing strategy highlighting the benefits of the solution, engage with potential customers through targeted marketing plans, and conduct webinars and training sessions to educate users on the features and advantages of the solution. Subscription licensing business model.	
KER #5	**Digital twin honeypot detection models**	**Individual – SID**
How are we going to exploit the result?	Through focused marketing initiatives showcasing the effectiveness and usability, collaborate with industry experts to validate the models, offer consulting services to assist organisations in implementing and optimising the models for their specific environments.	
KER #6	**IRIS-enhanced MeliCERTes platform**	**Individual – INTRA**
How are we going to exploit the result?	Develop marketing materials and strategy, create case studies demonstrating the value of the enhanced EME platform for both CERTs/CSIRTs and CI Operators / OESs for information governance, sharing and online collaboration, offer training programs to educate users on the new features, collaborate with industry partners to integrate the platform into their cybersecurity solutions, participate in relevant industry events and conferences to showcase the capabilities of EME, provide the platform as open source along with technical support and training for local deployment and use of the platform.	
KER #7	**APIs for advanced threat intelligence orchestrator**	**Individual – ICCS**
How are we going to exploit the result?	(Licensing) Develop API documentation and SDKs, offer developer support and assistance, participate in relevant industry events and conferences to showcase the capabilities of the APIs.	
KER #8	**Collaborative threat intelligence sharing and storage**	**Individual – CERTH**
How are we going to exploit the result?	(Further develop) Continue training and fine-tuning our AI-based algorithms to diverse data coming from more end-users and from different domains. Utilise, test and integrate different AI techniques to assess their effectiveness.	

ID	Name	Exploitation Type
	We aim to commercialise the developed module through the spinoff company Infalia (www.infalia.com), licensing the developed tool to interested clients. The Information Technologies Institute of CERTH has all the necessary support including legal support and business management in order to create innovative enterprises.	
KER #9	**DLT-based control services for accountability, traceability, and auditing**	**Joint – INOV, TUD**
How are we going to exploit the result?	Collaborate with industry stakeholders to develop frameworks for utilizing DLT in cybersecurity, offer consulting services to assist organizations in implementing DLT-based control services, publish research papers highlighting the benefits of DLT in accountability and traceability.	
KER #10	**IRIS secure crypto functions for data management**	**Joint – TUD, INOV**
How are we going to exploit the result?	Develop a marketing plan targeting organizations handling sensitive data, collaborate with encryption technology vendors to integrate the secure crypto functions into their products, offer consulting services for implementing and optimising secure data management solutions.	
KER #11	**IRIS cybersecurity exercises and training scenarios**	**Individual – KEMEA**
How are we going to exploit the result?	Develop a comprehensive training programme for cybersecurity professionals, offer hands-on exercises and simulations, collaborate with cybersecurity organisations to incorporate the exercises and scenarios into their curricula.	
KER #12	**IRIS lab pods**	**Joint – THALES, CLS, CERTH, ICCS, KEMEA**
How are we going to exploit the result?	Collaborate with partner organisations to offer lab pod deployments, provide technical support and training for lab pod users, develop case studies showcasing the benefits of lab pods, engage with industry conferences and events to showcase the capabilities of lab pods.	
KER #13	**IRIS cyber range environment platform**	**Individual – THALES**
How are we going to exploit the result?	Develop marketing materials highlighting the advantages of the platform, offer training programmes for cybersecurity professionals, collaborate with industry partners to integrate the platform into their cybersecurity solutions.	
KER #14	**IRIS smart city IoT and control system pilot**	**IMI, All pilot partners**
How are we going to exploit the result?	Collaborate with smart city stakeholders to deploy and demonstrate the pilot project, showcase the benefits and successes of the pilot, collaborate with regulatory bodies to establish standards and frameworks for secure smart city deployments.	
KER #15	**IRIS smart city autonomous transport system pilot**	**TALTECH, All pilot partners**
How are we going to exploit the result?	Collaborate with smart city stakeholders and transportation industry partners to deploy and demonstrate the pilot project, showcase the benefits and successes of the pilot, engage with regulatory bodies to address cybersecurity concerns in autonomous transport systems.	
KER #16	**IRIS cross-border smart grid pilot**	**FVH,**

ID	Name	Exploitation Type
		All pilot partners
How are we going to exploit the result?	Collaborate with smart grid stakeholders and energy industry partners to deploy and demonstrate the pilot project, showcase the benefits and successes of the pilot, engage with regulatory bodies to address cybersecurity challenges in cross-border smart grid deployments.	
KER #17	**Integrated IRIS Platform**	**Joint – via the 4 service bundles**
How are we going to exploit the result?	Develop a unified marketing strategy for the integrated platform, showcase the seamless integration of the KERs and the added value it provides, collaborate with industry partners to promote and implement the integrated platform, and mainly exploit the platform via the offering of the 4 service bundles.	
KER #18	**Autonomous Threat Analytics (ATA) Service Bundle**	**Joint (partners participating in respective KER)**
How are we going to exploit the result?	*A detailed description of the potential exploitation paths of this service bundle is presented in Table 4.*	
KER #19	**Enhanced MeliCERTes Ecosystem (EME) Service Bundle**	**Joint (partners participating in respective KER)**
How are we going to exploit the result?	*A detailed description of the potential exploitation paths of this service bundle is presented in Table 4.*	
KER #20	**Virtual Cyber Range training (VCR) Service Bundle**	**Joint (partners participating in respective KER)**
How are we going to exploit the result?	*A detailed description of the potential exploitation paths of this service bundle is presented in Table 4.*	
KER #21	**Add-ons Services Service Bundle**	**Joint (partners participating in respective KER)**
How are we going to exploit the result?	*A detailed description of the potential exploitation paths of this service bundle is presented in Table 4.*	

Table 15: IRIS KER Exploitation Type and Paths

In summary, the IRIS KER will be mostly exploited within 1 (max 2) year after the project completion. Under this framework, the IRIS roadmap to commercialisation can be separated in two stages: mid-term, which refers to 1-2 years after the project completion and involves mostly exploitation activities like marketing of new services, licensing of KER, and deployment of new use cases via new research projects; and long term >3 years after the project completion, where the KER are expected to be used by a wider group of potential stakeholders (CERTs, Cybersecurity Agencies, National authorities in cybersecurity) and their exploitation will escalade. The IRIS roadmap to commercialisation is presented in the figure that follows.

Figure 14 : IRIS Roadmap to Commercialisation

A detailed presentation of the IRIS service bundles along with their indicative (and potential so far) key business features is presented below.

Service bundle	KER Included	Partners involved	License
#1: Autonomous Threat Analytics (ATA)	#2, #3, #4, #5	ATOS, CEA, CLS, SID	Proprietary
Current TRL	7		
Target groups	• **Cybersecurity providers**: Companies or organisations offering advanced threat detection and response services. • **Industrial players and SMEs**: Businesses that want to enhance their cybersecurity posture and protect their digital assets. • **Critical Infrastructure Operators (demand side)**: Operators who want to effectively protect the digital assets of critical infrastructures in the EU. • **National authorities**: Government entities seeking improved cybersecurity capabilities to safeguard critical infrastructure and national security.		
Benefits	• Improved detection and response capabilities • Actionable insights for threat mitigation • Enhanced cyber resilience		
Pricing model	• **Subscription-based pricing**: This model involves charging customers a recurring fee for access to the ATA module. The fee can be based on factors such as the number of users, the volume of data analysed, or the level of service provided. • **Usage-based pricing**: With this model, customers are charged based on their actual usage of the ATA module. This can be measured in terms of the number of threat alerts generated, the amount of data processed, or the duration of system usage.		

Service bundle	KER Included	Partners involved	License
	• **Tiered pricing**: This model offers different levels of service and functionality at different price points. Customers can choose the tier that best suits their needs and budget, with higher tiers offering more advanced features and capabilities.		
#2: Enhanced MeliCERTes Ecosystem (EME)	#6, #7, #8	INTRA, ICCS, CERTH	Open Source (like MeliCERTes)
Current TRL	7		
Target groups	• **CERTs/CSIRT teams**: EME provides improved incident management capabilities, allowing these teams to effectively respond to and mitigate cybersecurity incidents. • **National authorities and Infrastructure Operators**: EME enables better incident management for infrastructure operators and national authorities, helping them protect critical infrastructures and ensure the resilience of their networks. • **Cybersecurity providers**: EME can be beneficial for cybersecurity providers, as it enhances their incident management capabilities and provides access to real-time threat intelligence, allowing them to offer more effective services to their clients. • **Research and Academia**: EME can be used by research institutions and academia for studying and analysing cybersecurity incidents, as well as for developing and testing new incident management techniques and strategies. • **Policymakers**: EME can assist policymakers in understanding the threat landscape and making informed decisions regarding cybersecurity policies and regulations. • **Open-source software community**: EME being an open-source module, the open-source software community can contribute to its development, customisation, and enhancement, fostering collaboration and knowledge sharing. • **ENISA**: The European Union Agency for Cybersecurity (ENISA) can benefit from EME by utilising its capabilities to enhance incident management and improve collaboration among stakeholders.		
Benefits	• Improved information sharing, situational awareness and incident management capabilities • Enhanced preparedness and response to incidents • Access to real-time threat intelligence • Better collaboration between different teams and organisations at regional, national and cross-border levels		
Pricing model	• **Freemium model**: In this model, the basic version of the EME bundle is offered for free, allowing customers to experience its benefits. Additional premium features and functionalities can be offered at an additional cost. • **Subscription-based pricing**: This model involves charging customers a recurring fee for accessing a set of advanced services of the EME module.		

Service bundle	KER Included	Partners involved	License
#3: Virtual Cyber Range training (VCR)	#11, #12, #13	KEMEA, THALES	Proprietary
Current TRL	7		
Target groups	• **CERTs/CSIRT teams**: Computer Emergency Response Teams or Computer Security Incident Response Teams responsible for responding to and mitigating cybersecurity incidents. • **National authorities**: Government entities involved in cybersecurity training and preparedness. • **Large corporations and SMEs**: Businesses that recognise the importance of cybersecurity training and skill development for their employees.		
Benefits	• Effective training and skill development in a realistic simulated environment • Capability to create customised training scenarios		
Pricing model	• **Subscription-based pricing**: Similar to the ATA module, a subscription-based model can be implemented for the VCR module. Customers would pay a recurring fee to access and use the training platform. The fee can be based on factors such as the number of users, the duration of access, or the level of service provided. • **Pay-per-use pricing**: With this model, customers are charged based on their actual usage of the VCR module. This can be measured in terms of the number of training sessions conducted, the duration of each session, or the complexity of the customised training scenarios created.		
#4: Add-ons Services	#9, #10	INOV, TUD	Open Source/ Proprietary
Current TRL	7		
Target groups	CERTs/CSIRT teams/ National authorities like Infrastructure Operators/ Cybersecurity providers (supply side)/Research/Academia/Policymakers/Open-source software community/ ENISA		
Benefits	• DLT-based control services for accountability, traceability, and auditing • IRIS-enhanced crypto functions for data management		
Pricing model	**Bundled pricing**: The Add-on services module can be offered as part of a bundled package along with other cybersecurity products or services. This can provide customers with a comprehensive solution and may offer cost savings compared to purchasing the components separately.		

Table 16: IRIS Service Bundles (Merged offerings of KER)

4.4 Cybersecurity market size, trends and analysis

Target Market: The IRIS platform and its **4 service bundles, along with the 17 KER,** target the **European cybersecurity market for IoT and AI systems.**

The platform (and most pertinent IRIS KER) aims to address key challenges in IoT and AI-driven ICT systems and enhance threat detection, intelligence coordination, and incident response. The target groups mentioned for the different service bundles, such as cybersecurity providers, industrial players, SMEs, national authorities, CERTs/CSIRT teams, large corporations, and academia, further support the focus on the European cybersecurity market. Additionally, the involvement of partners like ATOS, CEA, CLS, SID, KEMEA, THALES, INTRA, ICCS, and CERTH indicates a strong European presence in the development and deployment of the IRIS platform.

Market Size and Growth: The EU cybersecurity market has been growing rapidly in recent years, driven by the increasing number and sophistication of cyber threats. According to the Research and Markets report[1], the European cybersecurity market is expected to reach €57.7 billion by 2026, growing at a CAGR of 9.7% from 2021 to 2026. In addition, the Statista report[2] forecasts the EU cybersecurity market to generate €33.3 billion in revenue in 2023, up from €24.6 billion in 2020.

Market Segmentation: Based on the type of solution, the EU cybersecurity market can be segmented into network security, endpoint security, application security, cloud security, and others. Among these, network security is expected to account for the largest share of the market in 2026, accounting for the largest share (€21.1 billion) followed by endpoint security (€14.8 billion) and cloud security (€10.6 billion), according to the Research and Markets report, driven by the increasing adoption of cloud-based solutions and the rising number of network-based cyber-attacks. Based on the industry vertical, the EU cybersecurity market can be segmented into government, BFSI (Banking, Financial Services, and Insurance), healthcare, retail, IT and telecom, and others. Among these, the BFSI segment is expected to be the largest revenue-generating segment in 2026, driven by the high risk of cyber-attacks in the financial sector.

Geographical Analysis: Geographically, the EU cybersecurity market can be segmented into Western Europe and Eastern Europe. Western Europe is expected to account for the largest share of the market in 2026, driven by the increasing adoption of cloud-based solutions, the rise in cyber-attacks, and the strict data protection laws in the region.

Key Trends

- **Increasing demand for cloud-based security solutions**: With the increasing adoption of cloud computing, there is a growing demand for cloud-based security solutions that can protect data and applications hosted in the cloud.
- **Rising adoption of IoT and connected devices**: The increasing use of IoT devices and connected devices in various industries is driving the demand for cybersecurity solutions that can protect these devices from cyber-attacks.
- **Growing need for threat intelligence and advanced analytics**: The increasing complexity of cyber threats is driving the need for threat intelligence and advanced analytics solutions that can detect and respond to cyber-attacks in real-time.

[1] https://www.researchandmarkets.com/reports/5354548/europe-cybersecurity-market-share-by-segment
[2] https://www.statista.com/outlook/tmo/cybersecurity/europe#revenue

Competitive Landscape: The EU cybersecurity market is highly fragmented, with numerous vendors offering a wide range of cybersecurity solutions. The key players in the market include Cisco Systems Inc., Palo Alto Networks Inc., IBM Corporation, Symantec Corporation, and Trend Micro Inc. These companies are focusing on product innovation, partnerships, and acquisitions to expand their market share.

The EU cybersecurity market is witnessing strong growth, driven by the increasing frequency of cyber-attacks and data breaches. The market is expected to continue to grow at a steady pace in the coming years, with network security being the largest revenue-generating segment. The BFSI segment is expected to be the largest industry vertical in the market, while Western Europe is expected to be the largest geographical segment.

4.5 Initial business models for the IRIS service bundles

In summary, the exploitation paths for each of the IRIS service bundles, as they are perceived by project partners so far, are outlined in the following table.

IRIS Service Bundle	Potential Exploitation Paths	Business model
ATA	• Offer training and support services to cybersecurity providers, industrial players, and infrastructure operators using the ATA module to detect and respond to threats in ICT systems. • Develop new services that leverage the ATA module to provide more robust threat detection and response capabilities for infrastructure operators and cybersecurity providers. • Partner with infrastructure operators to integrate the ATA module into their existing systems to improve overall cybersecurity posture.	Service-based.
EME	• License the open source EME module to CERTs/CSIRTs, critical infrastructure operators/operators of essential services, and cybersecurity providers for use in their own systems and tools. • Offer support services and training to help organisations effectively implement and use the EME module. • Conduct research and collaborate with academia to further develop and improve the EME module and related tools. • Engage with policymakers to promote the adoption of the EME module as a best practice for securing critical infrastructure.	Open source based. Offer the software for free and generate revenue from support services, training, and consulting.
VCR	• Offer new services that leverage the VCR platform to provide more advanced and immersive cybersecurity	Service-based.

IRIS Service Bundle	Potential Exploitation Paths	Business model
	training experiences for CERTs/CSIRTs, infrastructure operators, and cybersecurity providers. • Partner with CERTs/CSIRTs to integrate the VCR platform into their existing training programmes to improve the effectiveness of their training and preparedness for cybersecurity incidents. • Provide support services and training to help organisations effectively use the VCR platform and associated tools.	
Add-on services	• Offer new services that provide additional functionality and capabilities to the EME modules. • Develop and license proprietary add-on modules to infrastructure operators and cybersecurity providers to enhance their cybersecurity posture.	Service-based. Offer additional services to complement the EME bundle.

Table 17: Potential Exploitation Paths per IRIS Service Bundle

Business models per service bundle

During the 2nd year of the project, partners have made a collaborative effort to create 3 separate business models, one for each of the core service bundles of IRIS, namely the ATA, EME and VCR bundles. These business models express initial exploitation ideas and will change in the next years, depending on partners exploitation views. However, they represent a concrete idea on how the IRIS platform could be offered to its stakeholders via these 3 bundles, expressing the key value proposition, customers, potential collaborations, channels of service provision, revenue streams, and cost structures among others. The set of business models is presented in the pages that follow. Given that the 4th service bundle (namely, the Add-on service bundle) has a more supportive role, we have designed tailored business models for the first three service bundles since they hold the most exploitation potential.

Business Model Canvas	*Designed for:*	*Designed by:*	*Date:*	*Version:*
	ATA Bundle	INTRA	M24	1st

Key Partners

- ATOS, CEA, CLS, and SID for development and implementation of the technology
- Cybersecurity providers, industrial players, SMEs, and infrastructure operators for customer acquisition and feedback

Key Activities

- R&D
- Integration and implementation of technologies into customer systems
- Sales and marketing to attract customers
- Support services

Key Resources

- IP rights for proprietary technology
- Skilled researchers and developers
- Sales and marketing
- Support personnel for customer service and maintenance

Value Propositions

- Comprehensive cybersecurity solution industrial players
- Mitigation of cyber risks and of potential financial and reputational losses
- Minimisation of attack surfaces and effective response to incidents
- Improved compliance with cybersecurity regulations

Customer Relation

- Personal assistance: The ATA bundle aims to provide personalised and tailored support to customers.
- Self-service: The ATA bundle also provides customers with self-service tools and resources.

Channels

- Direct sales
- Online platforms
- Conferences and events

Customer Segments

- Cybersecurity providers
- Industrial players and SMEs
- National authorities

Cost Structure

Revenue Streams

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

• Research and development costs • Implementation and integration costs • Sales and marketing costs • Support and maintenance costs	• Direct sales • Training and consulting fees • Support and maintenance fees from customers

	Designed for:	*Designed by:*	*Date:*	*Version:*
Business Model Canvas	**EME Bundle**	INTRA	M24	1st

Key Partners	Key Activities	Value Propositions	Customer Relati	Customer Segmen
• INTRA, ICCS, CERTH for development and implementation of open source components • Cybersecurity providers, industrial players, SMEs, CERTs/CSIRTs, Critical Infrastructure Operators, research and academia for	• R&D • Implementation and customisation of technologies • Sales and marketing to attract users • Provision of support services • Open source software maintenance	• Comprehensive cybersecurity solution • Access to open source software components for customizable solutions • Minimisation of attack surfaces and effective response to incidents • Improved compliance with cybersecurity regulations	• Support • Training: Offering training programs • New Services: Providing new services to meet evolving user needs and stay ahead of competitors.	• CERTs/CSIRT teams • National authorities and Critical Infrastructure Operators • Cybersecurity providers • Research and Academia • Policymakers • Open-source software community
	Key Resources		**Channels**	

customer acquisition and feedback • Policymakers and open source software community for awareness and adoption of open source components	• Open source software components • Skilled researchers and developers • Sales and marketing personnel • Support personnel	• Provision of common platform for CTI sharing, SIEM, and trusted collaboration	• Direct Sales • Partner Networks • Online Platforms • Industry Events	• ENISA

Cost Structure	Revenue Streams
• Research and development costs • Implementation and integration costs • Open source software maintenance costs • Sales and marketing costs • Support and maintenance costs	• Commercial Support and Consulting • Customisation and Integration Services • Value-added Services,Premium Features and Add-ons • Training fees

	Designed for:	*Designed by:*	*Date:*	*Version*
Business Model Canvas	**VCR Bundle**	INTRA	M24	1st

Key Partners	Key Activities	Value Propositions	Customer Relatior	Customer Segments

<table>
<tr>
<td>

KEMEA, THALES for development and implementation of proprietary technology
Cybersecurity providers, industrial players, SMEs, and infrastructure operators for customer acquisition and feedback

</td>
<td>

R&D
Integration and implementation of technologies into customer systems
Sales and marketing
Provision of support services, such as training and maintenance, to customers

Key Resources

IP
Skilled developers
Sales and marketing personnel
Support personnel

</td>
<td>

Mitigation of cyber risks and potential financial and reputational losses
Minimisation of attack surfaces and effective response to incidents
Improved compliance with cybersecurity regulations

</td>
<td>

Collaborative: facilitate collaborative training exercises for CERT/CSIRTs and other stakeholders
Support: support services to customers using the platform, such as technical assistance or troubleshooting.

Channels

Online
Direct sales
Partnerships

</td>
<td>

CERTs/CSIRT teams
National authorities
Large corporations and SMEs

</td>
</tr>
<tr>
<td colspan="3">
Cost Structure

Research and development costs
Marketing and sales costs
Salaries for development, sales, and customer support
Ongoing costs for hosting and maintaining the platform
Potential legal fees related to licensing and intellectual property

</td>
<td colspan="3">
Revenue Streams

Licensing fees for use of the proprietary platform
Support and maintenance fees for ongoing customer support
Training fees for providing training to customers

</td>
</tr>
</table>

Table 18 :Tailored business models for the first three service bundles

4.6 Future steps in exploitation

The future steps in the exploitation activities, over the 3rd year of the project, revolve around the following pillars: (i) further elaboration on practical exploitation pathways for the 4 services bundles, (ii) value proposition analysis and link of the IRIS KER with the market needs, (iii) further definition of the business cases per KER and creation of tailored individual/joint exploitation paths, (iv) business planning activities accompanied with potential financial estimations, (v) further implementation of the IPR Management Strategy and the IRIS innovation management log. We aim also to apply and upload the list of KER to the EC services for supporting exploitation activities of R&I projects, namely the Horizon Results Booster, the Innovation Radar, and the Horizon Results platform.

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

5 CLUSTERING ACTIVITIES FROM M12 UNTIL M24 AND FUTURE STEPS

The IRIS project has made great effort to raise the project awareness and engage relevant stakeholders since the beginning of the project. However, the progress made the second year is remarkable. Below, we provide an overview of the activities made to this end.

5.1 Stakeholders and Industrial Workshops

IRIS has organised two Stakeholder and Industrial Workshops (SIW) so far. The 1st SIW was held on 22 February 2023 online. During the workshop, the 40 attendees had the chance to get introduced to the project, learn all the information about the three pilot demonstrations that will be held within the project as well as the IRIS architecture and different components. The workshop closed with a discussion under the title “Threat Reporting and Incident Response – What IRIS has to offer?” with the participation of the technical partners and different stakeholders. The aim of the workshop was to take feedback on where to focus its research efforts.

The 2nd SIW was held on 30 May 2023 in conjunction with RISE-SD 2023 in Rhodes, Greece. The about 30 workshop’s participants watched demonstrations of the most mature solutions and tools that have been developed within the project, so far. The workshop**’**s aim was to get feedback from the stakeholders, to validate the methodologies and justify the focus of the project’s future developments and pilots. The discussions between the external experts and the technical partners were fruitful and engaging.

The recordings and presentations of both the workshops are available on IRIS website. Both the workshops were promoted through dedicated social campaigns on the IRIS social media, supported by all the consortium partners with reposts and posts’ sharing. Also, there were announcements on the IRIS website as well as in several partners’ websites. Finally, the workshops were promoted through the IRIS Stakeholders Community, the Advisory Board mailing list, the IRIS newsletter registrants list and the Communication Task Force joint mailing, in which ten H2020 projects participate.

Figure 15: Picture from the 2nd SIW

5.2 H2020 Synergies

The IRIS project has built strong synergies with other similar H2020 projects in order to increase the Impact of the project, identify commonalties that can lead to future cooperation and exchange of knowledge. The activities resulted from these synergies are presented below:

5.2.1 Communication Task Force (CTF)

Monthly meetings take place with the participation of the EU funded projects ARCADIAN, SECANT, SENTINEL, IDUNN, ELECTRON, TRUST aWARE, SPATIAL, ERATOSTHENES and, of course, IRIS. Several activities have taken place and efforts made for a joint dissemination strategy have been presented.

5.2.2 ELECTRON International event

The event held in Baku and online on 5-7 December 2022. This event aimed to shed light on the most critical elements in energy cybersecurity while presenting modern solutions for protecting the energy and power systems from harmful actions and cyberattacks while empowering the digital culture of European citizens. Among the H2020 projects that were presented was IRIS, represented by ICCS.

Figure 16: ELECTRON event social media banner

5.2.3 EU-made cybersecurity for safe, resilient and trustworthy applications and services Workshop

The workshop held on 27 February 2023, jointly organised by ARCADIAN-IoT, ELECTRON, ERATOSTHENES, IDUNN, IRIS, KRAKEN, SECANT, SENTINEL, SPATIAL, TRUST aWARE projects provided an overview on how novel solutions can protect the complex ICT infrastructures and create a stronger, more innovative and resilient European industry. The EU-made cybersecurity workshop was designed to provide the about 60 attendees with the knowledge to create safe, resilient, and trustworthy applications and services. The online workshop covered a range of topics related to cybersecurity, including best practices for designing and building secure applications and services, techniques for identifying and mitigating cybersecurity risks, and strategies for ensuring the resilience of applications and services in the face of cyber threats. After the organisation of the workshop, all the projects contributed and

delivered a Policy Brief based on the conclusions derived from the workshop and which was forwarded to the EC.

Figure 17: Social media banner created for the joint workshop

5.2.4 Horizon Booster

The projects participating in the Communication Task Force have decided to go a step further regarding this cooperation and have applied to the Horizon Booster Module A "Identifying and creating the portfolio of R&I projects results". Each project within the group was asked to complete a short survey. The survey investigated objectives, challenges addressed by the projects, the primary target audiences and the Key Exploitable results with the main objective of identifying the commonalities among the projects within the project group.

Figure 18: Horizon Booster logo

5.2.5 Meetings with PALANTIR project

PALANTIR is another H2020 project with which IRIS had two meetings in March 2023 with the aim of finding common ground and seek opportunities for collaboration. Hopefully, there will be

a chance for further collaboration before the end of the PALANTIR project.

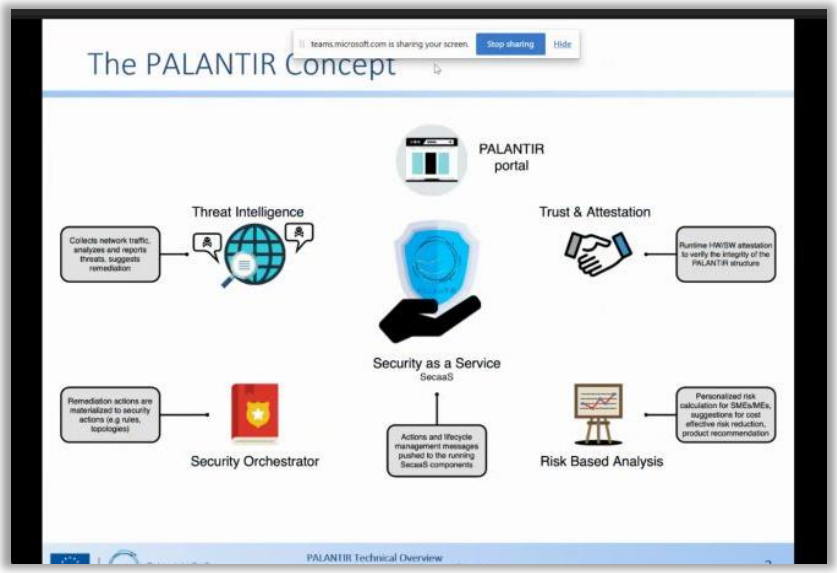


Figure 19: Screenshot from the meeting with PALANTIR project

5.2.6 ERATOSTHENES "Trust and Identity Management for IoT" Workshop

The workshop showcased how Europe's Research and Innovation community is addressing the issues of identity, trust, security, and privacy for IoT devices and network systems. The way we address these aspects will impact Europe's collective resilience against cyber threats so that citizens and businesses can fully benefit from trustworthy and reliable services and digital tools. The workshop was organised by ERATOSTHENES project as part of its 2nd formal workshop and its primal focus is on the presentation of recent technologies and outcomes as well as identification of synergies between the projects. IRIS was represented by ATOS.

Figure 20: Screenshot from ERATOSTHENES Workshop

5.3 European Cluster of Securing Critical Infrastructures (ECSCI)

ECSCI 's aim is to create synergies and foster emerging disruptive solutions to security issues via cross-projects collaboration and innovation. The research activities focus on how to protect critical infrastructures and services, highlighting the different approaches between the clustered projects and establishing tight and productive connections with closely related and complementary H2020 projects. IRIS is one of the 31 members since June 2023.

Figure 21: ECSCI Cluster

5.4 Future steps

IRIS will continue seeking for collaboration with new H2020 projects and preserve the established relationships with the projects within the CTF.

More specifically the projects of the CTF have already been organising a Joint Cluster Physical Meeting at the UNINOVA campus, Lisbon, Portugal, held hopefully next October 2023, with the objective to encourage collaboration and synergy among the various projects involved in EU cybersecurity, to address the current knowledge gap in the cybersecurity field by promoting joint training sessions and collaborative learning initiatives and finally to explore the potential of joint business exploitation plans and identify strategies for commercialising collaborative cybersecurity solutions. Moreover, all the CTF projects will continue with the Module B "Helping projects from the portfolio to design and execute a portfolio dissemination plan" of the Horizon Booster services. Finally, within the 3rd year of the project, a 3rd SIW will be organised.

6 POLICY AND STANDARDISATION ACTIVITIES FROM M12 UNTIL M24 AND FUTURE STEPS

This chapter provides an update of the policy landscape compared to what has been presented in D8.3 and gives an overview of the standardisation activities. It is structured in two parts to present the policy context and the standardisation landscape, highlighting the relevance of the IRIS project.

6.1 Policy landscape

IRIS responds to the needs of building more resilient digital infrastructures as covered in the EU Security Union Strategy[3] (July 2020) and then developed in the EU Cybersecurity Strategy for the Digital Decade[4] (December 2020).

The EU Security Union Strategy identifies the tools and measures to be developed over the next 5 years (2020-2025) to ensure security in both physical and digital environment. The priority areas include the prevention and detection of hybrid threats, increased resilience of the critical infrastructure, promotion of cybersecurity and relevant research and innovation activities. The objective of the EU cyber security strategy is to strengthen Europe's collective resilience by relying on trusted digital services and devices and resilient critical infrastructure. The strategy focuses on three main areas: resilience and technological sovereignty, developing operational capabilities for prevention, deterrence and response, and international collaboration.

As for “resilience and technological sovereignty”, the Commission intends to create a network of Security Operation Centres (SOCs) capable of detecting the signs of a cyber-attack, and platform for sharing CTI between the public and private sector. This network should be the EU's first line of defence, the so-called European Cyber Shield. In this regard, the Commission already invested EUR 110 million, with additional EUR 80 million coming from public national level and/or private sector. A call for proposal ended on 15 February 2023[5]. This first initiative was later encapsulated in the Cyber Solidarity Act, that was published by the Commission on 18 April 2023. The Cyber Solidarity Act aims at laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents. The Cyber Solidarity Act is based on three key actions: the creation of the European Cyber Shield, the Cyber Emergency Mechanism, and European Cybersecurity Incident Review Mechanism. The Cyber Emergency Mechanism will include the preparedness support and coordinated testing of critical entities, and establish the EU Cybersecurity Reserve of trusted and certified private companies that will be ready to major incidents. The European Cybersecurity Incident Review Mechanism will facilitate the assessment and review of specific cybersecurity incidents.

Regarding the “operational capacity for prevention, deterrence and response”, and increase collaboration between the public and private sector by building bridges between research and the

[3] European Commission. Communication from the Commission on the EU Security Union Strategy COM(2020) 605 final. July 2020.

[4] European Commission. Joint Communication to the European Parliament and the Council. The EU’s Cybersecurity Strategy for the Digital Decade JOIN(2020) 18 final. December 2020.

[5] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-eccc-2022-cyber-03-soc;callCode=DIGITAL-ECCC-2022-CYBER-03;freeTextSearchKeyword=;matchWholeText=true;typeCodes=1;statusCodes=31094501,31094502,31094503;programmePeriod=null;programCcm2Id=null;programDivisionCode=null;focusAreaCode=null;destinationGroup=null;missionGroup=null;geographicalZonesCode=null;programmeDivisionProspect=null;startDateLte=null;startDateGte=null;crossCuttingPriorityCode=null;cpvCode=null;performanceOfDelivery=null;sortQuery=sortStatus;orderBy=asc;onlyTenders=false;topicListKey=callTopicSearchTableState

market, the Commission has set up the **Cyber Security Competence Centre (ECCC)**[6] based in Bucharest, Romania. This centre will coordinate collaboration between a network of **National Coordination Centres (NCCs)**[7] and the community, understood as an ecosystem of companies, universities, and research institutes, that contributes to the cybersecurity of the European Union and its citizens. One of the missions of the ECCC is to foster the Union's resilience to cybersecurity incidents and ability to face and respond to those events, including supporting the implementation of specific policies, some of them will be discussed in the remaining of this section. The Centre will increase the collaboration between the public and private sector by building bridges between research and the market.

The IRIS project aims at the integration and demonstration of a single platform addressed to CERTs/CSIRTs for assessing, detecting, responding and sharing information regarding threats and vulnerabilities of IoT and AI-driven systems, addressing some of the key impact areas to achieve the mission of the ECCC. The recently approved **ECCC Strategic Agenda**[8] identifies the main priorities and actions "deemed of strategic importance in boosting cybersecurity innovation in Europe" and the following ones are relevant for the IRIS project:

- "1.1.1 *Develop and implement technologies, services and processes for supporting information sharing, coordinated and collaborative prevention, detection and response/recovery and investigation of cybersecurity incidents. This includes the development and deployment of Security Operations Centres (SOCs) across sectors and value chains, as well as strengthening the capacities and resources of the national reference CSIRT/CERT in essential and important entities defined in NIS2 and other related directives or legislations. It also includes the support and enhancement of CSIRT/CERT communities and Information Sharing & Analysis Centres (ISACs), supporting timely and secure cross-border exchange of notification data or single entry points for incident/breach notification (including mitigation actions for response and supporting cyber investigations).*
- *"1.2.1 Increase the resilience of essential and important entities defined in NIS2 including their digital supply chain against cyber threats, in line with the CRA and NIS2 directive…. "*
- *"3.4.2 Promote the creation and capacity building of Information Sharing and Analysis Centre (ISAC) style cooperation initiatives in cross-border, cross-sectoral, cross-community (including with law enforcement and cyber defence) and multi-lingual contexts, using standardised taxonomies and/or ontologies and comparable maturity indicators. The increase of shared cybersecurity information is beneficial on multiple layers: it supports improved security measures from sharing experiences and lessons learned, research activities, organisational risk management decision-making, detection and incident response, as well as other relevant domains.*

IRIS has the ambition to address part of the priorities identified above by developing solutions and tools that could contribute to a resilient EU cybersecurity ecosystem.

From a legislative point of view, the Commission has proposed directives and regulations for various products and services. The Directive on measures for a high common level of cybersecurity in the Union (NIS Directive revisited or 'NIS 2') and the Critical Entities Resilience

[6] https://cybersecurity-centre.europa.eu/index_en

[7] https://cybersecurity-centre.europa.eu/nccs_en

[8] https://cybersecurity-centre.europa.eu/system/files/2023-03/20230224%20-%20ECCC%20Strategic%20Agenda%20with%20cover.pdf

Directive (CER) are essential proposals to strengthen the resilience of critical infrastructures such as smart cities.

The NIS2 Directive was proposed by the Commission in December 2020, as an improvement of the previous NIS directive, and was subsequently negotiated in a trilogue between the Commission, the European Parliament, and the Council. A political agreement was reached by the co-legislators in May 2022 and the final technical details were added in June. The final text was voted by the plenary of the European Parliament on 10 November and it entered into force on 16 January and Member states will have 21 months to transpose its provisions into their national laws (October 2024).

The NIS2 Directive will establish a set of requirements for the cybersecurity risk management of critical entities, in particular those related to energy, health, transport and digital infrastructure. The directive aims to eliminate divergences between the member states regarding cybersecurity and reporting obligations to the public authority. To this end, it sets minimum standards and establishes mechanisms for effective cooperation between the competent authorities of each EU Member State. Compared to the first NIS, NIS2 updates the list of areas subject to cybersecurity obligations and provides for heavy sanctions to ensure enforcement.

NIS2 will apply to the critical infrastructures identified by the first NIS and to all medium- and large-sized entities operating in critical sectors such as social media, wastewater management, space, healthcare, postal services, food, and public administration at central and regional level. Entities operating in the defence, public security and justice sectors are excluded from the application of the rule.

Reporting requirements to the public authority of cyber incidents represent another key point of the standard. In fact, it will be mandatory to report to the relevant public authority and to those using the service, the impact of a cyber-attack that compromises the functioning of the service or the disclosure of sensitive data, and the actions to be taken to mitigate the damage. NIS2 also mandates ENISA to establish a European database of known vulnerabilities, modelled on the US National Vulnerability Database (NVD).

Other legislation to make the EU more digitally secure include the EU institutions' own cyber security regulation and the Cyber Resilience Act (CRA), which will propose minimum cyber security requirements for all digital products and services across all sectors. The CRA will be a turning point for European cybersecurity in the years to come and will have an impact in several sectors. The most significant impact is expected to fall on IoT products with a low level of security or limited ability to receive updates to heal vulnerabilities. There will also be a significant impact on network infrastructure hardware products and opensource software for sale. It will also try to solve the problem of supply chain security. The most sophisticated cyber-attacks in recent years have in fact targeted software and hardware components that were then used by many companies downstream in the supply chain. The CRA will have common cybersecurity requirements for all products, regardless of sector or field of application, but will also provide for three risk categories, minimum, medium and high. For the first two, a self-declaration of compliance by the manufacturer will suffice, while for the high-risk category, an external compliance check will be required. The CRA could have an impact for the IRIS solution as it might extend to IoT devices, while the GDPR, that requires the implementation of appropriate technical and organisational measures to protect personal data whenever they are collected or processed, concerns both companies that are part of the IoT supply ecosystem as well as end-user organisations.

6.1.1 Information sharing in EU Policy

One of the key aspects linked to IRIS is information sharing. Chapter V of the NIS2 Directive is about information sharing on a voluntary basis. In particular Article 26.1 indicates that "*… important entities and, where relevant, other relevant entities not covered by the scope of this Directive may exchange on a voluntary basis relevant cybersecurity information among themselves including information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat actor specific information, cybersecurity alerts and recommendations regarding configuration of cybersecurity tools to detect cyber attacks, where such information sharing: (a) aims at preventing, detecting, responding to or mitigating incidents; (b) enhances the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding such threats 'ability to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection, containment and prevention techniques, mitigation strategies, or response and recovery stages or promoting collaborative cyber threat research between public and private entities.*

ENISA should also support information-sharing arrangements, and there is a provision in the NIS Directive to avoid the imposition of additional obligations to the entities that shares information on a voluntary basis.

The proposal for a Cyber Solidarity Act creates a network of SOCs at EU level with the idea of sharing information and Cyber Threat Intelligence across the European Union. In particular, Chapter III about the European Cyber Shield defines how this network of SOCs would operate and how information will be shared. Art. 6.1 of the proposal for a Cyber Solidarity Act says that "*Members of a Hosting Consortium shall exchange relevant information among themselves within the Cross-border SOC including information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity alerts and recommendations regarding the configuration of cybersecurity tools to detect cyber-attacks, where such information sharing:*

a) *aims to prevent, detect, respond to or recover from incidents or to mitigate their impact;*
b) *enhances the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding the ability of such threats to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection, containment and prevention techniques, mitigation strategies, or response and recovery stages or promoting collaborative threat research between public and private entities".*

6.2 Standardisation landscape

This section updates the analysis presented in D8.3. Standards play a key role in ensuring inter-dependency and interoperability of technical solutions across different geographical regions and communities. As such, IRIS takes specific actions to ensure reference and integration of standards to easy the reuse and uptake of the tools and implemented solutions. The standardisation effort in IRIS is a joint activity with other work packages meant to analyse the standard landscape, orchestrate the cooperation with international organisations, and define a roadmap.

In D8.3 we reported the relevant standards identified by the IRIS partners, herein briefly reminded. The IRIS platform should support existing technical standards (MISP, STIX/TAXII etc.) and processes (RFC formats for incident response reports etc.). In particular, the IRIS Platform will contain a standardised taxonomy/ontology which is mapped to widely used, e.g. existing ENISA

and/or NIST taxonomies/ontologies (STIX 2.1, MISP Standards etc.). The Structured Threat Information Expression (STIX™), defined by the OASIS Cyber Treat Intelligence (CTI) Technical Committee, is a programming language and serialization format for exchanging cyber threat intelligence (CTI). STIX allows organisations to share CTI in a consistent and machine-readable manner, in a way which improves capabilities such as collaborative threat analysis, automated threat exchange, automated detection and response, and others.

In IRIS, the CTI threat analysis and sharing techniques will be driven by secure and efficient security information representation in standardised formats, e.g., STIX or JSON, being able to provide sharing mechanisms with external entities using standard. More specifically, the AI/IoT CTI relevant information, generated within WP3 cybersecurity threat/attack detection modules, will be structured in a standardised format. These standardized and secure CTI representation ontology (e.g. STIX v2.1, MISP Standards) will be considered in the IRIS Enhanced MeliCERTes platform, currently under development in WP4. The WP4 plans to develop a distributed ledger that provides dynamic accountability, auditing and traceability to threat intelligence publication, consumption and access control with self-encryption and recovery capabilities. Standards in this domain are under development by ISO/TC 307 and other technical groups such as CEN-CENELEC JTC19, ETSI ISG PDL, ITU-T Groups and IEEE[9].

Another technology relevant for IRIS is Artificial Intelligence, with a growing effort to develop standards and best practices to ensure integrity and confidentiality of data. In this regard, the European Telecommunications Standards Institute (ETSI) finalised five group reports offering gap analysis and definitions that could be in turn useful to scope for standards. ISO/IEC JTC 1/SC 42 is another relevant body working on standards of AI.

IRIS partners are directly involved in the standardisation committees. The table below indicates the different standards and the relevance for IRIS.

IRIS partner	Standard Organisations	Technical Committee / Working Group	Standard	Relevance for IRIS
ICCS	CEN/CENELEC	TC CEN/WS DIV	Requirements for acquiring digital information from victims during search and rescue operations	
ICCS	CEN/CENELEC	TC CEN/WS DigScen	Specifications for Digital Scenarios for Search and Rescue Exercises	
IMI	UNE	CTN178	Several with focus on Smart Cities ICT	Cybersecurity modules in Smart City Platform

[9] European Cyber Security Organisation. ECSO Technical Paper on Distributed Ledger Technologies. June 2022

IRIS partner	Standard Organisations	Technical Committee / Working Group	Standard	Relevance for IRIS
			Architectures and in particular 178104	
SID	ISO/IEC	TS 27008:2019	“information security management systems controls”	Relevant for WP3/T3.2/SiVi Risk-based selection is utilised for security management. As a consequence, the information risk management provided by the tool is enchanting.
SID	ISO/IEC		27032:2012	Relevant for WP3/T3.2/SiVi SiVi can manage many types of data, including cybersecurity events, and it follows the instructions to improve the status of cybersecurity and the services it delivers. SiVi bolsters the security domains, including information security, network security, internet security, and protection of vital information infrastructure, by these actions.
SID	ISO/IEC		27034-5:2017	Relevant for WP3/T3.2/SiVi Throughout the Systems Development Life Cycle, precise direction was provided for the development of the tool (SDLC)
SID	ISO/IEC		27035-1:2016	Relevant for WP3/T3.2/SiVi SiVi's approach to security was impacted by ISO/IEC 27035-1:2016, including basic ideas linked to information security management, efficient incident response, effective detection of information security events, and suitable assessment of such occurrences. ISO/IEC 27035-2:2016 was used to plan the tool's incident response function. SiVi and its sensors provide a full Intrusion Detection System (IDS) that follows ISO/IEC 27039:2015 for

IRIS partner	Standard Organisations	Technical Committee / Working Group	Standard	Relevance for IRIS
				deployment and operating guidelines.
SID	ISO/IEC		27042:201	Relevant for WP3/T3.2/SiVi Security incidents require additional analysis to interpret, identify, or collect information. SiVi follows ISO/IEC 27042:2015, ISO/IEC 27037:2012, and ISO/IEC 27043:2015 for digital evidence gathering and preservation.
ICCS	N/A	Network Working Group	IETF HTTP standard	Relevance for WP4: T4.3-Advanced Threat Intelligence Orchestrator. HTTP functions as a request–response protocol in the client–server model. Moreover, is an application layer protocol designed within the framework of the Internet protocol suite. Its definition presumes an underlying and reliable transport layer protocol
ICCS	N/A	ECMA-404, ISO/IEC 21778:2017, IETF STD 90 RFC 8259	JSON Data Interchange Standard. JSON Schema	Relevance for "WP4: T4.3-Advanced Threat Intelligence Orchestrator" and "WP6: T6.1- APIs for integration with the smart city's IoT- and AI-enabled infrastructures". JSON (JavaScript Object Notation) is a lightweight, text-based, language-independent syntax for defining data interchange formats. JSON Schema is a vocabulary that allows you to annotate and validate JSON documents, says json-schema.org. A language and platform agnostic tool, JSON describes a set of constraints for interaction between JSON documents. Since JSON is a common REST API data format, JSON Schema has been growing in use and importance.

IRIS partner	Standard Organisations	Technical Committee / Working Group	Standard	Relevance for IRIS
ICCS	N/A	Technical Steering Committee (TSC), Technical Oversight Board (“TOB”)	OpenAPI Specification (OAS)	Relevance for “WP6: T6.1- APIs for integration with the smart city’s IoT- and AI-enabled infrastructures” The OpenAPI Specification (OAS) defines a standard, language-agnostic interface to HTTP APIs which allows both humans and computers to discover and understand the capabilities of the service without access to source code, documentation, or through network traffic inspection.
UPC	MISP Standard		https://www.misp-standard.org/standards/	Relevance for WP4 It is necessary for the exchange of information with different CERTs that the project needs
UPC	ENISA		https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool/results#Smart%20Cities	Relevance for WP7 Good practices for IoT infrastructures, smart cities
UPC	MITRE		https://attack.mitre.org/	Relevance for WP7 Possibility to use some of the techniques defined here to perform some of the attacks on the pilots
CERTH	ISO		ISO/IEC/IEEE 29119-1:2022: Software Testing	Relevance for WP3, WP4, and WP5. To test the developed components
CERTH	ISO		ISO/IEC 27001:2013 — Information security management	Relevance for WP3, WP4, and WP5. To secure any kind of digital information
CERTH	ISO		ISO/IEC 27002:2022	Relevance for WP4/T4.1, T4.2/CTI Sharing and Storing

IRIS partner	Standard Organisations	Technical Committee / Working Group	Standard	Relevance for IRIS
			Information security, cybersecurity and privacy protection — Information security controls	To collect and analyse information relating to information security threats.
TUD	Hyperledger Foundation an open source project from the Linux Foundation		Hyperledger Fabric	Relevant for WP4 – DPA. Provides the distributed ledger software (standard for enterprise blockchain)
TUD	SAFE NETWORK	MaidSafe	Self-Encryption	Relevant for WP4 – DPA. Provides the robust encryption of the data
TUD	ISO/IEC 19592-2:2017		Secret sharing	Relevant for WP4 – DPA. Provides the basic principles of secret sharing.
CISCO	ISA/IEC	ISA99/IEC62443	Security for industrial automation and control systems	Cisco Cybervision which is part of the infrastructure of PUC1 in WP7 allows to implement ISA/IEC 62443 by providing asset visibility, defining zones and conduits and assigning controls to zones. As described here: https://blogs.cisco.com/security/it-and-ot-cybersecurity-united-we-stand-divided-we-fall?dtid=oblgcdc000651
CLS	ISA/IEC	ISA99/IEC62443	Security for industrial automation and controls systems	CLS's Nightwatch which is part of the infrastructure of PUC1 aligns to and supports the implementation of the ISA/IEC 62443 by providing OT & IoT asset visibility as well as AI monitoring, threat detection and response for industrial systems.

Table 19: Standards and the relevance for IRIS

IRIS is also monitoring a set of standards that either are used and well established or are under development.

Standard Organisations	Technical Committee / Working Group	Standard	Why this is relevant ?	Usage in WP / Task / Component
N/A	OASIS Cyber Treat Intelligence (CTI) Technical Committee.	Structured Threat Information Expression (STIX™)	STIX is a programming language and serialisation format for exchanging cyber threat intelligence (CTI). Allows organizations to share CTI in a consistent and machine-readable manner, in a way which improves capabilities such as collaborative threat analysis, automated threat exchange, automated detection and response, and others.	Related with WP4 in total and the total scope of the project.
ISO/IEC JTC 1	SC 42 has established the five working groups of Foundational Standards (WG 1), Big Data (WG 2), Trustworthiness (WG 3), Use Cases and Applications (WG 4), and Computational Approaches and Computational Characteristics of AI Systems (WG 5)	AI standardization.	The SC 42 WG 3 Trustworthiness Working Group is concerned with AI's dependability and ethics. It has conducted research and development on AI credibility, robustness evaluations, algorithm bias, and ethics, among other areas.	WP3
ISO/IEC TR 24027 Information technology		Artificial Intelligence (AI) — Bias in AI	It focuses mostly on algorithmic bias in AI systems and AI-assisted decision systems.	WP3

Standard Organisations	Technical Committee / Working Group	Standard	Why this is relevant ?	Usage in WP / Task / Component
		systems and AI-aided decision making		
		TR Information Technology — Artificial Intelligence — Overview of Ethics and Social Concern	It focuses on AI research from the ethical and social aspects.	WP3
ISO/IEC/IEEE 29119-11		Software and Systems Engineering — Software Testing — Testing of AI-Based System	It intends to standardise testing of artificial intelligence systems.	WP3
OASIS Open		CACAO: Collaborative Automated Course of Action Operations for Cyber Security	It could be relevant to Task 3.3 to potentially establish standardised response actions within the risk-based response and self-recovery module based on CACAO or to support the Permissible Actions Protocol (PAP).	WP3

Table 20: well established, used or under development standards

7 COMMUNITY BUILDING AND LIASON ACTIVITIES WITH RELEVANT STAKEHOLDERS FROM M12 UNTIL M24 AND FUTURE STEPS

After initially creating a broad list of stakeholders that is available for all partners on the IRIS Depository, our efforts were pointed towards engaging with industry representatives, more specifically Chief Information Security Officers (CISO). Established and coordinated by IRIS partner ECSO, the 1st European CISO Community brings together 348 CISOs, CISO Team Members or equivalent position decision-makers from 28 European countries. This makes it a unique Community in the European cybersecurity ecosystem with one of the main goals being a timely exchange of Cyber Threat Intelligence.

The 1st physical meeting of the CISO Community, CISO Meetup, was held in Brussels in October 2022 with the participation of almost 100 CISOs from 20 European Countries. The IRIS Project was presented by the Project Coordinator, who took advantage of this occasion to invite the CISOs to join the IRIS Stakeholder Group. By joining the Group, CISOs (and Team Members) will gain insights into challenges and solutions on how to share threat information, how to conduct effective threat response, and how to improve incident reporting to CERTs/CSIRTs which has become an essential part of the CISO tasks with the recently adopted NIS2 Directive. 14 individuals sent a request to join the Stakeholder Group and the list with a title, company and country is available below.

IRIS CISO Stakeholder Community		
Title	**Company**	**Country**
Group CISO	Generix Group	France
Cybersecurity Officer EMEA	Becton Dickinson France S.A.S. Belgian Branch	Belgium
CISO	ValidatedID	Spain
Cybersecurity Director	Barilla	Italy
Cyber Resilience Specialist	Inizio Health	Ireland
CISO	Inizio Health	Ireland
GRC and Compliance Lead	Inizio Health	Ireland
Cybersecurity Senior Expert	Électricité de France	France
CISO	Indra	Spain
Head of Information Security Architecture and Governance	Indra	Spain
Head of Information Security Engineering and Operation	Indra	Spain
Head of CSIRT	Indra	Spain
Information Security Architecture	Indra	Spain
Founder of Italian CISO Community	Via Virtuosa	Italy

Table 21:IRIS CISO Stakeholder Community

These individuals represent a group of end-users, security practitioners and decision-makers that will be invited to IRIS Events and provide input through the focus groups and evaluation sessions according to the project needs.

More specifically, the CISO Community was engaged for the IRIS Launch Event, Stakeholder and Industrial Workshops, and will be invited for the Final Exploitation Workshop.

The CISO Community was also asked to provide input on the Survey “Human factors for co-design” for the needs of the IRIS T2.6 “System evaluation and Assessment”. The survey seeks feedback from security practitioners on IRIS technology, more specifically on the social acceptance of technology, taking into account cultural specificities, behavioural patterns and the willingness to adopt innovative cybersecurity services.

In the final 12 months of the project, a Final Exploitation Workshop will be organised to involve all major stakeholders with whom links were created during the lifetime of the project. Additional stakeholders will be engaged in feedback activities based on the needs expressed by the partners participating in the technical deliverables. Finally, the work carried out in the task will be reported in the D8.8 “Report on connection with stakeholders” with the due date M36.

8 CONCLUSION

The current report provides a complete overview of the dissemination, communication, standardisation and exploitation activities that have been conducted during the second year of the project's lifetime.

The document presented an overview of the activities relating dissemination and communication of the project performed in the second year of the project and of those to come in the third year, the exploitation and business modelling activities of IRIS project implemented along with the planned future steps, all the clustering and liaising activities held with relevant stakeholders and similar H2020 projects in the past 12 months and the ones scheduled to start in the third project year, the work performed regarding the standardisation activities in the second project year and those that are about to performed in the next months and the activities and effort made to create links with stakeholders from Industry, SMEs, CERTs/CSIRTs and policy makers at the EU and national level.

The activities presented in this report demonstrate a productive second project year. Also, the high performance of these activities are an indication of a fruitful third year of the project.

A further and final update on the actions discussed and foreseen in this deliverable will be covered in the next report namely the deliverable D8.5 Final report on dissemination, communication, standardisation and exploitation, that will be submitted in month 36.

9 ANNEXES

ANNEX 1: LIST OF RELEVANT CONFERENCES & JOURNALS PER PROJECT YEAR

Event	Website	Date	Place
ESORICS 2023	https://www.esorics2023.org/	25-29 Septeber 2023	Hague, the Netherlands
Cybertech Europe 2023	| Cybertech Europe 2023 (cybertechconference.com)	3-4 October 2023	Rome, Italy
ESEC/FSE 2023	https://conf.researchr.org/home/fse-2023	11-17 Nov 2023	USA
FIC 2024	https://www.forum-fic.com/	TBC April 2024?	TBC
Cyber Act forum 2023	https://www.cyberactforum.it/?ref=infosec-conferences.com	6-Oct-23	Italy
World Summit AI 2023	https://worldsummit.ai/?ref=infosec-conferences.com	11-12 October 2023	Netherlands Amsterdam
SCEWC 2023	https://www.smartcityexpo.com/	7-9 November 2023	Barcelona and online
MWC 2024	https://www.mwcbarcelona.com/	26-29 February 2024	Barcelona Spain
Cybersecurity Congress 2023	https://www.barcel	21-23 May 2024	Barcelona Spain
cybersec europe 2024	https://www.cybers	29-30 May 2024	Brussels Belgium
Global IoT Summit 2024	Home - Global IoT Su	TBC June 2024	TBC

Relevant Events 2021-2022 | 2022-2023 (until Aug 2023) | **2023-2024 (from September 2023)** | Journals

Figure 22: List of relevant events and journals

ANNEX 2: UPDATED DESCRIPTION OF THE KEY EXPLOITABLE RESULTS

ID	Updated Description
KER #1	IRIS devises the 'close the loop' model, which aims to observe, understand, and evaluate how social acceptance drives the market of AI-based cross-border technology. This model includes the six fundamental dimensions over which social acceptability is measured and assessed. The method of evaluating technological follows these steps: (i) perception works on a subject's conscious and subconscious mental patterns; (ii) motivation illustrates the moral basis according to which subjects align their preferences; (iii) trust represents the level of reciprocity of individual and social expectations; (iv) awareness shows the ability for individuals to choose and judge using universal values; (v) capacity for action pinpoints to what extent a technology enables people to all of the above; (vi) accountability refers to the degree to which a society and its institutions can introduce policies that favour complex models of acceptance. Technology acceptability is measured and assessed through a two-step approach. The first step is carried out through a set of tools (including inter-alia questionnaires, webinars, roundtables, sentiment analysis) extracting information about the psychological status and feelings of a collective at a given point in time. The information obtained at the end of this first assessment step represents a predictive analysis of the social impact on stakeholders' expectations. It is further used to derive specific topics to formulate target questionnaires to be submitted in the second assessment phase to the group of IRIS stakeholders selected for the project's pilots. The questionnaires will be used to evaluate the IRIS platform, based on the already-assessed technology, in both the lab and in realistic scenarios. Thus, a set of more pertinent IRIS-related questions are built, and answers will be compared to data collected during the first phase.
KER #2	A key aspect of any risk assessment process is the identification and analysis of vulnerabilities and potential risks associated to the assets, services and devices that belong to the monitored infrastructure. IRIS will extend current approaches in risk and vulnerability assessment by providing IoT and AI-provision capabilities to map abnormal behaviours detected in the target system with attack patterns that can be associated to the presence of zero-days vulnerabilities. It will also offer sharing mechanisms with external entities using standard well-known standards and formats (e.g., JSON, STIX). In addition, it will enrich the knowledge base through vulnerability feeds from open source threat intelligence platforms (e.g., MISP), and will perform a thorough risk analysis that comprises the identification of several security factors, such as root causes (considering aspects such as complexity, design flows, human factors); impact (considering aspects such as data at risk, severity, damage); and remediation (considering aspects such as cost, recovery time, resilience, etc.).
KER #3	Detecting attacks against IoT and AI-provisions introduces a unique challenge for traditional proactive threat detection systems, such as network or host-based intrusion detection systems. Attacks against IoT systems often take advantage of a lack of inherent security in their data generation and consumption and the inherent embedded and static nature of their operation, whereas for AI-provisions attacks are subtly interweaved in input data that is designed to disrupt or confuse their decision-making process. To address this challenge, IRIS will extend the capabilities of traditional intrusion detection systems to monitor the unique characteristics of IoT and AI-provision, such as the data they consume and

ID	Updated Description
	generate, as well as their responses to different technical workflows and interactions between them. IRIS develops machine learning anomaly classifiers for IoT, and AI that will monitor for abnormal deviations in behavioural data telemetry and decision response. The autonomous threat analytics engine employs a threat-intelligence enriched knowledge-framework to monitor attack patterns against IoT infrastructure and AI-provisioned systems.
KER #4	IRIS introduces a novel risk-based response mechanism that intelligently models attack and threat inputs from multiple sources (e.g., via the ATA module detection engine or the CTI module), leveraging insights from IoT and AI-provision risk and vulnerability assessment module in ATA. This risk-based response will apply game-theoretic strategies for finding optimal response solutions based on the impact of threats and the likelihood of their realisation and the expected impact mitigating response actions may have on the system. IRIS's risk-based decision making will be supervised with policies defined by CERT/CSIRT operators. The policies will establish the trigger/threshold conditions for self-recovery based on the optimal impact resolution reported. For example, in the case of data poisoning attacks to an AI-provision, the risk-based response process will decide whether to act on self-recovery procedures or changing its model configuration based on the policy set by human operators. The system will support reporting the response and decision-making criteria in an explainable format. For each identified risk, and optimal response solution, IRIS will extract a standardised set of actions that will represent the optimal response and self-recovery strategy.
KER #5	IRIS develops a Digital Twin Honeypot for IoT and AI-provisioned applications and services to accurately analyse and predict threats against specific technological interfaces. Digital Twin cybersecurity measures provide a crucial attack telemetry channel to the ATA and CTI modules for field-testing new IoT and AI technology. Digital Twins expose functional and internal systems components that can facilitate the discovery of new attack vectors. The Digital Twin honeypots serve as tripwires that support automated threat intelligence orchestration for implementing proactive defence measures against threats that have yet to materialise or be identified on production systems. As part of the Digital Twin honeypot development cycle, a collection of data computational models and representation models will be applied. It will perform analytics and processing during the honeypot lifecycle phases. Using AI algorithms, inferred data acquired during the run time will be incorporated into the Digital Twin knowledge base. This will enable continuous learning and feature enhancement. The Digital Twin honeypots will support customized analytics and will perform a series of cybersecurity tasks, such as Threat Detection, service analysis, incident sharing, and incident response. Adaptive high-interaction Digital Twin honeypots will be capable of scaling operations and adapt to threats against IoT and AI-driven systems that will allow continual learning. By employing the capabilities of software-defined operations and leveraging low-overhead virtualization environments, IRIS's Digital Twin honeypots will extend current capability beyond the state-of-the-art, which is statically defined using configuration files.
KER #6	Several ongoing research and development activities [SGAV20] show the need of the society to efficiently handle threat intelligence, security information, and incident sharing for the effective prevention, management, and response of cyber-attacks against services or critical infrastructure. There is increased ongoing effort, coordinated by ENISA, to establish a de facto platform for security information

ID	Updated Description
	sharing, secure online communication and collaboration among all relevant stakeholders offering services or owners of CIs and CERTs/CSIRTs. A relevant open-source software platform has been built, MeliCERTes CSP (https://github.com/melicertes/csp), co-developed by INTRA (in the context of the SMART 2015/1089 tender call and awarded project [EC19]) to provide such capabilities in a distributed architecture (i.e., different instances running at the infrastructure of different authorities) – the target users have been CERT/CSIRT authorities. While a follow up project has been funded to be extended and adopted by the relevant authorities. MeliCERTes is widely adopted by the community and open-source platforms, such as MISP. Another project that INTRA is a partner, has been funded to support the development of ISACs and tools for secure information sharing and incident reporting. Other relevant indicative platforms, that provide specific functionalities (primarily focused on threat intelligence), are the OpenCTI (https://www.opencti.io/en/), which is open source, and Anomali (https://www.anomali.com/) its commercial counterpart. In IRIS, the above ongoing efforts will be extended and enhanced, to allow (i) for more secure and efficient security information representation in standardized formats and sharing capitalizing and extending existing ontologies, such as STIX 2.1 (https://oasis-open.github.io/cti-documentation/stix/intro.html); (ii) to securely share any type of disclosed information for better preparation, detection and response capabilities (such as threats, vulnerabilities, incidents, countermeasures, etc.); (iii) to securely communicate and collaborate online with a more extended pool of stakeholders/operators of essential services or critical infrastructures and with the CERT/CSIRT authorities, capitalizing on the capabilities of the underlying technologies of the proposed enhanced MeliCERTes ecosystem; (iv) to securely store and augment the cybersecurity knowledge base of AI targeted attacks, incidents, countermeasures, etc. at a European level; and v) to provide customised views of its dashboard and security incident reporting capabilities, access control and access rights to shared data in accordance to the type of user/operator and the type of service/infrastructure they provide. The architecture of the enhanced MeliCERTes ecosystem will be distributed, with different customised instances deployed at each stakeholders' premises.
KER #7	The progress made in the cybersecurity field in the last years, although resulting in effective and efficient tools, sets a challenge for Security Operations Centres (SOCs), CSIRTs and CERTs to manage them and their diverse functionalities (including those related to threat detection, sharing, responding and recovering). IoT and AI-driven systems require special methodologies, compared to more traditional ICT systems, to be protected by potential cyber-attacks. This demands extensive manpower for monitoring, decision-making and remediation processes. For these reasons a new approach is being adopted by the cybersecurity community by developing Security Orchestration, Automation and Response systems that converge all the tools, systems and applications within an organization. The IRIS Advanced Threat Intelligence and Analytics Orchestrator ensures that all the essential steps for cyber-incident detection, reporting/sharing and response/recovery will be implemented by integrating the toolset provided by the ATA and CTI components of IRIS platform. The integration will be made by providing interfaces, intelligent workflow (playbooks and runbooks) design, automatic/semi-automatic execution capabilities (Orchestration Workflow Manager OWM) and a workflow execution engine. The OWM will offer a workflow design functionality, orchestration process monitoring and Threat Sharing and Response

ID	Updated Description
	tasks management by a tracking system for the automated or semi-automated processes. In the event of a cyber-attack detection the response and self-recovery module will be capable of interacting with the ATAs' risk and vulnerability assessment and detection engine and the CTI Threat Intelligence Companion. For any intervention requiring human-in-the-loop, the Threat Sharing and Response manager will provide information (coming from the CTI module and the MeliCERTes platform) about the recommended response measures. Additionally, a risk-based optimisation/ranking module will support CSIRTs/CERTs on decision making**.**
KER #8	Organisations, CERTs/CSIRTs, and other stakeholders can collectively increase their cyber resilience by sharing threat information. The IRIS platform will include a collaborative threat intelligence sharing component, which will be part of the CTI module. This will be responsible for (i) allowing the connection and exchange of information among different components of the architecture as well as the collection of information from external repositories; and (ii) supporting the collaboration among all stakeholders when analysing threats. The threat intelligence sharing component will be the "brain" of the CTI, providing a connectivity nexus among the orchestrator, the ATA and DPA modules of the platform, the collection of information from external repositories, and their sharing configurations. It will automatically collect the threat intelligence extracted from the ATA module and enhance this information (a) by utilising and correlating the intelligence collected locally and through external feeds; (b) and by leveraging the dynamically generated taxonomies and ontologies. The sharing component will automatically be updated when new data entries interact with the DPA to store the collected information efficiently and securely in the cloud using DPAs' blockchain-based storage mechanisms. It will provide a GUI that will support the presentation and editing of the collected data and the configuration of the underlying gathering, correlation, and sharing procedures. To account for the challenges introduced during threat intelligence sharing, the module will follow proposed guidelines for secure information sharing (e.g., NIST 800-150) and the best security practices and security requirements (including privacy related requirements) from the platform's stakeholders. Advanced filtering and anonymization techniques will be supported to protect organisations from accidentally sharing classified information and to meet each organisation's sharing requirements. Moreover, the collaborative nature of the platform will allow the analysis of common threats among different organisations which will result in a holistic perspective of threats. IRIS users will be able to access through a human friendly GUI the information shared by other stakeholders, the extracted intelligence, add new information, propose changes in the existing knowledge, and comment/discuss. Furthermore, new data added to the platform will be automatically correlated with existing intelligence (extracted by the platform's modules or retrieved from external sources) based on different attributes (such as Indication of Compromise - IoC) to avoid analysing processed data and expand the existing knowledge about specific threats.
KER #9	The cybersecurity threat landscape sees novel and impactful attack vectors and vulnerabilities reported daily. Large volumes of information related to emerging threats require continuous collection, dissection, and analysis so that Tactics, Techniques, and Procedures (TTPs) of malicious actors can be recorded and systematically formulated. TTPs for traditional attack vectors have matured into the development of a consistent framework of threat repositories for consumption by CERTs and CSIRTs. However, 'next generation' attack vectors targeting unique

ID	Updated Description
	IoT and AI-provisioned systems are not documented in threat intelligence repositories. This gap in 'next-generation' IoT and AI threat intelligence formulation can be largely attributed to a lack of technical understanding of such attacks, their characteristic attributes, behaviour, and impact. To address this gap, IRIS will propose a dynamic knowledge repository on evolving threats that specifically target IoT and AI-enabled ICT systems. The aim of this repository will be to both facilitate the detection of these threats and support the orchestration of risk-based response and recovery. The repository will receive and store structured intelligence from threats identified by the Automated Threat Analytics module (ATA) and enrich this information with risk-based analysis to facilitate autonomous response processes and self-recovery procedures. The produced knowledge base will cover threats to both cybersecurity and privacy, focusing on (i) threats introduced by cyber-physical vulnerabilities in IoT platforms; and (ii) threats targeting AI-enabled systems by utilising, adversarial techniques to attack the algorithms and autonomous decision-making processes they employ. To facilitate the enrichment of the knowledge base, the repository will be based on existing taxonomies and ontologies related to threats targeting IoT and AI-based systems, such as those already defined by NIST (Draft NISTIR 8269). Techniques for generating dynamic taxonomies and ontologies in a (semi-)automatic way will be proposed utilising rule-based and machine learning-based methods. Named entities and concepts of interest will be extracted from attack telemetry and the relations among them will be estimated. The resulting information will be subsequently verified and updated by domain experts.
KER #10	To support a distributed, collaborative, and secure threat intelligence system, IRIS will combine a cloud-based storage system with a DLT. The cloud-based storage system will store full copies of data flows generated across systems, and the DLT will be used as mini digital twins and an immutable event log for the collaborative threat intelligence network. The ledger will store data pointers which securely link to the cloud storage system. IRIS will provide a permissioned ledger and make use of ledger and cloud access control mechanisms to enable all partners to deliver a smart and intelligent collaboration. IRIS will leverage DLT to maintain data integrity, traceability, and immutability in its whole data life cycle. IRIS enables a collaborative threat intelligence community to maintain its own permissioned ledger within an authenticated private network. Within the private network, the system autonomously defines ledger data access, read/write policies within its infrastructure, and monitors a general view of data flow. Permissioned ledger access can be dynamically extended to external partners on-demand. In addition, IRIS will ensure data and event traceability across the collaborative threat intelligence system and provide ledger security: (i) Block data integrity - tamper-proof ledger data; (ii) Block data verification; (iii) Mining validation; (iv) Agreement on validation - a majority or all network users to reach an agreement on validation via PBFT; (v) Membership authentication - provide access control over ledger (read & write rights) for authenticated partners; (vi) Guarantee of actions - deliver a mechanism that an action will be executed; (vii) Customized block data security to provide multi-level data protection on the ledger. An extensible smart contract will be leveraged and deployed in the core of IRIS's DLT platform as real-time event recorder and trigger to ensure the collaborative threat intelligence community event log and attestation history to be traceable, immutable, and end-to-end transparent to authenticated partners. The novel combination of smart contract, ledger access

ID	Updated Description
	control layer and secure tools will be used to guarantee ledger security. No action can be deniable and untraceable by using IRIS's DLT design.
KER #11	IRIS will use encryption techniques to protect ICT data from being compromised and tampered by network attackers. IRIS will investigate the usage of encryption schemes such as self-encryption (SE) to provide end-to-end encryption to the privacy toolkit. IRIS will re-design and re-implement SE in a novel way by: (i) injecting randomness into each key to make the key and its encryption randomised. This will help encrypted data chunks void static encryption attacks; (ii) leveraging a chain mode on data chunks to maintain the whole integrity of all chunks and make them tightly bounded in ciphertext format; (iii) injecting digital fingerprints into data, e.g., identity, device serial number, so that data can be tracked and linked to fingerprints. This will provide flexible traceability of data. To enhance the data traceability in data computation, quality evaluation, risk assessment, and other real-time data analysis, IRIS will use a lightweight cryptographic digital signature (DS). IRIS will bring anonymity to SE and DS as it will only allow a trusted authority to reveal and examine the identities behind the encryption and signatures. Anonymous encryption and signature schemes will be used to hide the identities either in a group of users or in encryption/decryption and signature keys. To support data recovery, IRIS will use a secret sharing (SS) scheme. The IRIS's SS scheme will be developed to enable (1) a data sender (e.g., a gateway or data centre node) to encrypt a piece of information flow using an encryption key; (2) the data senders splits the corresponding decryption key (i.e. a piece of secret information secret share) for a group of data receivers (e.g., a group of local network nodes); (3) as long as some receivers, in which the size of the receivers must reach a special number - threshold, work together to reconstruct the decryption key. IRIS will further merge the privacy toolkit- a mix of SE, SS, and DS on the ledger to safeguard the confidentiality of data, traceability of data source, flexibility, and data recovery. Any change and operation related to the toolkit will be reflected on the ledger by the smart contract.
KER #12	Training for CERT/CSIRTS analysts and in general for cybersecurity professionals is an effective solution for mitigating risks, as it fosters awareness, refine technical skills, and improve the adoption of well-tested processes. Nonetheless, to enhance effectiveness, training requires mandatory hands-on sessions where trainees put in practice what they have learned during the theoretical lessons. On the human level, the virtual training exercises revolve around two distinct teams (1) the "red team", made up of professional penetration testers, belonging to the organisation of Cyber Range. They reproduce targeted attacks of increasing complexity, to challenge the defence according to its room for improvement throughout the training; and (2) the "blue team", responsible for the defence of networks and information systems, which is therefore made up of trainees participating in the training program. Cyber Range will also have to implement training courses, to transfer to the trainees not only knowledge, but also the abilities and attitudes that meet the needs of CERTs/CSIRTs.
KER #13	These represent virtual IRIS enhanced-MeliCERTes nodes including fully functional ATA, CTI and DPA modules. Indeed, each one of the IRIS components developed as part of the ATA, CTI, and DPA modules will be provided also as a standalone pod version to be employed as core building block to the VCR environment. The VCR enabled pods will be employed for testing, validation, and training purposes. To ease the composability of complex scenarios using those

ID	Updated Description
	pods, IRIS will leverage on standardised YAML-based information models aimed at providing simple yet effective management and configuration, simplifying the advertising of computation, network, and storage requirements and the external connections of assets. Inter-pods communications will make extensive use of RESTful interfaces to simplify their runtime orchestration and will align with cloud-native principles.
KER #14	IRIS will deliver an immersive virtual environment platform for modelling and emulating real-world scenarios enabling collaborative CERTs/CSIRTs training. The cyber range platform will operate as a sandbox to train and test new response methodologies in a safe environment. It will eliminate the risk of data loss or adverse impact on operational components. It will leverage established virtualisation technologies and softwarised components, to enable ultra-fast and automated deployments and the capability to run on both managed (e.g., AWS, Google Cloud Platform, Microsoft Azure) and local deployments (e.g., based on VMWare vSphere, OpenStack, Kubernetes). AI and ML concepts will be used to create non-scripted simulation experience (e.g., emulating attackers, defenders, and end-user behaviours). IRIS cyber range platform will support multiple users working either independently over the same replicated infrastructure (or on different infrastructures) or cooperating as a team on a single target. Moreover, it will provide an easy to use catalogue of assets for setting up training scenarios (via drag & drop or via description models), including all the ATA, CPI, and DPA pods developed in IRIS. The cyber range platform will host the virtualised SIEM (Security Information and Event Management) component, grouping security information and event management functionalities for the real-time monitoring and notification of security events of the emulated system; these, once filtered and appropriately grouped together, will be presented into a management/supervision dashboard for setting up and monitoring the exercises, and a user interface capable of providing situational awareness to the trainees.
KER #15	The proliferation of IoT-enabled infrastructure has provided significant benefits for both societal and economic contexts in urban and city environments. The advent of connected sensors, lights, and meters has enabled the application of novel AI. The AI is used to implement intelligent automation and orchestration capabilities for services, providing cost savings and efficiencies in reducing workforce and maintenance requirements, and energy consumption. However, malicious actors aim to disrupt, degrade, intercept or control the data and function of the IoT-enabled infrastructure while the aggregation of data from multiple data sources introduces a further privacy and confidentiality risk. Within this pilot, the IRIS platform will monitor intermediate and upstream IoT control systems and gateways providing CSIRTs with a sophisticated capability to detect and report threats to the distributed IoT-infrastructure interfaces. Specifically, the IRIS's ATA module will provide a dynamic threat detection and response toolkit for operators. Simultaneously, IRIS's CTI module will communicate threat intelligence with IRIS's stakeholders (e.g., municipal/national CSIRTs/CERTs) that monitor related vulnerable platforms (e.g., SENTILO, WONDERWARE) as to the impact of the breach on IoT-infrastructure and control systems.
KER #16	Modern solutions to public transportation include autonomous vehicles with a which can optimise their behaviour using AI approaches. This autonomy leaves a city exposed to highly impactful cyberattacks via the attack surface created by the autonomous vehicles and their surrounding infrastructure. Further, targeting

ID	Updated Description
	directly or indirectly AI, the aggregation of citizen data required for subscription to the smart transport services is severely threatened. This pilot scenario will demonstrate the potentially catastrophic consequences of a coordinated attack to the infrastructure of a modern, AI-controlled public transportation system; and where IRIS can minimise impact by identifying the threat, self-recovering from it and sharing the corresponding intelligence with other related system operators and platforms. By using the IRIS platform, system operators can effectively identify when specially crafted data, designed to confuse AI-based decision making, (e.g., spoofed/fuzzed) is received from onboard vehicle sensor, or injected directly to APIs using directly monitored data on targets systems or via it's unique Digital twin honeypots. Operators can then leverage IRIS to self-recover from such malformed data injection. IRIS's CTI provision will provide collaborative parties to discover and share attack signatures to respond to IoT and AI-targeted attack vectors. Moreover, IRIS will provide CSIRTs/CERTs with the tools capable of identifying where an attack has breached, and exposed, large-scale private data. Such privacy data breach identification equips incident response with key information to operate at speed for protecting citizens from vulnerable IoT and AI systems.
KER #17	The city of Helsinki, introduced in 2014, a requirement for the Kalasatama district which states that all the new buildings must have an API that connects them to smart grid and electrical energy markets. The API should follow the IEC 61987 standard on Common Information Model and its communication should be secured with a Virtual Private Network (VPN). Malicious actors can manipulate the localised information that smart buildings elicit from their environment to initiate cascading attacks to the smart grid. Smart Buildings can participate in the energy market, since they have a data interface that provides information on consumption of electricity (smart meters). Additionally, they provide load control functions that the distribution system operator (DSO) can use in situations where the production has reached its peak. In this pilot, the IRIS deployment can reduce the likelihood of a malicious actor in compromising components of the smart grid through their APIs and localised interfaces. IRIS will be able to monitor the interfaces of the smart grids and their automated decision-making processes to increase their security posture. Behavioural anomalies, which deviate from the normalised operations will be more easily detected and shared between relevant stakeholders for auditing and analysis. Crucially, the IRIS VCR platform and its Lab Pods provide a comprehensive and interactive learning environment for CSIRTs/CERTs monitoring critical infrastructure for smart cities to train and gain experience executing IRIS-enhanced incident response against novel AI threats. As the VCR exercises emulate real-world scenarios, rich collaborative threat intelligence activity between the IRIS stakeholders within exercises will take place through policy-based sharing of threat data, activated by human-in-the-loop automation and orchestration, propagating at speed actionable indicators of compromise such as malware signatures, malicious network traffic records, etc. IRIS will demonstrate within its extensible VCR sandbox, how the platform arms CSIRTs/CERTs with formidable detection (ATA), threat intelligence orchestration (CTI), privacy and policy-aware data sharing and distribution (DPA) capabilities, which allow for swift threat identification, precision response and collaborative intelligence sharing tools and technologies
KER #18	As a whole, the IRIS artificial intelligence threat reporting and incident response platform will provide a dynamic, holistic and disruptive security-enabling solution for minimising the attack surface in these complex ICT systems by exploiting (i)

ID	Updated Description
	emerging automated threat detection and analytics mechanisms and honeypot-style defences to augment machine learning for deception; (ii) beyond the state-of-the-art machine learning and deep learning methods and privacy-aware analytics; (iii) novel encryption/decryption algorithms with recovery/self-healing capabilities; (iv) the latest distributed ledger technologies providing a viable scheme for enabling security, reliability, accountability, preserving privacy, and assuring trustworthiness when cyber threat information is being shared among network of CERTs/CSIRTs; (v) automated remediation strategies; and (vi) structured training and cyber exercises to prepare CERTs/CSIRTs to protect critical infrastructures and systems. One of the strengths of the platform is that it allows to test large-scale IoT and AI-driven ICT infrastructures as well as to test automated remediation strategies by exploiting the IRIS's cyber range capabilities towards emulating complex ICT systems. By implementing this highly flexible and scalable virtual cyber range service, IRIS introduces innovations in the field of cybersecurity training, with the human-centric force-on-force cyber games and exercises, assisting the next-generation CERTs/CSIRTs to collaboratively improve their ability in handling and forecasting security incidents, complex attacks, and propagated vulnerabilities in IoT and AI-driven ICT systems. Another major strength of the platform is that it enables seamless secure exchange of CTI information, incidents and response policies among the involved stakeholders being it Critical Infrastructure Operators and CERTs/CSIRTs in an attempt to increase the cyber awareness, preparedness and cyber resilience of Critical Infrastructures and enable advanced collaboration of the latter with CERT/CSIRT authorities**.**
KER#19	Synthesis of KER #2, #3, #4, #5
KER#20	Synthesis of KER #6, #7, #8, #9
KER#21	Synthesis of KER #12, #13, #14
KER#22	Synthesis of KER #10, #11

Table 22: Updated IRIS KERs