Artificial Intelligence Threat Reporting and Incident Response System

D8.3 Initial 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:	31/8/2022
Deliverable Submission Date:	30/8/2022
Deliverable Version:	V1.1
Main author(s) and Organisation:	Maria Tsirigoti (ICCS) Irene Karapistoli, Irene Tabakis (CLS) Sebastijan Čutura, Nina Olesen, Roberto Cascella, Luigi Rebuffi (ECSO) Sebastien Bardin (CEA)
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	22/07/2022
Peer Review 1	Sebastijan Čutura	ECSO	27/07/2022
Peer Review 2	Sebastien Bardin	CEA	29/07/2022
Submitted by (Project Coordinator)	Gonçalo Cadete	INOV	30/8/2022

Contributors

Organisation
All IRIS partners

Document History

Version	Date	Modification	Partners_
V0.1	18/07/2022	Draft Version (missing input for exploitation and standardisation)	ICCS
V0.2	20/07/2022	Draft Version (missing input for standardisation chapter and part of exploitation chapter)	ICCS, CLS
V0.3	22/07/2022	Draft Version (missing input for standardisation chapter	ICCS
V0.4	29/07/2022	Review and input by ECSO	ECSO
V0.5	29/07/2022	Review and input by CEA	CEA
V1.0	23/8/2022	Version for submission	ICCS, CLS, INOV, ECSO
V1.1	30/8/2022	Updates communication indicators	ICCS, INOV

Legal Disclaimer

IRIS is an EU project funded by the Horizon 2020 research and innovation programme under grant agreement No 101021727. The information and views set out in this deliverable are those of the author(s) and do not necessarily reflect the official opinion of the European Union. The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any specific purpose. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein. The IRIS Consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.

Contents

List of Figures

List of Tables

List of Abbreviations and Acronyms

Abbreviation/ Acronym	Meaning
AI	Artificial Intelligence
ATA	Automated Threat Analytics
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
CSP	Cyber Security Platform
CTI	Cyber Threat Intelligence
D	Deliverable
DG	Directorate-General
DLT	Distributed Ledger Technology
DoA	Document of Action
DPA	Data Protection and Accountability
EC	European Commission
ECSO	European Cyber Security Organisation
EU	European Union
HitL	Human-in-the-Loop
ICCS	Institute of Communication & Computer Systems
ICT	Information and Communication Technology
INTRA	Netcompany-Intrasoft
IoT	Internet of Things
IPR	Intellectual Property Rights
KERs	Key Exploitable Results
KPI	Key Performance Indicator
MISP	Malware Information Sharing Platform
NCP	National Contact Point
Q&As	Questions & Answers
R&D	Research & Development
R&I	Research & Innovation
REA	European Research Executive Agency
SMEs	Small and Medium Enterprises
SOAR	Security Orchestration, Automation and Response
T	Task
VCR	Virtual Cyber Range
VDM	Vulnerability Discovery Manager
WP	Work Package

EXECUTIVE SUMMARY

The purpose of this deliverable is to provide a report of the activities performed in the IRIS project in its first 12 months regarding the dissemination, communication, policy, standardisation, and exploitation of the project. The document sets out the activities and impact of actions undertaken by the IRIS project partners.

The document begins with the presentation of the IRIS Dissemination and Communication activities and tools. Then, it describes the internal reporting procedure established to keep a record of the dissemination and communication activities and their evaluation based on the expected Key Performance Indicators (KPIs) mentioned in the Grant Agreement (GA). Moreover, there is a reference on the future dissemination and communication plans. The final sections refer to the policy, standardisation and exploitation activities performed up to month 12 of the project.

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 and 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 dissemination and communication activities that have been undertaken during the first twelve months of the project, as well as those still planned. The deliverable also includes the analysis of the policy and standardisation landscape relevant for IRIS as well as all the exploitation activities performed.

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 to learn 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 D8.3 "Initial 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 will serve as guiding document for the future deliverables:

D8.4: Interim report on dissemination, communication, standardisation and exploitation, which will include all dissemination, communication and standardisation activities that have been undertaken, during the first two years of the project, and those still planned.

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 summarise the most important dissemination, communication, and standardisation achievements of IRIS during the project 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 IRIS DISSEMINATION AND COMMUNICATION CHANNELS AND ACTIVITIES UP TO M12

All the dissemination 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" with the aim to raise awareness for the project, engage the defined stakeholders and promote the project's goals and outcomes. To this end, there was a regular flow of information about the project though the social media and the website, open dialogue with defined stakeholder groups, as well as promotion of the project mostly within Europe but also internationally. Each activity is followed by a table presenting the related expected Key Performance Indicators and the currents status.

2.1 Project identity

The IRIS project is trying to build a strong project identity through effective branding and delivering clear messages to a variety of target audiences. A project logo, a colour palette and a dedicated brand book have been designed to create a consistent appearance that will be used in all applicable communication and dissemination channels (website, leaflets, poster, templates, and presentations). This is the most effective way to ensure that a consistent IRIS project identity is widely communicated. The official logo, the colour palette and the brand book are all available in the IRIS repository for the IRIS partners and on the website for the general public. A detailed description of the IRIS logo, colour palette, brand book and templates are presented in chapter 4.1.2 of the deliverable D8.2 "Plans for Dissemination, Communication and Exploitation" which was submitted in M6.

2.2 IRIS Brochure & Rollup banner

The first version of the IRIS brochure and roll-up banner are available in the IRIS repository, the IRIS website and the IRIS Zenodo Community for all partners to use at conferences, workshops, meetings and events. A second version of the brochure and another two versions of the roll-up banner will be produced by the end of the project. Both the brochure and the roll up banner are presented also in the chapter 4.2.1 of the deliverable D8.2 "Plans for Dissemination, Communication and Exploitation" which has been submitted in M6.

Table 1: Expected and Current Performance regarding IRIS Dissemination Material

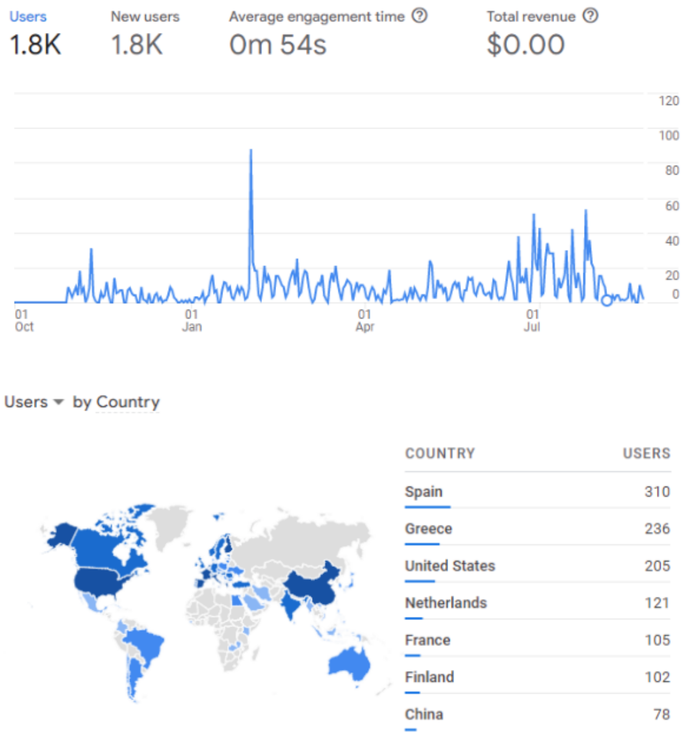
Activity	KPI M36	Current Status
Dissemination Material	2 brochures & 3 roll up banners	1 brochure & 1 roll up banner

2.3 General Presentation

An IRIS General Presentation was created at the beginning of the project. The presentation includes general information about the project such as the consortium partners, the duration, the website and social media, the aim and objectives of the project and information about the architecture and the three pilot demonstrations. The general presentation can be used with no prior approval from the consortium to conferences and events and it is available on the IRIS repository. The General Presentation has been used, in some cases with few changes, in most of the events IRIS partners have participated in. The General Presentation is presented in Appendix I.

2.4 Website

The IRIS website www.iris-h2020.eu went live at the beginning of the project. Its concept, objectives, design, and many more details are presented in the deliverable D8.1 "Project Website" submitted in M3.



Users 1.8K | New users 1.8K | Average engagement time 0m 54s | Total revenue $0.00

COUNTRY	USERS
Spain	310
Greece	236
United States	205
Netherlands	121
France	105
Finland	102
China	78

Figure 1: IRIS Website statistics 1st year

Table 2: Expected and Current Performance regarding IRIS website

Activity	Expected KPI	Current Status M12
www.iris.eu	5000 per year	1800
	Ready by M2	accomplished

2.5 Social Media

Social media play an important role in making our stakeholders aware of the IRIS project and highlighting our progress. IRIS is currently active on three social media platforms: Twitter, LinkedIn, and YouTube. Details on the IRIS social media profiles can also be found in chapter 3 of the deliverable D8.2 "Plans for Dissemination, Communication and Exploitation" which was submitted in M6. A social media grid can be seen below which displays the rationale for the platforms that IRIS will be active on throughout the project.

Table 3: Social Media Grid

Media	Reasons
Twitter	• Active base of relevant stakeholders (i.e., other projects, researchers) • Effective for 'live-tweeting' of events (i.e., plenary meetings, conferences) • Provides strong interaction and engagement with stakeholders thanks to retweets, tags, likes
LinkedIn	• Wide base of professional stakeholders • Allows different type of engagement (i.e., more focused on dissemination than communication)
YouTube Channel	• The ideal platform for sharing video content

2.5.1 Twitter

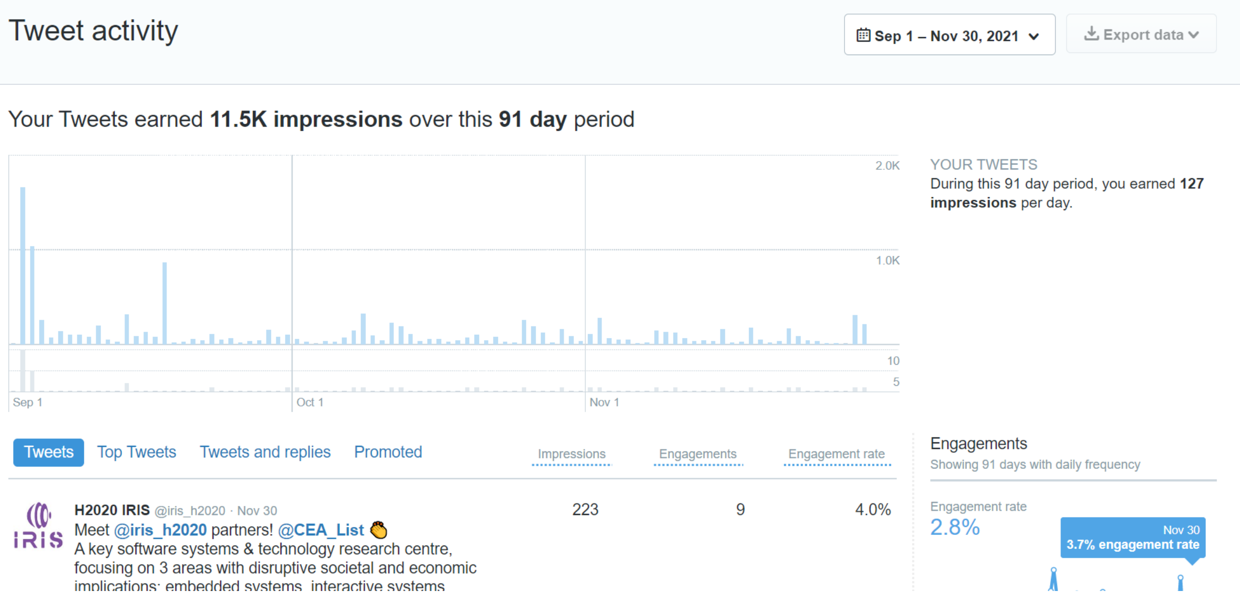
@iris_h2020 is mostly used to raise awareness about the project's progress, interact with key stakeholders, and build relationships with other H2020 projects as well as to disseminate the project's news and current results. The account has gained 293 followers and made 160 tweets up until M12. In the table below you can see the impressions[1] gained and engagement[2] rate of the project's tweets since the beginning of the project, according to the Twitter analytics.

Table 4: Impressions and Engagement Rate of tweets

Period	Total Impressions	Engagement Rate (average)
September 2021-August 2022	38 K	3,5%

[1] Number of times users saw the tweet on Twitter

[2] Number of engagements (clicks, retweets, replies) divided by the total number of impressions



Tweet activity

Sep 1 – Nov 30, 2021

Export data

Your Tweets earned **11.5K impressions** over this **91 day** period

YOUR TWEETS
During this 91 day period, you earned **127 impressions** per day.

Tweets | Top Tweets | Tweets and replies | Promoted

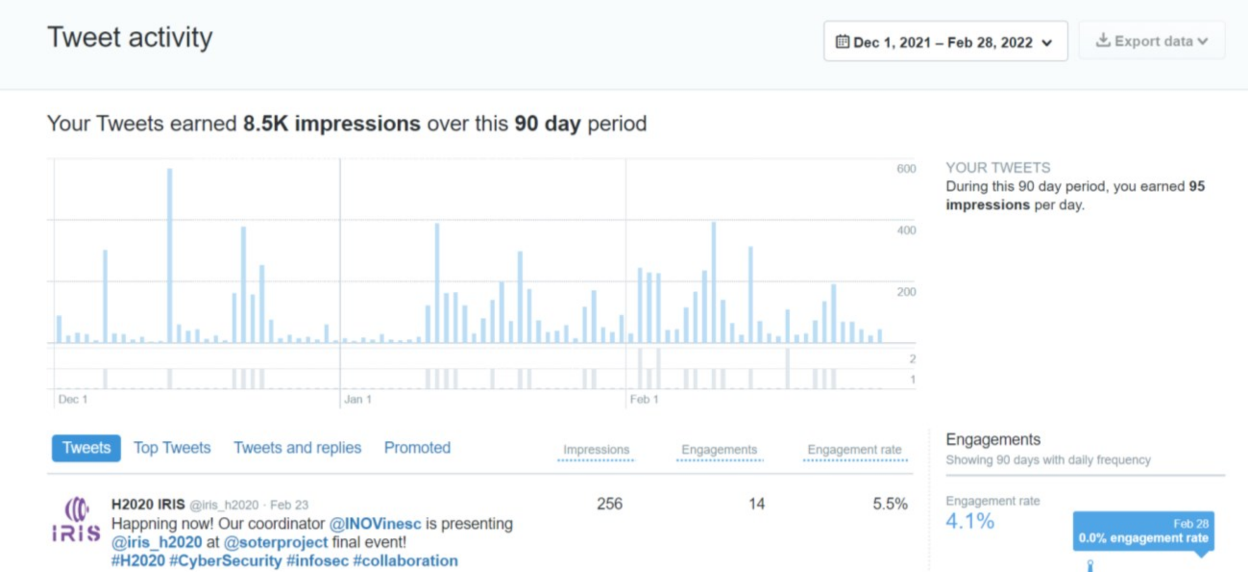
	Impressions	Engagements	Engagement rate
H2020 IRIS @iris_h2020 · Nov 30 Meet @iris_h2020 partners! @CEA_List A key software systems & technology research centre, focusing on 3 areas with disruptive societal and economic implications: embedded systems, interactive systems	223	9	4.0%

Engagements
Showing 91 days with daily frequency

Engagement rate
2.8%

Nov 30
3.7% engagement rate

Figure 2: Impressions & Engagement Rate_ Sept 2021-Nov 2022



Tweet activity

Dec 1, 2021 – Feb 28, 2022

Export data

Your Tweets earned **8.5K impressions** over this **90 day** period

YOUR TWEETS
During this 90 day period, you earned **95 impressions** per day.

Tweets | Top Tweets | Tweets and replies | Promoted

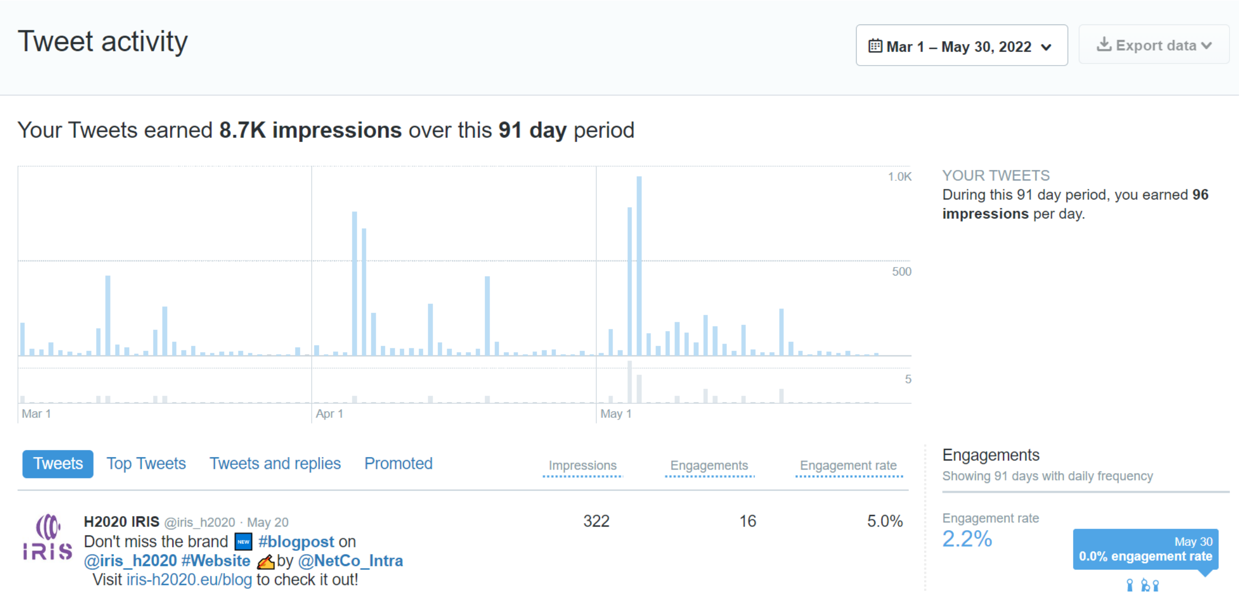
	Impressions	Engagements	Engagement rate
H2020 IRIS @iris_h2020 · Feb 23 Happning now! Our coordinator @INOVinesc is presenting @iris_h2020 at @soterproject final event! #H2020 #CyberSecurity #infosec #collaboration	256	14	5.5%

Engagements
Showing 90 days with daily frequency

Engagement rate
4.1%

Feb 28
0.0% engagement rate

Figure 3: Impressions & Engagement Rate _Dec 2021- Feb 2022



Tweet activity

Mar 1 – May 30, 2022 ⌄ | Export data ⌄

Your Tweets earned **8.7K impressions** over this **91 day** period

YOUR TWEETS
During this 91 day period, you earned **96 impressions** per day.

Tweets | Top Tweets | Tweets and replies | Promoted

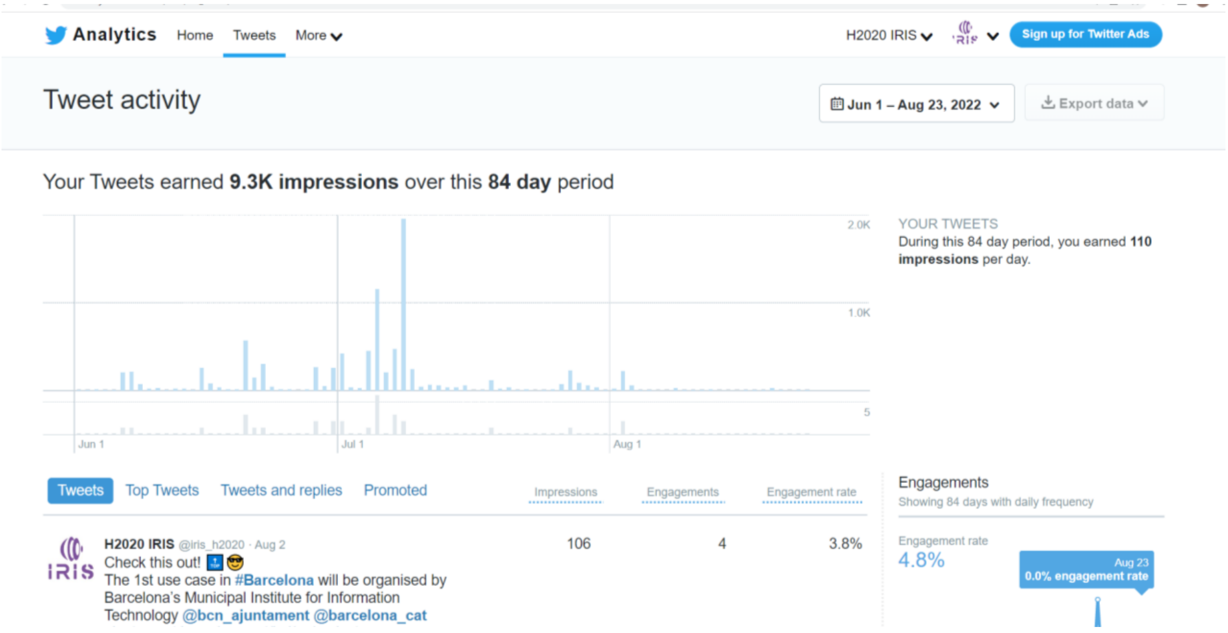
	Impressions	Engagements	Engagement rate
H2020 IRIS @iris_h2020 · May 20 Don't miss the brand 🆕 **#blogpost** on **@iris_h2020 #Website** ✍ by **@NetCo_Intra** Visit iris-h2020.eu/blog to check it out!	322	16	5.0%

Engagements
Showing 91 days with daily frequency

Engagement rate
2.2%

May 30
0.0% engagement rate

Figure 4: Impressions & Engagement Rate _Mar-May 2022



Analytics Home Tweets More ⌄ | H2020 IRIS ⌄ | Sign up for Twitter Ads

Tweet activity

Jun 1 – Aug 23, 2022 ⌄ | Export data ⌄

Your Tweets earned **9.3K impressions** over this **84 day** period

YOUR TWEETS
During this 84 day period, you earned **110 impressions** per day.

Tweets | Top Tweets | Tweets and replies | Promoted

	Impressions	Engagements	Engagement rate
H2020 IRIS @iris_h2020 · Aug 2 Check this out! 🇪🇺 😎 The 1st use case in **#Barcelona** will be organised by Barcelona's Municipal Institute for Information Technology **@bcn_ajuntament @barcelona_cat**	106	4	3.8%

Engagements
Showing 84 days with daily frequency

Engagement rate
4.8%

Aug 23
0.0% engagement rate

Figure 5: Impressions & Engagement Rate _ Jun-Aug 2022

2.5.2 LinkedIn

The IRIS H2020 Project LinkedIn account has 176 followers so far, coming from multiple professional fields and various European locations. Most of our followers come from Research and Academia, IT and Programme Management and the three top countries from which our followers come are Spain, Portugal, and Italy. LinkedIn hosts more than 500 million professional accounts and thus tends to be the most popular social networking platform and the most powerful among professionals. Registered members are able to establish connections with professionals who are in their interest and interact in group discussions.

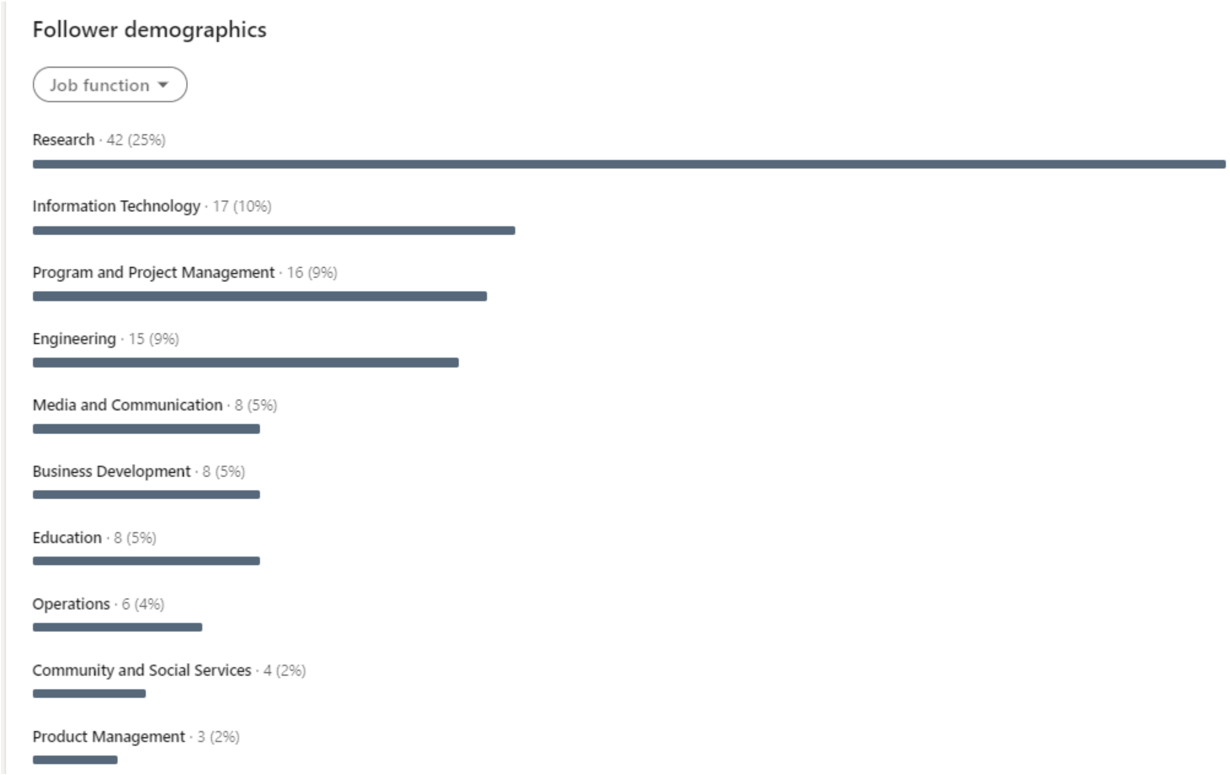
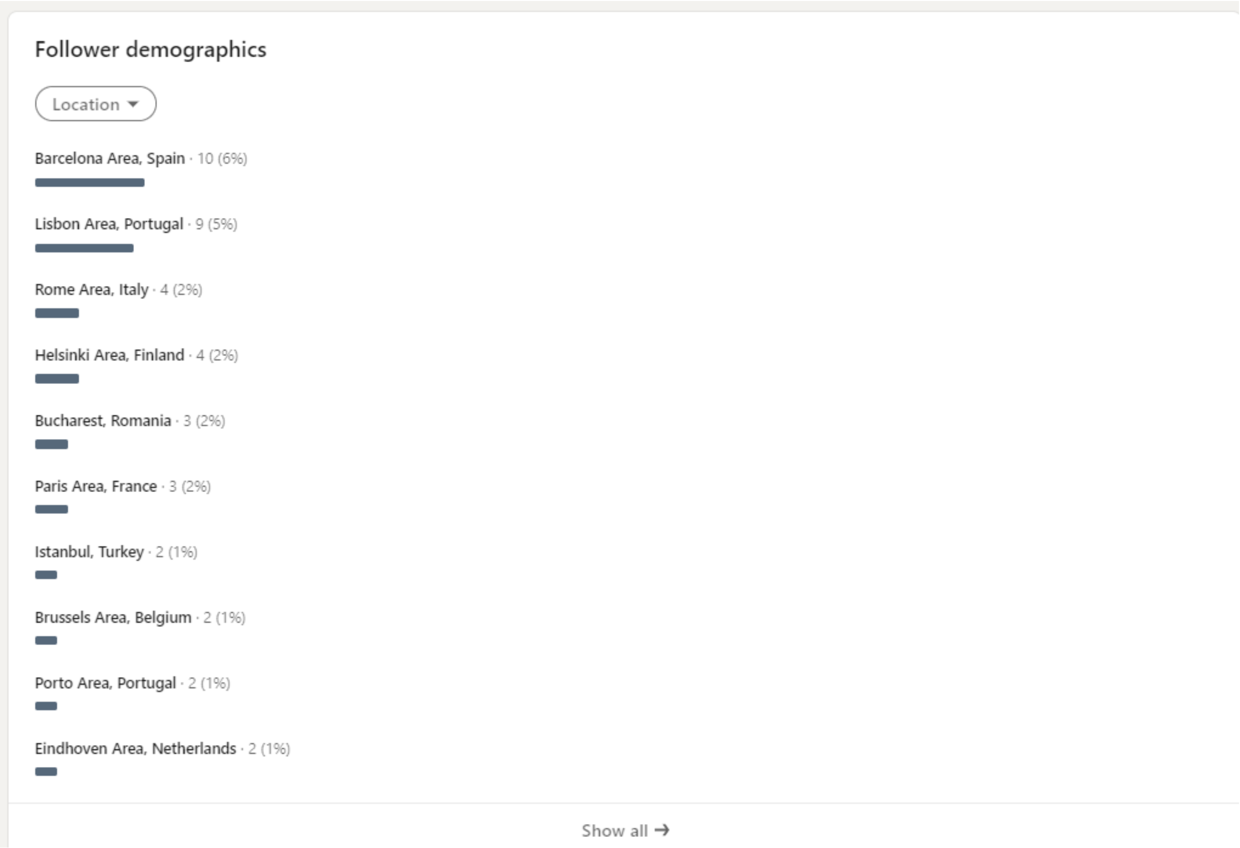


Figure 6: LinkedIn Followers_ Job Functions



Follower demographics

Location ▾

Barcelona Area, Spain · 10 (6%)

Lisbon Area, Portugal · 9 (5%)

Rome Area, Italy · 4 (2%)

Helsinki Area, Finland · 4 (2%)

Bucharest, Romania · 3 (2%)

Paris Area, France · 3 (2%)

Istanbul, Turkey · 2 (1%)

Brussels Area, Belgium · 2 (1%)

Porto Area, Portugal · 2 (1%)

Eindhoven Area, Netherlands · 2 (1%)

Show all →

Figure 7: LinkedIn Followers _ Location

Table 5: Expected and Current Performance regarding IRIS Social Media

Social Media	Expected KPI	Current Status M12
Twitter @iris_h2020	300 followers in total	293 followers
LinkedIn IRIS H2020 Project	100 followers in total	176 followers
YouTube Channel	N/A	one YouTube channel including one video

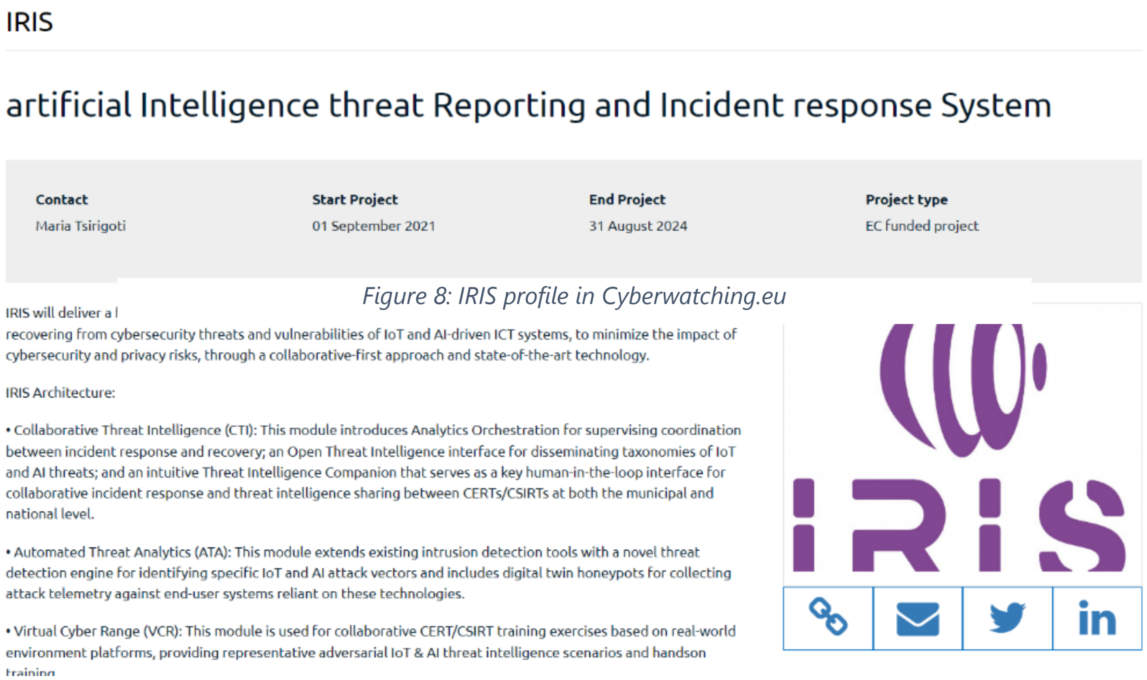
2.6 Online Platforms

2.6.1 Cyberwatching.eu

The Cyberwatching.eu project hub is a complete and unabridged compilation of EU-funded research projects on cybersecurity topics. It was created specifically to facilitate information transfer, communication, and cross-pollination. The IRIS profile can be found here.

2.6.2 Zenodo Community

The IRIS Zenodo Community will eventually include all the public information regarding the project. So far, the dissemination material (brochure, poster, banner, newsletter, brand book, colour palette, logo) has been uploaded, and it is available publicly. Moreover, all the public deliverables, once the EC approves them, will be uploaded along with all the scientific papers that will be submitted by the consortium partners. Therefore, everyone interested in the project or similar projects and research can access and download this material.



IRIS

artificial Intelligence threat Reporting and Incident response System

Contact	Start Project	End Project	Project type
Maria Tsirigoti	01 September 2021	31 August 2024	EC funded project

IRIS will deliver a f

recovering from cybersecurity threats and vulnerabilities of IoT and AI-driven ICT systems, to minimize the impact of cybersecurity and privacy risks, through a collaborative-first approach and state-of-the-art technology.

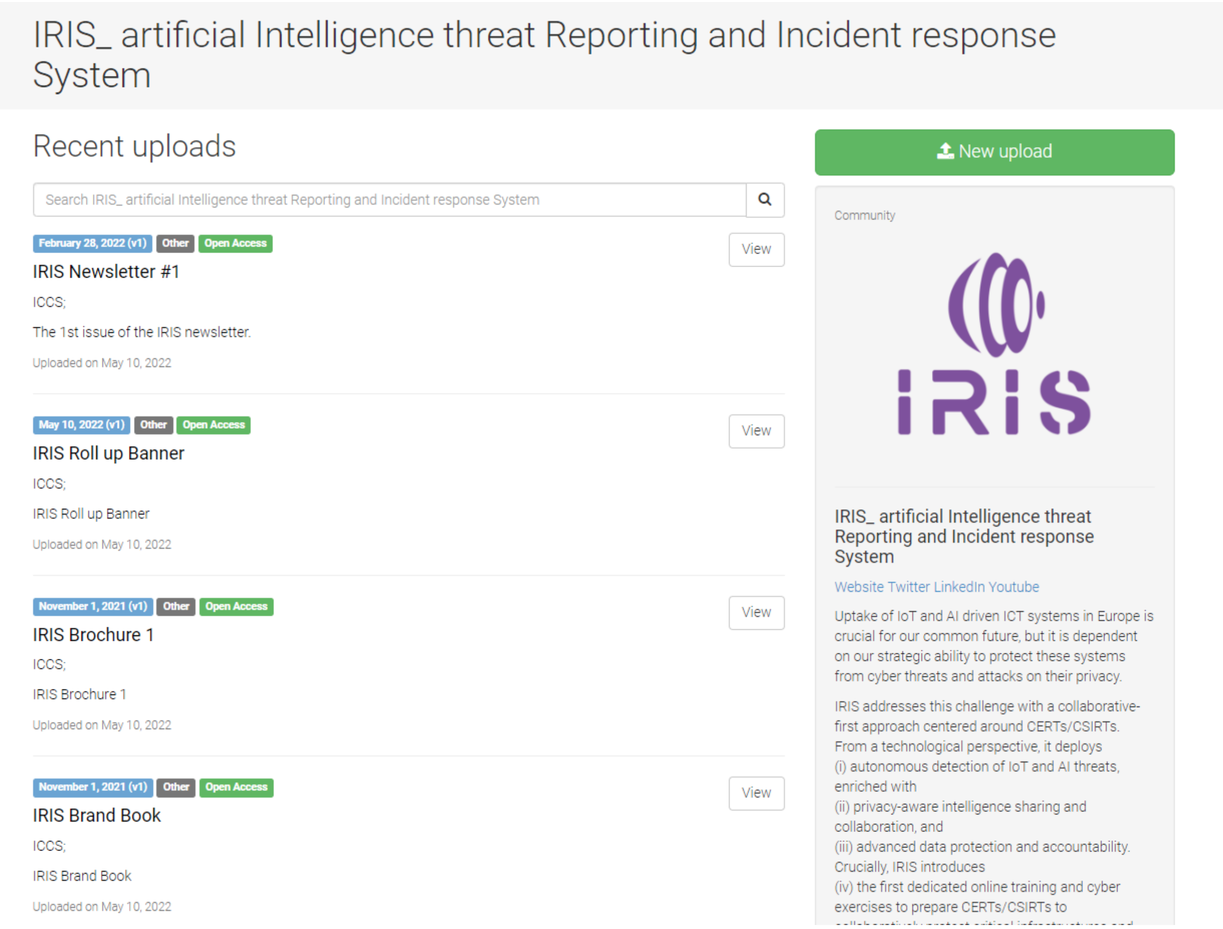
IRIS Architecture:

• Collaborative Threat Intelligence (CTI): This module introduces Analytics Orchestration for supervising coordination between incident response and recovery; an Open Threat Intelligence interface for disseminating taxonomies of IoT and AI threats; and an intuitive Threat Intelligence Companion that serves as a key human-in-the-loop interface for collaborative incident response and threat intelligence sharing between CERTs/CSIRTs at both the municipal and national level.

• Automated Threat Analytics (ATA): This module extends existing intrusion detection tools with a novel threat detection engine for identifying specific IoT and AI attack vectors and includes digital twin honeypots for collecting attack telemetry against end-user systems reliant on these technologies.

• Virtual Cyber Range (VCR): This module is used for collaborative CERT/CSIRT training exercises based on real-world environment platforms, providing representative adversarial IoT & AI threat intelligence scenarios and handson training

Figure 8: IRIS profile in Cyberwatching.eu


New upload
Search IRIS_ artificial Intelligence threat Reporting and Incident response System
View
View
View
View
Community
iRiS

IRIS_ artificial Intelligence threat Reporting and Incident response System

Recent uploads

February 28, 2022 (v1) Other Open Access

IRIS Newsletter #1

ICCS;

The 1st issue of the IRIS newsletter.

Uploaded on May 10, 2022

May 10, 2022 (v1) Other Open Access

IRIS Roll up Banner

ICCS;

IRIS Roll up Banner

Uploaded on May 10, 2022

November 1, 2021 (v1) Other Open Access

IRIS Brochure 1

ICCS;

IRIS Brochure 1

Uploaded on May 10, 2022

November 1, 2021 (v1) Other Open Access

IRIS Brand Book

ICCS;

IRIS Brand Book

Uploaded on May 10, 2022

IRIS_ artificial Intelligence threat Reporting and Incident response System

Website Twitter LinkedIn Youtube

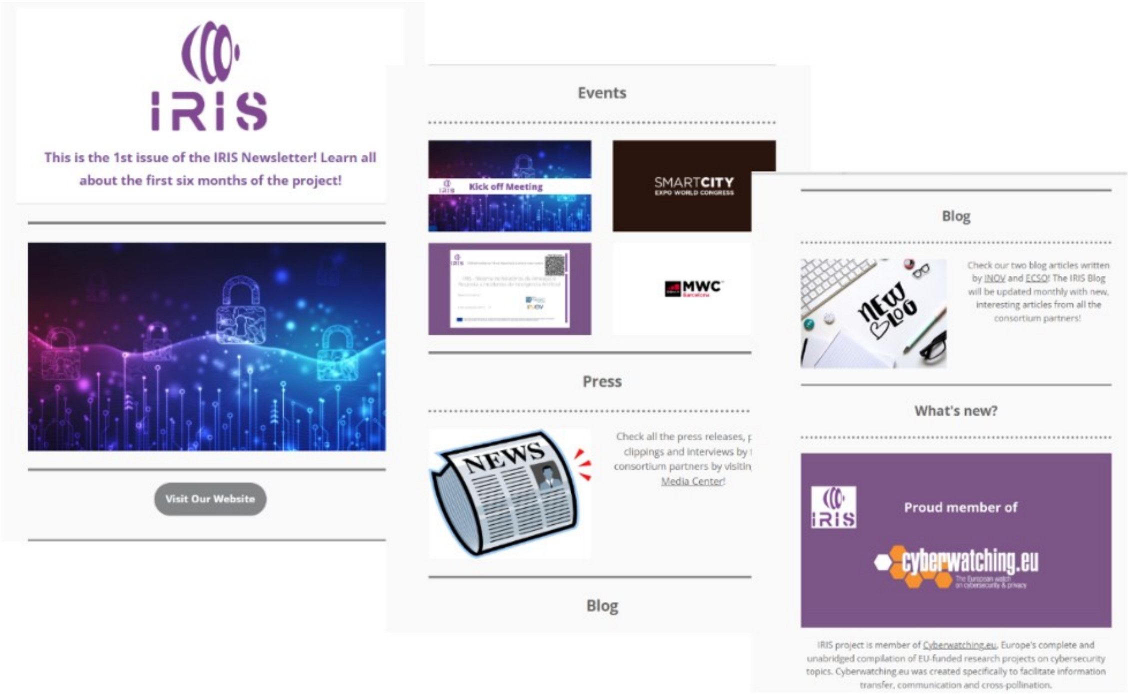
Uptake of IoT and AI driven ICT systems in Europe is crucial for our common future, but it is dependent on our strategic ability to protect these systems from cyber threats and attacks on their privacy.

IRIS addresses this challenge with a collaborative-first approach centered around CERTs/CSIRTs.
From a technological perspective, it deploys
(i) autonomous detection of IoT and AI threats, enriched with
(ii) privacy-aware intelligence sharing and collaboration, and
(iii) advanced data protection and accountability.
Crucially, IRIS introduces
(iv) the first dedicated online training and cyber exercises to prepare CERTs/CSIRTs to

Figure 9: IRIS Zenodo Community

2.7 Newsletters

The IRIS e-newsletters are sent to the dedicated registrants by email and they are published on the IRIS website, the project's social media and its Zenodo community. There is a dedicated section on the website in which people can register for the newsletter. The e-newsletters are being created using Mailchimp which is a marketing automation platform designed and developed for businesses using email to reach out to their target markets. So far, we have published two newsletters. The first included an overview of the project, the events, and activities of the first six months of the project, blog articles written by the consortium partners and information on our H2020 synergies. The second issue of the IRIS newsletter was published in M11 and included information about the IRIS Launch Event held online in July 2022, all the events IRIS partners participated in, news from other H2020 projects, and IRIS Zenodo Community.



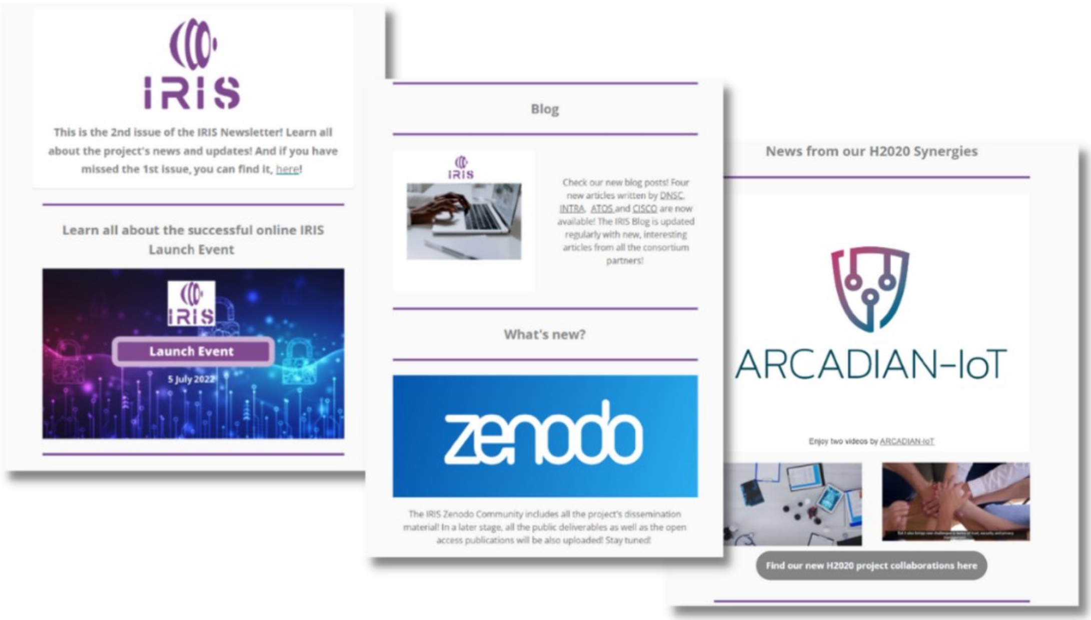
This is the 1st issue of the IRIS Newsletter! Learn all about the first six months of the project!

Check all the press releases, p
clippings and interviews by t
consortium partners by visitin
Media Center!

Check our two blog articles written by INOV and ECSO! The IRIS Blog will be updated monthly with new, interesting articles from all the consortium partners!

IRIS project is member of Cyberwatching.eu, Europe's complete and unabridged compilation of EU-funded research projects on cybersecurity topics. Cyberwatching.eu was created specifically to facilitate information transfer, communication and cross-pollination.

Figure 10: IRIS 1st newsletter



This is the 2nd issue of the IRIS Newsletter! Learn all about the project's news and updates! And if you have missed the 1st issue, you can find it, here!

Learn all about the successful online IRIS Launch Event

Blog

Check our new blog posts! Four new articles written by DNSC, INTRA, ATOS and CISCO are now available! The IRIS Blog is updated regularly with new, interesting articles from all the consortium partners!

What's new?

The IRIS Zenodo Community includes all the project's dissemination material! In a later stage, all the public deliverables as well as the open access publications will be also uploaded! Stay tuned!

News from our H2020 Synergies

Enjoy two videos by ARCADIAN-IoT

Find our new H2020 project collaborations here

Figure 11: IRIS 2nd newsletter

Table 6: Expected and Current Performance regarding IRIS Newsletters

Activity	KPI M36	Current Status
Newsletter • 1st issue M6 • 2nd issue M11	6	2 published

2.8 Press Releases & Activities

The IRIS partners use their press contacts to communicate the developments of the project through press articles and press releases and will be responsible for translations and regional adaptations. Partners' efforts will also focus on publishing major IRIS achievements through channels and means offered by the European Commission (i.e., the Horizon Magazine, research*EU results magazine, Futuris Magazine etc.). All the press activities and press releases are available on the IRIS website.

Table 7: Expected and Current Performance regarding IRIS Press Releases and Activities

Activity	Expected KPI M36	Current Status
Press releases • **1st IRIS Press Release Kick off Meeting (**4 republications in partners' websites **)** • Ζητήματα κυβερνοασφάλειας στις έξυπνες πόλεις του αύριο θα αντιμετωπίσει το IRIS (**translation**: *The IRIS project will deal with the cyber security issues of the smart cities)* • Cisco and Barcelona City Council will test IRIS cyber security platform to protect EU cities and communities	6	3 (+4 republications)
Press Clippings • Amna.gr • Metaforesspress.gr • Ecopress • ICT Plus • ANEA • Europa Press • Gente Digital • El periódico • Silicon • Diario Abierto • Computing	N/A	11
Media Appearances • Radio interview in Parapolitika 90,1 FM (ICCS) • Interview in El Espanol magazine (CISCO) • Media article in cit.upc.edu (UPC)	3	3
Articles in partners websites	N/A	4

• cit.upc.edu/en/ ⇨ https://cit.upc.edu/es/portfolio-item/iris-una-plataforma-para-evaluar-detectar-y-responder-a-las-vulnerabilidades-y-amenazas-en-las-redes-tic/ • www.dnsc.ro ⇨ https://dnsc.ro/pagini/proiect-iris • www.barcelona.cat ⇨ https://ajuntament.barcelona.cat/imi/ca/projectes/artificial-intelligence-threat-reporting-and-incident-response-system-iris • i-sense.iccs.gr ⇨ https://i-sense.iccs.gr/news/iris-a-new-project-for-i-sense-iccs-with-an-impact-on-cybersecurity/		

2.9 Events

IRIS participated in a number of event and conference in the first 12 months of the project. Consortium representatives have networked and engaged with relevant stakeholders, as well as presented some of the core objectives of the project. Below is a list of these events:

Table 8: IRIS participation in Events

Event	Activity	Expected KPI M36	Current Status
• Fuzzing@NDSS 2022 / **24-25 April 2022** • 2nd ECSI Workshop /**27-29 April 2022** • IoT Week 2022 **21 June 2022**	**Oral Presentations in conferences**	**18**	**3** (2 paper presentations, 1 keynote speech)
• Smart City Expo /**8 Nov 2022** • Portuguese National CSIRT Network General meeting /**12 Dec 2021** • SOTER Final Event /**23 Feb 2022** • MWC 2022 /**28 Feb-3 Mar 2022**	**Project presentations**	**7 project presentations** ➢ 5 in communications events ➢ 2 in technical events	**8** ➢ 6 in communications events ➢ 2 in technical events

• Privacy Symposium 2022 /**5-7 April 2022** • Clustering Webinar on Security, Privacy and Data Protection /**12 May 2022** • AI Roundtable /**16 June 2022** • Phoenix Final Event /**7 June 2022**			

2.10 Publications

Event	Status	Activity	Expected KPI M36	Current Status
Fine-Grained Coverage-Based Fuzzing[3] / Fuzzing@NDSS 2022	Published	Scientific papers in journals/conference proceedings	**3**	**2**
IRIS Advanced Threat Intelligence Orchestrator- A way to manage cybersecurity challenges of IoT ecosystems in Smart Cities[4] / IoT Week 2022	Presented			

2.11 H2020 Synergies

The IRIS project has started building strong synergies with other H2020 projects. So far, we have contacted thirteen (13) H2020 projects and most of them can be seen on our dedicated webpage. All the activities performed with the aim to develop the collaboration between IRIS and other H2020 projects, are presented below:

- ✓ **Communication Task Force (CTF)**: IRIS is participating in the Communication Task Force which consists of a group of H2020 projects, namely the ARCADIAN-IoT project, ELECTRON project, ERATOSTHENES project, IDUNN project, SECANT project, SPATIAL project, TRUST aWARE project, CitySCAPE project, SENTINEL project. The CTF has monthly meetings and a common mailing list through which the participants are kept informed of

[3] Authors: Bernard Nongpoh, Marwan Nour, Michaël Marcozzi, Sébastien Bardin (CEA)

[4] Authors: Vasiliki-Georgia Bilali, Dimitrios Kosyvas, Thodoris Theodoropoulos, Eleftherios Ouzounoglou, Lazaros Karagiannidis, Angelos Amditis (ICCS)

the projects' communication activities (participation in events, organisation of workshops, publication of newsletters etc.).

- ✓ **Clustering Webinar on Security, Privacy and Data Protection:** IRIS participated in the joint clustering webinar with projects funded under the H2020-SU-DS02 and H2020-SU-DS03 topics to explore possible collaborations between EU funded projects relevant to Cybersecurity, Personal data protection and GDPR compliance topics. The Webinar was held online on the 12th of May 2022 with representatives from ten EU projects (SENTINEL, PALANTIR, TRAPEZE, PUZZLE, CyberKit4SME, ARCADIAN-IoT, IRIS, ERATOSTHENES, IDUNN, SECANT) coming together for experience exchange, enhancement of technical know-how and identification of common challenges that can be addressed collaboratively.
- ✓ **SOTER Project Final Event:** Our project coordinator INOV presented the IRIS project and then participated in the Q&As section.
- ✓ **Project to Policy Seminar**: IRIS project participated in the Project to Policy Seminar, organised by the European Research Executive Agency (REA) and DG HOME and had the chance to meet and discuss not only with the representatives of the projects with which we had already come in touch but also and more importantly with other projects with which, we now start our collaboration namely the CyberSEAS project, SOTERIA project, Testable project and Phoenix Project.
- ✓ **PHOENIX Project Final Event:** Our partner INTRA presented the IRIS project and then participated in panel discussion that followed.

2.12 Community building and liaison with relevant stakeholders

The goal of T8.5 is to create links with stakeholders from Industry, SMEs, CERTs/CSIRTs and policy makers at the EU and national level. Liaison activities within the academic domain and cooperation with related R&D Initiatives and other projects is also an important part of community building. Additionally, as part of this task, operational links between IRIS and numerous cybersecurity providers will be created to exchange information, training tools and materials.

As it greatly improves the activities conducted under WP8, such as dissemination, exploitation, and communication, the work of this Task is directly tied to all tasks and activity under WP8.

Furthermore, T8.5 is reliant on the technical developments of the project and the technical work packages WP2, WP3, WP4, WP5, and WP6. Concrete operational links with the stakeholders will be sought at the later stages of the IRIS Project once the technical deliverables are finished.

List of Relevant Stakeholders

The first step during the task was to categorize relevant stakeholders. The identified categories are as follows:

- CERT/CSIRT
- Public Administrations (National/EU)
- SMEs and Cybersecurity Providers
- Universities and other R&D initiatives
- Relevant EU project consortia

- Policy/Standardisation experts
- Relevant Event organizers

The second step was to create a list of relevant stakeholders. A template was created and sent to the project partners. Partners were asked to identify organisations and points of contact for each of the above categories. The "List of Relevant Stakeholders" was uploaded to the IRIS repository and new stakeholders can be added to the list over the lifetime of the IRIS Project. One sheet in the list consists of the stakeholders identified by the partners and the other one is a list of stakeholders from ECSO's own community that ECSO can help to establish contact with.

After identification of all potential links and with the establishment of the initial database, the next step will be for IRIS to initiate contact with them either as a consortium via specific partners or through each individual partner. At this stage, stakeholders are contacted mainly as part of the dissemination activities. All the identified stakeholders were invited to the IRIS Launch Event and will be invited to the Expert Group as identified per T8.4 (if applicable) and to the Workshops organised as part of the T8.3.

2.12.1 IRIS Launch Event

The IRIS Launch Event was organised in the presence of the European Institutions and key stakeholders to give high visibility to the project, raise awareness on the project priorities and start engaging with key experts (to also form the expert group for T8.4).

The Event was organised remotely on 5th of July and was a success qualitatively and quantitatively. Part I revolved around the presentation of the IRIS Project. INOV gave an overview of the project which was followed by a presentation from Atos on the IRIS Architecture and 3 Pilot Use Cases. The overarching theme of Part II of the event was Threat Information Sharing. As a prelude to the panel discussion, INTRA presented IRIS Enhanced MeliCERTes 2 Ecosystem. A high-level panel then took place on the topic of 'Threat intelligence and information sharing: technical and policy perspectives' which was organised and moderated by ECSO. External stakeholders were successfully engaged as the panel speakers represented stakeholders from multiple categories – EU Institutions/Agencies (ENISA), Industry representative (Erium), CERT (CERT Catalonia) and a project coordinator of a closely related EU project (Empowering EU ISACs). There was great interest and turnout for the event with 121 people registered and 72 in attendance. Positive feedback was received both from participants and the EC project officer. Registrants will be invited to participate in other activities of the IRIS Project at later stages (when applicable).

2.13 Clustering Activities

Clustering activities in IRIS take essentially two forms.

- **Stakeholders and Industrial Workshops (SIW).** The goal of these actions is to present the most mature results to industrial stakeholders along with methodological insights. Cross-sector practitioners, policy makers, investors, and researchers will be invited to those workshops to ensure a balanced attendance and fruitful discussions. Three Stakeholders and Industrial Workshops (SIW) will be organised by ICCS in M16, M26, and M34 where IRIS partners will present the most mature results to industrial stakeholders along with methodological insights.

- **Liaising with the SU-ICT-03 pilots.** The goal of these actions is to perform clustering actions with the cybersecurity community at large, through the lever of the SU-ICT-03 pilots. SPARTA is a natural target here, as several members of IRIS are deeply implicated into it. The IRIS project was represented at the SPARTA workshop held on June 14-15 in Paris (Campus Cyber Defense). The session features three European projects presentations (STARLIGHT, IRIS, and REWIRE) followed by a panel discussion among the speakers and the audience on the topic of aligning cybersecurity efforts to strengthen the European strategic autonomy. The topics range from values and cybersecurity, to the contribution of these projects to EU-level roadmaps, the importance of community building, and the link between cybersecurity certification and strategic autonomy.

3 DISSEMINATION PROCEDURES

In order to ensure high-quality publications, presentations, and other communication material, avoid overlaps and possible disclosure of restricted or confidential information as well as monitor and record the project's communication and dissemination activities, the IRIS Dissemination Procedures have been created and should be followed by all partners.

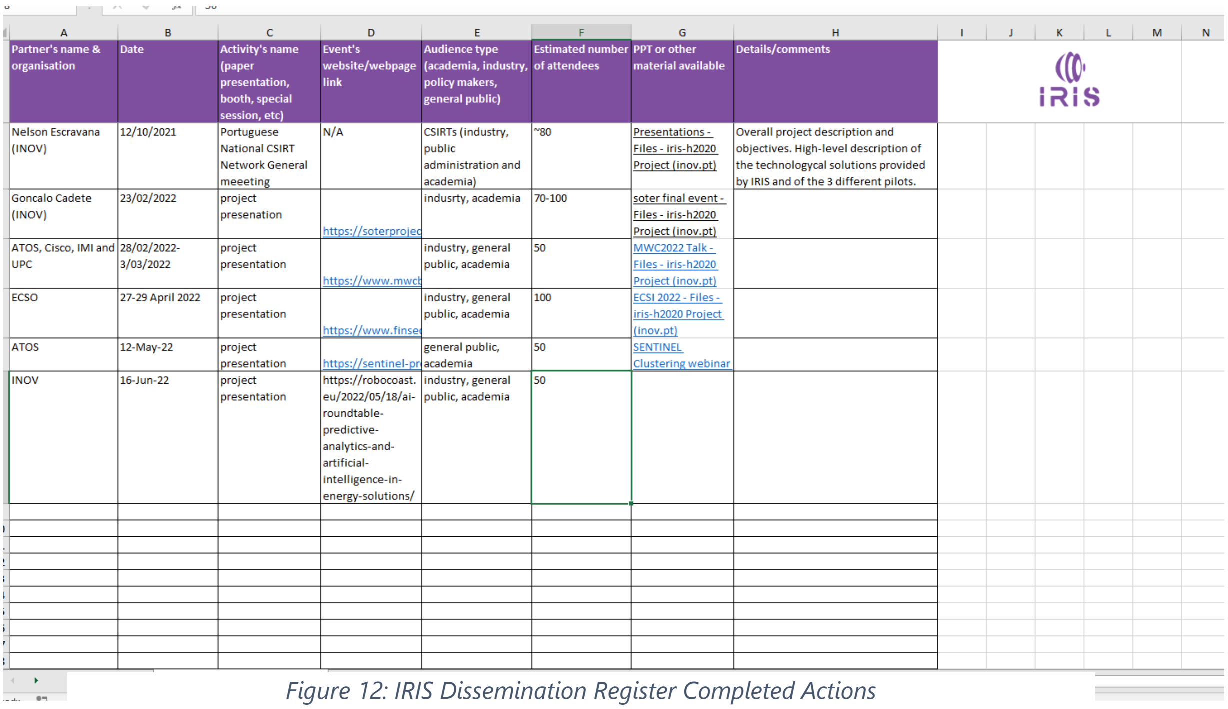
The step-by-step procedure was presented to the Consortium and is available for all in the IRIS repository and is also presented in the Appendix 9 of the deliverable D8.2 "Plans for Dissemination, Communication and Exploitation"', submitted in M6.

3.1 EU Acknowledgement

The EU Acknowledgement and the EU flag should be included in all dissemination and communication activities so that it is always clear that the project is funded by the EU. The texts that should be included in all dissemination and communication activities are presented in detail in chapter 6.4 of the deliverable D8.2 "'Plans for Dissemination, Communication and Exploitation", submitted in M6.

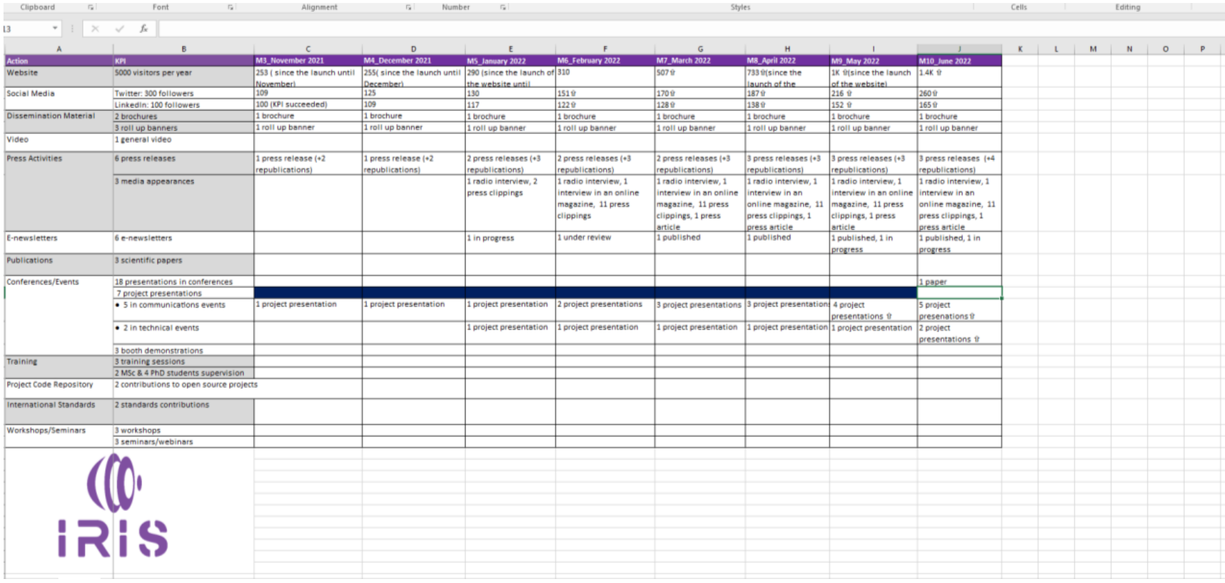
3.2 Activities' Monitoring and Recording

All dissemination activities are and will be monitored and recorded during the project execution and for this purpose, an MS Excel spreadsheet has been created. According to the dissemination procedures, the IRIS partners are obliged to fill in the excel file with all the required information each time they perform a dissemination activity. In addition to this, ICCS sends a monthly excel file presenting the progress performed regarding the dissemination and communication KPIs in order to keep the whole consortium updated on the work performed and also deal with any issue that may occur. These files are also available on the IRIS repository.



Partner's name & organisation	Date	Activity's name (paper presentation, booth, special session, etc)	Event's website/webpage link	Audience type (academia, industry, policy makers, general public)	Estimated number of attendees	PPT or other material available	Details/comments
Nelson Escravana (INOV)	12/10/2021	Portuguese National CSIRT Network General meeeting	N/A	CSIRTs (industry, public administration and academia)	~80	Presentations - Files - iris-h2020 Project (inov.pt)	Overall project description and objectives. High-level description of the technologycal solutions provided by IRIS and of the 3 different pilots.
Goncalo Cadete (INOV)	23/02/2022	project presenation	https://soterprojec	indusrty, academia	70-100	soter final event - Files - iris-h2020 Project (inov.pt)	
ATOS, Cisco, IMI and UPC	28/02/2022-3/03/2022	project presentation	https://www.mwcb	industry, general public, academia	50	MWC2022 Talk - Files - iris-h2020 Project (inov.pt)	
ECSO	27-29 April 2022	project presentation	https://www.finsec	industry, general public, academia	100	ECSI 2022 - Files - iris-h2020 Project (inov.pt)	
ATOS	12-May-22	project presentation	https://sentinel-pr	general public, academia	50	SENTINEL Clustering webinar	
INOV	16-Jun-22	project presentation	https://robocoast.eu/2022/05/18/ai-roundtable-predictive-analytics-and-artificial-intelligence-in-energy-solutions/	industry, general public, academia	50		

Figure 12: IRIS Dissemination Register Completed Actions



Action	KPI	M3_November 2021	M4_December 2021	M5_January 2022	M6_February 2022	M7_March 2022	M8_April 2022	M9_May 2022	M10_June 2022
Website	5000 visitors per year	253 (since the launch until November)	255(since the launch until December)	290 (since the launch of the website until	310	507 ⇧	733 ⇧(since the launch of the	1K ⇧(since the launch of the website)	1.4K ⇧
Social Media	Twitter: 300 followers	109	125	130	151 ⇧	170 ⇧	187 ⇧	216 ⇧	260 ⇧
	LinkedIn: 100 followers	100 (KPI succeeded)	109	117	122 ⇧	128 ⇧	138 ⇧	152 ⇧	165 ⇧
Dissemination Material	2 brochures	1 brochure	1 brochure	1 brochure	1 brochure	1 brochure	1 brochure	1 brochure	1 brochure
	3 roll up banners	1 roll up banner	1 roll up banner	1 roll up banner	1 roll up banner	1 roll up banner	1 roll up banner	1 roll up banner	1 roll up banner
Video	1 general video								
Press Activities	6 press releases	1 press release (+2 republications)	1 press release (+2 republications)	2 press releases (+3 republications)	2 press releases (+3 republications)	2 press releases (+3 republications)	3 press releases (+3 republications)	3 press releases (+3 republications)	3 press releases (+4 republications)
	3 media appearances			1 radio interview, 2 press clippings	1 radio interview, 1 interview in an online magazine, 11 press clippings	1 radio interview, 1 interview in an online magazine, 11 press clippings, 1 press article	1 radio interview, 1 interview in an online magazine, 11 press clippings, 1 press article	1 radio interview, 1 interview in an online magazine, 11 press clippings, 1 press article	1 radio interview, 1 interview in an online magazine, 11 press clippings, 1 press article
E-newsletters	6 e-newsletters			1 in progress	1 under review	1 published	1 published	1 published, 1 in progress	1 published, 1 in progress
Publications	3 scientific papers								
Conferences/Events	18 presentations in conferences								1 paper
	7 project presentations								
	• 5 in communications events	1 project presentation	1 project presentation	1 project presentation	2 project presentations	3 project presentations	3 project presentation	4 project presentations ⇧	5 project presenations ⇧
	• 2 in technical events			1 project presentation	1 project presentation	1 project presentation	1 project presentation	1 project presentation	2 project presentations ⇧
	3 booth demonstrations								
Training	3 training sessions								
	2 MSc & 4 PhD students supervision								
Project Code Repository	2 contributions to open source projects								
International Standards	2 standards contributions								
Workshops/Seminars	3 workshops								
	3 seminars/webinars								

Figure 13: Monthly Excel File regarding the KPIs Performance

4 FUTURE STEPS ON DISSEMINATION AND COMMUNICATION (M12-M24)

All the dissemination and communication activities that will be conducted in the second phase of the project will focus on the IRIS key audiences, as these have been defined in an earlier stage of the project. These activities will concentrate 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 a focal point for communicating our messages and sharing the project's results. The website will be regularly updated with the project's news and updates as it has been so far. A section where the public deliverables can be viewed and downloaded once they have been approved by the European Commission will soon be added. Regarding the website visitors' number, a more major effort will be made by introducing the IRIS podcast, enhancing the IRIS Blog, and promoting the website through the social media in order to achieve the KPI number.

Social Media: The project's social media accounts will keep being active and will give emphasis to the communication of the project's results. We intend to engage even more followers and exceed by far the Twitter followers expected KPI, a goal that has been achieved in LinkedIn account.

Online Platforms: The IRIS results will be upload 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 the publication of at least one press release.

Events: Consortium partners will focus more 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.

H2020 Synergies: The established relationships between IRIS and the H2020 projects, mentioned in section 2.10 will move a step further by organizing at least another joint webinar. Of course, the continuous communication with the other projects through the Communication Task Force monthly calls will remain.

IRIS Podcast Series: IRIS will launch a podcast series in which we will invite other H2020 projects, professionals from the cybersecurity sector, researchers etc in order to communicate the project's results, raise further awareness about the project and its consortium and also assist the collaboration between IRIS and other H2020 projects.

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.

5 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○

Table 9: Dissemination and Communication KPIs

Action	Expected KPI	Current Status M12
Website	5000 visitors per year	1800 visitors ○
Social media	Twitter: 300 followers in total LinkedIn: 100 followers in total	293 followers○ 176 followers ○
Dissemination material	2 brochures 3 roll up banners	1 brochure ○ 1 roll up banner○
Video	1 general video	○
Press Activities	6 press releases 3 media appearances	3 press releases ○ 3 media appearances ○
E-newsletters	6 e-newsletters	2 published ○
Journal Publications/ Conferences Proceedings	3 scientific papers	2 papers in conference proceedings ○
Conferences/Events	• 18 oral presentations in conferences • 7 project presentations ➢ 5 in communications events ➢ 2 in technical events • 3 booth demonstrations	• 3 oral presentations ○ • 8 project presentations ○ ➢ 6 in communication events ➢ 2 in technical events • No booth demonstrations ○
Training	• 3 training sessions for students	○

	• 2 MSc & 4 PhD students supervision	○
Project code repository	2 contributions to open source projects	○
International Standards	2 standards contributions	○
Workshops/Webinars	3 workshops 3 seminars/webinars	1 online event ○

6 POLICY AND STANDARDISATION ACTIVITIES UP TO M12 AND FUTURE STEPS

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. This section is organised 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[5] (July 2020) and then developed in the EU Cybersecurity Strategy for the Digital Decade[6] (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 Centers (SOCs) capable of detecting the signs of a cyber-attack, and platform for sharing CTI between the public and private sector. Regarding the “operational capacity for prevention, deterrence and response”, the Commission intends to create a new Joint Cyber Unit to strengthen collaboration between national authorities, Europol, the European Cyber Security Agency (ENISA) and the civil, diplomatic and defence community. To increase collaboration between the public and private sector by building bridges between research and the market, the Commission is currently in the process of creating a cyber-security competence center (ECCC) based in Bucharest, Romania. This center will coordinate collaboration between a network of national competence centers (NCCs) 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.

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

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

[6] 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.

in the Union (NIS Directive revisited or 'NIS 2') and the Critical Entities Resilience Directive (CER) are essential proposals to strengthen the resilience of critical infrastructures such as smart cities.

The NIS2 Directive was proposed by the European 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. Once approved by the European Parliament, the Member States will have 21 months from the entry into force of the directive to transpose its provisions into their national laws.

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, as was the case in 2016 with the Personal Data Protection Regulation (GDPR). As with the GDPR, the CRA will be an opportunity for European companies to differentiate themselves on the international market and sell products certified with the most stringent cybersecurity requirements and, consequently, accepted not only in Europe, but worldwide. 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 organizational 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. Another regulation that could be potentially relevant for the IRIS solution is the eIDAS. The EC has recently proposed a new regulation on digital identity that could also have a potential impact on IoT, for instance potentially linking the devices with legal persons.

The IRIS platform will use cloud services. As far as the cloud sector is concerned, ENISA is preparing a cybersecurity certification scheme on cloud services (EUCS) under the Cybersecurity Act. The EU cybersecurity agency envisages a voluntary three-level certification system.

6.2 Standardisation landscape

In general, standards play a key role in ensuring inter-dependency and interoperability of technical solutions across different geographical regions and communities. As such, the standardisation process is essential to achieve effective cooperation in cross-border, cross-community, and cross-sector environments. The IRIS project and the platform are no exception to ensure easy integration 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. The remainder of this section discusses the first two points that will be used later to define a common participation strategy.

The preliminary analysis of the envisioned solutions for IRIS platform described in D2.2 and D2.5 highlight the potential relevance of the following standards. 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 serialisation 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 standardized 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 standardized 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.

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.

Other relevant standards for the IRIS solution are the ISO/IEC 27001:2013 on Information security management and the ISO/IEC 27002:2022 on Information security, cybersecurity, and privacy protection - Information security controls – will be relevant for the technical WPs to consider best practices to secure any kind of digital information and to collect and analyse information relating to information security threats.

7 EXPLOITATION ACTIVITIES UP TO M12 AND FUTURE STEPS

This section summarises the exploitation activities that were executed in the context of WP8 "Dissemination, Communication and Exploitation of Results" during the first year of the IRIS project. In particular, it presents the IRIS exploitation strategy to promote the achievements coming out of the IRIS project. This strategy is being updated throughout the project lifetime to keep track with the associated activities, including any modification in the exploitation plans, the identification of new opportunities, or the emergence of new needs related to the exploitable assets. The remainder of this section is organised as follows: Section 7.1 reports on the IRIS exploitation strategy that is being adopted in the context of Task 8.2. Section 7.2 elaborates on the project's Key Exploitable Results (KERs), their exploitation types and devises a framework for the joint exploitation of the outcomes of the IRIS project. Finally, Section 7.3 presents the updated exploitation plans of the IRIS partners.

7.1 Exploitation Strategy

According to the DoA, the IRIS Consortium will work together to design and develop a comprehensive and market-oriented solution for automated threat analytics, threat intelligence sharing, risk-based response & self-recovery as well as for hands-on cybersecurity training. To facilitate the proper uptake of the project results by relevant stakeholders, an exploitation strategy should be in place identifying and describing the exploitable outcomes, the potential users (target groups), the activities, instruments, and channels via which the project results will be exploited and protected.

The overall aim of the **IRIS Exploitation Strategy** is to spread the outputs and results in line with the needs of the relevant stakeholders and reach out the proper audience so as to enable them to benefit from the activities and results of the project. The exploitation strategy of the IRIS project will define a tailored set of instruments and mechanisms for effective and sustainable exploitation of the project results ensuring maximum impact of the project during its lifetime and after its completion.

The IRIS exploitation strategy compliments the dissemination and communication plan defined in D8.2 and further updated in this deliverable, and together will guide, align, coordinate, and support communication to third parties, and will ensure smooth information flow to the project's external stakeholders. The exploitation strategy proposes actions on how to create added value of the manifold activities and project results during and after its completion. In addition, it contributes to the European Union's external policies and paves the way for scientific and economic exploitation of the project's results.

Overall, the IRIS exploitation strategy builds upon two distinct levels of execution: the **consortium level**, and the **partner level**. On the consortium level, the main duty will be to coordinate the partners in their various exploitation activities and promote these activities in a unified manner among the relevant audiences. The consortium will be responsible for dividing the tasks among the partners according to their areas of expertise, comparative strengths, and respective networks. On the partner level, the exploitation strategy for delivering the IRIS business plan for the exploitation of the results is tailored to two directions: the **individual exploitation**, and the **joint exploitation**.

The joint commercialisation of the IRIS platform would involve all project partners with different roles. The direct exploitation route of the project will be mainly through the **industrial partners** by incorporating the IRIS-enhanced developed components into their products and services portfolios. IRIS's industrial partners have extensive expertise in launching products and services targeting wide markets and/or specific groups. The **non-industrial partners** will exploit the technological achievements of the project through technology, know-how and patents licensing as well as through the project's wide network of cybersecurity stakeholders. Each member of the consortium has already devised their initial exploitation plans for the foreseen results of the project, while the joint exploitation activities will be co-managed by the involved parties as the project matures.

To ensure the correct exploitation of the project results, the IRIS exploitation strategy encompasses several activities to be considered by the Consortium partners. These activities will aim to transform research results and outcomes of the IRIS project into empirical knowledge and potential market products and services, which may be followed by the commercialisation of several of the IRIS's components. These activities include the following:

- Identification of the key exploitable results of the project.
- Identification of all relevant stakeholders in the exploitation value chain.
- Derivation of exploitation plans per partner.
- Reflection upon steps to protect and exploit the project results.
- Evolvement of the plans to become more precise during the project lifetime (including a risk analysis related to the exploitation of the results).

To illustrate the activities, a roadmap of the exploitation strategy has been designed and is depicted in the following figure.

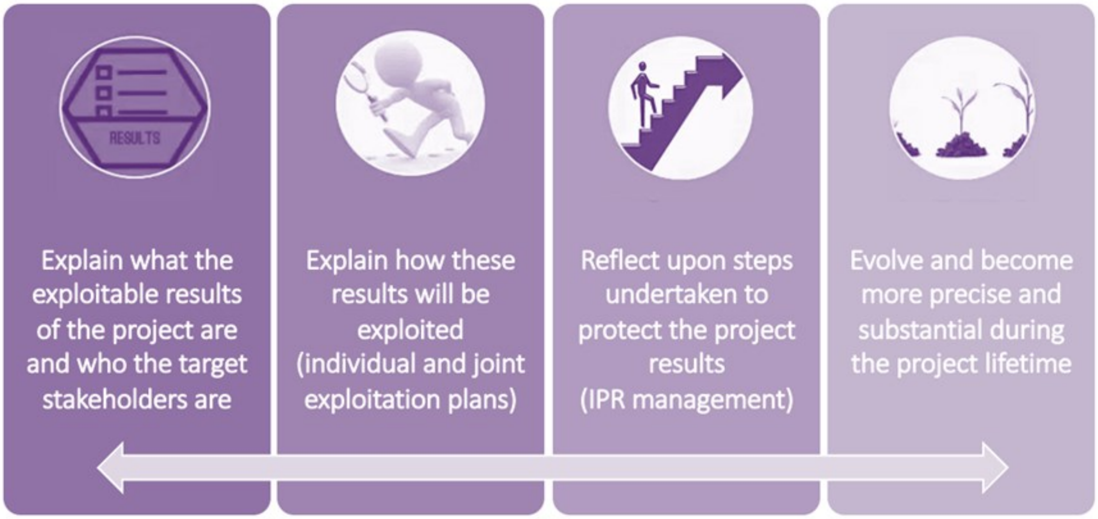

RESULTS
Explain what the exploitable results of the project are and who the target stakeholders are
Explain how these results will be exploited (individual and joint exploitation plans)
Reflect upon steps undertaken to protect the project results (IPR management)
Evolve and become more precise and substantial during the project lifetime

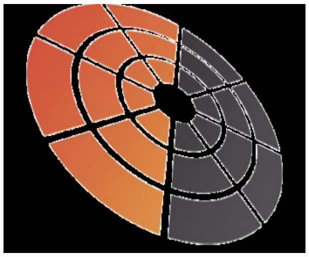
Figure 14: The stages of the exploitation strategy for the IRIS project

In each stage of this roadmap, certain activities take place and the required input for each stage is associated with deliverables coming not only from WP8 but from all work packages of the project.

EC services to support exploitation in H2020 projects

During its lifetime, IRIS will try to make active use of the most common facility services supporting dissemination and exploitation in EU-funded R&I projects. These services are free of any charge and are available on demand. The most relevant services identified by the IRIS consortium are the following two:

Innovation Radar[7]



"The Innovation Radar is a European Commission initiative to identify high potential innovations and innovators in EU-funded research and innovation projects. Our goal is to allow every citizen, public official, professional and businessperson to discover the outputs of EU innovation funding and give them a chance to seek out innovators."

In view of the IRIS project, the Innovation Radar can be used:

1. To understand how real innovations emerge from EU-funded projects.
2. To get an idea where the innovators are located and learn about their features.
3. To search for innovations and partners related to the IRIS project.

Horizon Results Booster[8]

"Horizon Results Booster is a new package of specialised services to maximise the impact of R&I public investment and further amplify the added value of the Framework Programmes (FPs). It helps to bring a continual stream of innovation to the market and beyond. It will help to speed up the journey towards creating an impact"

In view of the IRIS project, the Horizon Results Booster can be used:

[7] https://www.innoradar.eu/

[8] https://www.horizonresultsbooster.eu/

1. To receive guidance and training for improving IRIS's existing strategy towards the effective exploitation of the anticipated key exploitable results.
2. To ensure the effective transfer of IRIS's project results to the industry, the policymakers, and the society.
3. To maximise the impact of the project and further amplify the added value of the Horizon 2020 work programme.

7.2 Key Exploitable Results

As a result of an internal analysis coordinated by the exploitation manager (CLS) and executed by all partners, the IRIS consortium identified a preliminary list of KERs that are expected to come out of the IRIS project. The following table summarises those KERs along with a short description of each identified KER, the type of KER result (tangible or intangible), expected TRL (at project end), and time to exploit (in years after the project end). An updated list of KERs will be populated in the upcoming versions of this deliverable (namely in D8.4 and in D8.5).

Table 10: Initial list of KERs of the IRIS project

KER name	Type of Result	Expected TRL	Time to exploit (in years)
KER_1: Social acceptance framework	Intangible increased knowledge	N/A	1+ to 3 years
The Social Acceptance of Technology is a proprietary CEL methodology with the ambition of evaluating the social acceptance of new and potentially disruptive technologies within given contexts and to become the best practice for thorough yet feasible research on the topic.			
KER_2: Risk and vulnerability assessment module	Tangible (product)	7	1+ to 3 years
The IoT & AI-provision risk and vulnerability assessment module, which integrates the tools developed by ATOS and CEA, provides identification and assessment of vulnerabilities covering IoT and AI layers and including threat intelligence capabilities.			
KER_3: AI threat analytics and detection engine	Tangible (product/software)	7	1+ to 3 years
This tool 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 generate, as well as their responses to different technical workflows and interactions between them. IRIS will develop machine learning anomaly classifiers for IoT, and AI that will monitor for abnormal deviations in behavioural data telemetry and decision response.			
KER_4: Risk-based response and self-recovery	Tangible (product/software)	7	1 to 2 years
The risk-based response and self-recovery module is a proprietary solution of CLS tasked with modelling attack and threat input from multiple sources to initiate autonomous response and self-recovery procedures.			
KER_5: Digital twin honeypot detection models	Tangible (product/software)	7	1+ to 3 years

KER name	Type of Result	Expected TRL	Time to exploit (in years)
Security models able to mimic the behaviour of deployed real industrial devices. Digital Twin Honeypots will generate threat intelligence based on the targeted environment to allow organizations to identify their adversaries and recognize their attack patterns.			
KER_6: IRIS-enhanced MeliCERTes platform	Tangible (product/software)	7	2 to 3 years
Enhanced MeliCERTes-based CSIRT / CIs communication, communities support, collaboration and information sharing with Unified Customizable Dashboard and Intuitive information visualization with Role-based Access Control for different types of end users			
KER_7: APIs for Advanced threat intelligence orchestration	Tangible (product/software)	7	1 to 2 years
IRIS's orchestrator will be built on the most recent advances in SOAR platforms, such as the open-source shuffle solution. It will provide two visual environments; (i) the Workflow Designer/Manager which enables the definition and execution of various incident response scenarios as well as the steps (if any) that should be executed automatically or manually, and (ii) the Threat Sharing and Response Tasks Management and Tracking which provides information on threat sharing and response tasks that have been automatically applied or should be manually/semi-automatically applied based on risk levels.			
KER_8: Collaborative threat intelligence sharing	Tangible (product/software)	7	1 to 3 years
The cyber threat intelligence sharing component provides the sharing techniques and schemes that support the privacy, disclosure, and incident response requirements for threat intelligence collaboration. A collaborative sharing policy engine will be established to perform semantic analysis of technical and human-based threat intelligence sharing formulation requirements. Additionally, this component enriches the threat intelligence sharing component of the MISP Platform within the MeliCERTes ecosystem, with unique management, processing, and policy enforcement capabilities.			
KER_9: Dynamic repositories of threats and vulnerabilities	Tangible (product/software)	7	1+ to 3 years
The specific tool will be based on the MISP Open-Source Threat Intelligence Platform. MISP, as a repository itself, will be able to collect threats and vulnerabilities that are stored in the MISP itself, store relevant threats and vulnerabilities that are targeted to IoT and AI-driven ICT systems that will be received from inside and outside sources as well as possibly from other external sources (surface and dark web, social networks, crawlers, etc.). As a result, this information is correlated, and the main output is the creation of a dynamic repository of taxonomies and ontologies of threats and vulnerabilities that is generated in a (semi-) automatic way.			
KER_10: DLT-based control services for accountability, traceability, and auditing	Tangible (service)	7	2 to 3 years
This tool (service) uses blockchain technology to provide accountability, auditing, and traceability capabilities on a collaborative threat intelligence network. The solution uses a combination of smart contract, ledger access control layer, and secure tools to guarantee ledger security and prevent actions from being denied and untraced.			
KER_11: IRIS secure crypto functions for data management	Tangible (product/software)	6+	2 to 3 years
The proposed tool combines a new type of data encryption scheme (self-encryption) and an existing highly secure data sharing scheme. The encrypted data can then be used by Task T4.5 (Accountability, Audit and Traceability via DLT). The tool will also allow the recovery of the encrypted data.			
KER_12: IRIS cybersecurity exercises and training scenarios	Tangible (service)	7	3+ years

KER name	Type of Result	Expected TRL	Time to exploit (in years)
Training for CERT/CSIRTS analysts and in general for cyber-security 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.			
KER_13: IRIS lab pods	Tangible (product/software)	7	2 to 3 years
The tool will be able to emulate a copy of the ATA, CTI and DPA modules involved in the pilot scenarios. Cyber security professional will be able to do actions on these emulated modules to react to malicious activities			
KER_14: IRIS cyber range environment platform	Tangible (prototype)	7+	3+ years
By implementing this highly flexible and scalable virtual cyber range service, IRIS introduces innovations in the field of cyber security 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.			
KER_15: IRIS smart city IoT and control system pilot	Tangible (prototype)	7	1 to 2 years
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, the IRIS CTI module will communicate threat intelligence with the IRIS 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: IRIS smart city autonomous transport system pilot	Tangible (prototype)	7	1 to 2 years
This pilot 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, 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.			
KER_17: IRIS cross-border smart grid pilot	Tangible (prototype)	7	1 to 2 years
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 localized 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 normalized 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			

KER name	Type of Result	Expected TRL	Time to exploit (in years)
CSIRTs/CERTs monitoring critical infrastructure for smart cities to train and gain experience executing IRIS-enhanced incident response against novel AI threats.			
KER_18: Integrated IRIS Platform	Tangible (prototype)	7	3+ years
The integrated IRIS threat reporting and incident response platform will provide a dynamic, holistic and disruptive security-enabling solution for minimizing the attack surface in these complex ICT systems. Ultimately, IRIS extends the capabilities of the MeliCERTes platform with an AI-enabled Analyst Threat Intel Companion for orchestrating collaborative human-in-the-loop (HiTL) exchange of intelligence related to novel IoT and AI-based (e.g., machine learning) threats targeting ICT systems.			

Next, we discuss each KER's exploitation type. As mentioned before, within IRIS, we identify two types of exploitation:

i. **Individual exploitation:** The corresponding KER is commercially exploited by a single partner / beneficiary.

ii. **Joint exploitation:** There is a group of partners / beneficiaries that are involved in the KER's commercial exploitation activities.

Table 11: Exploitation type per KER of the IRIS project

KER name	Exploitation type	Lead beneficiary	Contributing partner(s)
KER_1	Individual	CEL	-
KER_2	Joint	ATOS	CEA
KER_3	Joint	ATOS	SID, CEA
KER_4	Individual	CLS	-
KER_5	Individual	SID	-
KER_6	Joint	INTRA	CERTH, ICCS
KER_7	Individual	ICCS	
KER_8	Individual	CERTH	-
KER_9	Individual	CERTH	-
KER_10	Individual	INOV	-
KER_11	Individual	TUD	-
KER_12	Individual	KEMEA	
KER_13	Joint	THALES	CLS, CERTH, ICCS, KEMEA
KER_14	Individual	THALES	-
KER_15	Joint	IMI	INOV, CERT-RO, INTRA, THALES, ATOS, CISCO, CLS, SID, CEA, CERTH, ICCS, TUD, esCERT, KEMEA
KER_16	Joint	TALTECH	INOV, CERT-RO, INTRA, THALES, ATOS, CLS. SID, CEA, CERTH, ICCS, TUD, KEMEA, FVH
KER_17	Joint	FVH	INOV, CERT-RO, INTRA, THALES, ATOS, CLS, SID, CERTH, ICCS, TUD TALTECH, KEMEA
KER_18	Joint	-	IRIS consortium partners

Framework for joint exploitation of results

A framework for the joint exploitation of the outcomes of the IRIS project is being discussed and defined in the context of Task 8.2. This framework is deemed necessary for the analysis of the **Intellectual Property Rights (IPRs)** generated within the project (foreground). Upon Consortium approval, this framework will also represent a guide for the subsequent exploitation analysis of the IRIS's joint exploitable results. The planned outcome is a general framework to help the involved parties agree on the joint exploitation of shared results. The result of such an activity will be a written agreement between the parties that cover the results of the joint exploitation, the purpose of the agreement, its duration, the roles, and responsibilities for each commercial action. It will also cover business models, pricing list, and revenue split between partners. Finally, the agreement will regulate the liabilities of each party and the confidentiality of information exchanged.

7.3 Stakeholder Analysis

A priority contributing to the success of the IRIS project is the identification of the relevant stakeholders and key actors representing the final end-users to adopt or apply the project's outcomes potentially benefiting from the generated knowledge. IRIS considers it very important to regularly inform these stakeholder groups about the aims, progress, results, and products of the project. The main stakeholder groups for our dissemination and exploitation activities were identified in D2.1 'Vision scenarios and use cases definition' and include the following:

- PUC end-users
- CERTs/CSIRTs
- Cybersecurity providers
- European key stakeholders in the IoT/AI sector
  - Industrial players
  - Small and medium sized enterprises
- Policy stakeholders relative to the IoT/AI sector
  - Regional policymakers
  - EC representatives
  - Policy delivery experts
  - National Contact Points (NCPs)
  - Policy analysts
- Research and innovators in IoT/AI sector
  - R&I Institutions
  - Research agencies
  - Thematic DG R&I Directorates
  - Researchers from academia

How to approach them: inform and engage

IRIS will follow an 'inform and engage' approach to reach out its stakeholders. Once an output, result or formal deliverable is ready to be disseminated, the IRIS partners will inform the concerned individuals and institutions. IRIS will establish a continuous dialogue with its potential users both during and after the project lifetime. (**INFORM**)

IRIS also follows a co-creation inspired exploitation strategy. This means that IRIS will involve key stakeholders whenever suitable. This principle ensures that the solutions being developed within the project are appropriate and meet their specific needs. (**ENGAGE**)

Stakeholder and user engagement is also closely linked to the IRIS project events that according to Section 2 have been designed with an exploitation perspective.

7.4 Updated Exploitation Plans

The advanced technological maturity which will be achieved by the end of the IRIS project in various domains and areas of expertise creates significant exploitation potential for all IRIS partners. An updated version of the individual exploitation plans of each IRIS partner are presented below.

7.4.1 Industrial Partners

CISCO: As we plan to deploy the network infrastructure, the three main goals are:

- integrating with the newly proposed solution proving new capabilities to maintain and gain a competitive edge in IoT and AI cybersecurity markets. At this moment, our solution called "Cyber Vision" is being implemented in the PUC1.
- further develop the testbed network we are working with Barcelona City Council to allow third-party companies to test their smart city solutions in a secure and real environment. In order to develop this safe environment for third-party companies we are still build the hardware part, the fibres are being deployed right now.
- based on the results and learnings form that project to develop new cybersecurity capabilities to secure future IoT networks. On this item, since we don't have any results yet, there are no further updates.

As a global player in the IT industry, including cyber-security, Cisco Systems can provide several channels through which it can initiate and realize the commercial opportunities emerging from the project:

a. Cisco Solution Partner Program allowing prospective partners to build and sell enterprise solutions that require configuration and are implemented in a customer environment. The partnership with Cisco ecosystem enables increased market share, as well as opens global commercial opportunities through Cisco's global sales channels.

b. Cisco DevNet - Cisco's developer program to help developers and IT professionals who want to write applications and develop integrations with Cisco products, platforms, and APIs. The key focus areas are IoT, Cloud, Networking, Data Center, Security, Analytics Automation, Open Source, Collaboration and Mobility. It provides an efficient sandboxing and development environment supported by relevant Cisco technical and business development resource to enable future integration within Cisco solutions. For the development of PUC1 we are using the API's from devnet https://developer.cisco.com/.
c. Cisco Marketplace is an online platform allowing dedicated online presence for Cisco-based approved solutions by creating a storefront for each of the solutions. The presence and links to Cisco website, its global branding and resources increases visibility both among Cisco sales teams as well as customers, leading to sales channels growth, generation of new leads, and expansion into new markets. In addition, potential buyers visiting the Marketplace can quickly search and discover the solutions, learn about them, and connect with the relevant party.
d. Cisco Partner Ecosystem includes a world-spanning network of collaborators with Cisco, enabling addressing all technical and commercial needs to realize a market opportunity. The Ecosystem includes:
    i. Developers – to design, test, and build everything from software to solutions to services.
    ii. Integrators, - to combine technologies from many different sources to create solutions. On this part, we have Italtel, they are helping us with the deployment of Cyber Vision for PUC1.
    iii. Builders, - to create new private cloud solutions from scratch.
    iv. Providers – to use our technology and services to offer other services.
    v. Consultants - to recommend technology and services from us and other partners.
    vi. Lifecycle advisors - to help customers choose the right software and services at every stage of the solution.
    vii. Distributors – to package up and sell our software, solutions, and services through resellers.
    viii. Resellers – to sell our software, solutions, and services directly to the prospective customers.

The partner ecosystem is critical for coverage of the opportunity. Cisco will lead the identification and engagement of key strategic partners for project outputs. This is a critical first step and intermediate commercial solution while other formal partnership routes, such as those set out below, are worked through.

INTRA: To support growth and innovation in its products and services portfolio, INTRA participates actively as a project and/or technical coordinator, as well as technology provider, in EU-funded research and development projects, that among others facilitate know-how exchange and business alliances. Furthermore, through its participation in IRIS, INTRA is specifically expecting to:

- Exploit the resulting enhanced MeliCERTes IRIS ecosystem in its current products and services as provider of AI-enabled services/products in diverse market segments. The respective offering could be bundled with its products and services to promote a cybersecurity and threat intelligence sharing culture to its clientele. INTRA is particularly interested to remain close to fast developments in the respective cybersecurity arena.
- Join in joint exploitation paths of the IRIS technological platform with the consortium partners, including of course open sourcing the resulting integrated platform, following the MeliCERTes CSP and MISP paradigms, to allow for wider adoption in the relevant communities
- Investigate the possibility of offering IRIS as a service ecosystem in collaboration with the rest of the Consortium partners (i.e., customization, maintenance, installation, service provision, training).
- Deliver consultancy services to customers interested in deploying similar infrastructures.

ATOS: Atos is a global leader in cybersecurity offering end-to-end security services and well positioned to prepare, implement, and manage sustainable long-term security models, crafted to individual industry sector conditions, for bold IoT and IoE adoption. The activities that Atos will develop in IRIS will allow not only to preserve the current business but also to extend it and provide our clients with the cutting-edge technology that impulses their business. In particular, the advances in threat intelligence and incident response suggested by IRIS project perfectly with the ATOS commitment to provide security, smart and trustworthiness IoE solutions.

Atos offers different types of solutions for cybersecurity, ranging from monitoring and analysis of data transfer to active protection and reaction to cyber critical infrastructures, all together with innovative solutions in a unique portfolio. The involvement of Atos in the development of risk & vulnerability assessment module will entail new business opportunities increasing our solutions and services portfolio. For this purpose, the first step is to approach the market through the Atos sales team and to promote the adoption of innovative solutions and emerging technologies. On other hand, Atos is fully committed with the technology transfer derived from R&D projects, promoting an inside-out technology push. Even more, Atos Research & Innovation department serves as the catalyst for innovation, through the different IT Labs, through robust partnerships like the one with Siemens, through Start-up’s mechanisms, etc. This project will be carried out by the R&D team of the Cybersecurity Unit who will ensure a continuous investigation in that area after the project. In this sense, the exploitation of IRIS results in current and future R&D projects is also of key importance for the company. Other exploitation activities will be establishing partnerships with the rest of Europe increasing our competitiveness, having the opportunity of exchange know-how with research institutions, public administrations, and industrial partners.

THALES: THALES proposes the Cybels Range platform as the foundation of its cyber training offer. THALES proposes a complete offer, from the delivery of the platform itself up to services to assists its clients in the platform usage and to increase their experience. The Cybels platform allows creating complex network topologies that reproduce the behaviour of real-life systems. The Cybels Range platform’s architecture consists of the following elements:

1. a virtualization platform that supports the virtualization of typical network topologies and their assets,
2. the virtualization of hosts and information systems,
3. a traffic generator,
4. an administration platform.

The innovations brought by IRIS will allow specializing the cyber range platform towards advanced CERT/CSIRT usage, both from a technical and methodological standpoint.

7.4.2 Small and Medium-sized Enterprises

CLS: CyberLens (traded as Exalens since September 2021) is interested in exploiting the outcomes of R&I projects by developing and releasing products that meet a set of quality requirements such as software tested, accompanying documentation, installation guidelines and best practices. Within IRIS, CLS intends to gain insights from the project results in order to reinforce the company's position through the advancement of its products, especially by expanding its existing software with risk-based incident response technologies to address threats and vulnerabilities in complex ICT infrastructures, systems, and services. Furthermore, CLS will attempt to showcase the added value that could be brought from the IRIS results in domains not relevant to the project's scopes (e.g., security solutions applicable to healthcare, maritime, smart power grid, and industrial control systems).

Finally, CLS will aim to identify opportunities for technology transfer into the industry, e.g., by transferring technological know-how and/or integrating the software components developed in the context of the IRIS project in future collaborations with industrial partners, e.g., software vendors, SMEs, and consultants, in the Netherlands and the rest of Europe. New business collaborations resulting from IRIS will give CLS the capacity to extend its line of business applications with solutions relevant to incident response and self-recovery.

CEL: CEL has the following exploitation goals:

1. Acquisition of knowledge related to IoT and AI technologies impact on society.
2. Reinforce CEL position in the market as an innovative service provider.
3. Enlarge CEL network to create new opportunities with new partners and customers for further strategic services.
4. Create awareness through a strong dissemination and communication action on the project field.

The approach and activities to achieve the exploitation plans include:

1. Provide privacy and ethics compliance in new and emergent sectors.

2. Enhance consultancy services for clients such as the public administration or private companies.
3. Formulate new training courses in the educational field.
4. Reinforce company business model based on Privacy and Ethics as Service. Participate to further research and innovation activities.

SID: SIDROCO brings a wide range of New Generation Internet of Things (NG-IoT) features and capabilities for developing, supporting, and managing ultra-innovative products and services by delivering efficient, effective, and secure NG-IoT solutions for diverse heterogeneous environments such as energy, healthcare, and autonomous driving. SID will inform the target audience about the technological advantages of IRIS, such as the deployment of secure infrastructure and software. The Technical audience in Cyprus and Southern Europe will benefit. SID will also benefit from IRIS' findings on the activities and private domain of Cyprus and Southern Europe. SID will demonstrate the benefits of IRIS in dealing with cyber risks to support the impact of exploitation.

7.4.3 Academic & Research Partners

INOV: INOV will carefully study the project results and will define a dedicated strategy for each specific IRIS outcome INOV is involved. Since INOV is a private non-profit research institute, direct commercial exploitation is not a goal. However, INOV plans to exploit the project results by using the know-how gained through the IRIS project to explore new business opportunities, either related to the project itself or to the technologies developed and demonstrated by the IRIS Consortium. The exploitation will mainly consist of an extended collaboration with the IRIS partners after the completion of the project, aiming to license the DLT technology developed for industrial partners as well as the exploration of further research and partnerships for results exploitation.

CERTH: CERTH plans to exploit the IRIS project results by reinforcing its research competencies in the area of Cyber Threat Intelligence (CTI) enrichment through advanced CTI extraction, analysis, and correlation techniques, and also by building and updating cybersecurity-related dynamic taxonomies and ontologies in an (semi-) automated manner, as well as in the area of sharing CTI among relevant stakeholders. Furthermore, CERTH aims to exploit the outcomes of IRIS by commercialising the developed modules : (1) through the Information Technologies Institute of CERTH that has all the necessary legal and business management support in order to create innovative enterprises, or (2) through its spinoff company Infalia (www.infalia.com) which is also active in the cybersecurity domain through its participation in the SPIDER project (https://spiderproject.eu), or (3) by licensing the developed services to interested clients. Furthermore, part of CERTH's business plan is to participate in joint spin-off commercial companies capable of exploiting its research when new market needs, and solutions are identified.

CEA: IRIS will complement the efforts of CEA List to develop and transfer its binary-level code analysis platform BINSEC. Thanks to IRIS, CEA List will lift its cyber-reasoning capabilities to detect vulnerabilities, opening both new research lines towards increasingly complex attacks and a new application domain to its core technology. IRIS will also set to CEA List the opportunity to showcase both its technology and its skills through the demonstrator. These activities will benefit from the proactive technology transfer mission of CEA List to its partners by means of the following mid- to long-term mechanisms:

- Joint Laboratories, consisting of specific contracts aiming at transferring some well-defined intellectual property from CEA to industry, possibly using a team of dedicated personnel,
- patents and intellectual properties sale, and
- the creation of start-up companies.

These means have already been applied in the LSL laboratory in the recent past, thus demonstrating their potential and effectiveness.

ICCS: Exploitation targets include the production of research results, of knowledge dissemination and of pursuing the potential of a spin-off company to exploit established experience in Cybersecurity training by deploying simulation environments. The main target group will be CERTs/CSIRTs at national and European level. The above goals will be achieved:

- At a scientific level, it will acquire in depth knowledge with respect to technologies enabled on cyber preparedness and protection tools and environments as well as enhance its visibility through collaborating with strategic industrial players of the consortium thus adding an application-oriented direction in its activities.
- At an R&D level, the gain of experience and increased reputation in the field of Cybersecurity competent authorities and actors through IRIS will enable successful participations of ICCS in future related R&D projects.

TUD: TUD will be planning to exploit the project results by reinforcing its research and engineering competencies in the areas of secure data encryption, data recovery and DLT. Furthermore, TUD will be aiming to exploit the project results in a commercial manner through local Dutch companies and industrial partners, e.g., Philips, and Dutch Blockchain Coalition.

TUD will be planning to exploit the outcomes of IRIS in a commercial manner through its industrial partners or licensing the developed services to interested partners. The university has all the necessary legal and business management support to collaborate with innovative enterprises.

TALTECH:

1. Understanding better the existing and possible future cybersecurity risks for the cities, research institutions, companies using Urban Data Platforms (UDP) for developing their services, business models, activities.

2. UDP is a basis for visualization of e.g., city infrastructures data and an attack that manipulates the data can result in diminished number of users for the UDP (loss of trust). Therefore, a functioning cyber-threat information sharing, and analytics system is a "must-have" for UDP.
3. The risk of cyber-attacks can be a reason for the cities and companies to refuse to use the UDP or to submit their data to the UDP. Having a working solution for this problem could enhance the use of UDP by different stakeholders.

TalTech Smart City of Excellence FinEst Twins (FT-CoE) is developing in close collaboration with FVH an urban open data platform (UOP) that brings together data flows across different city systems like infrastructure, environmental sensors and from private and public sectors. One of the goals of FT-CoE is to enhance the use of UOP in cross-border context of the cities of Tallinn and Helsinki, with up-scaling possibility to other cities in Estonia and Finland. The data that comes into UOP is translated into open standards and is ready to be further developed by public, private sector or by people to solve different social, environmental, and economic problems. In Europe, Urban Data Platforms (UDP) are being developed in ca 80 cities. UDP is becoming an important information and communication channel for people as well as for public and private sectors. Therefore, the IRIS project offers a great possibility for TalTech FT-CoE to understand better cybersecurity risks connected with UDP and test solutions for protecting the data flows from IoT devices. The results of the projects could be up-scalable for other cities using UDP-s and offer a good basis for information sharing and for debating cybersecurity risks and solutions with other EU cities.

7.4.4 Stakeholders

ECSO: IRIS objectives are in line with the ongoing work in ECSO. The project outcomes will be able to leverage ECSO's policy engagement activities and ECSO's broad cybersecurity community which is supported by the European Commission. ECSO's network of members includes all categories of stakeholders representing 27 EU Member States. This network will be utilized to transfer and scale up project outcomes at the EU, regional, national, and local levels. Furthermore, ECSO will align project outcomes with its own activities in WG3 on strengthening Cyber Resilience of Economy, Infrastructure and Services through the CISOs European Community, WG1 on standardization and Certification, and WG5 on Education, Skills and Cyber Ranges. Finally, ECSO is in a good position to align project outcomes with market demand, cyber range environments, and relevant EU policies and strategies.

ECSO will ensure exploitation through:

- European level outreach - reaching national / regional / local stakeholders through its members
- Leveraging on social media presence to communicate results and messages beyond the lifetime of the project
- Linking project outcomes with the activities of ECSO WGs (especially WG1, WG3, and WG5) and the CISO Community
- Advocating for alignment of project outcomes with existing EU policies and strategies

DNSC: In accordance with the NIS directive requirements, DNSC plays the role of the national cyber security competent authority. DNSC also plays the role of Single point of contact at national level for cyber issues and National CSIRT. Thus, DNSC will exploit the outcomes of the IRIS project to strengthen the national cyber security level. The project will also be useful to expand the partners' collaboration network regarding new research and development initiatives.

DNSC acts as an end-user partner, participating in the pilot deployments. DNSC will apply the knowledge and expertise gained through IRIS on a methodological level, as well as in its future research activities. On an operational level, the project will help DNSC in identifying the critical risks of the ITC infrastructure in its jurisdiction and will provide a powerful tool to mitigate possible attacks.

Also, the platform will be used to guarantee that information is securely stored and transferred, maintaining the privacy of the personal information of its users. Based on the activities from IRIS project, DNSC will also be able to train its staff members in dealing with crisis situations and to extend its expertise in this domain and will provide important input towards its activities related to smart city service offering.

UPC-esCERT: UPC-esCERT will exploit the insights gained from its participation in PUC1 to extend the capabilities of the Barcelona IoT and Smart City infrastructure while also significantly strengthening its cybersecurity posture. Another expected benefit from esCERT's participation in IRIS is the background knowledge that it will gain which will facilitate participation in future projects in the public and private sectors. In particular, UPC-esCERT plans to exploit the outcome of the IRIS project as know-how and starting point for security auditing in the area of IoT and smartcities by providing security consultancy, compliance and governance assessment and best practices to third parties interested. In fact, the leading technology transfer team in UPC-esCERT will greatly benefit of such knowledge by using it to further secure the infrastructure of already existing partners and collaborators. UPC-esCERT will also validate that the IRIS platform is performing as expected within the PUC1 environment. In practice, this validation, will enhance the set of skills of UPC-esCERT team with automation capabilities which will prove very useful to exploit with the aforementioned partners and collaborators. By strengthening the understanding of IoT security enhanced knowledge, UPC-esCERT expects to provide a more competitive and up-to-date portfolio of solutions to the table.

KEMEA: KEMEA as the think tank of the Hellenic Ministry of Citizen Protection regarding to security policies, R&D and innovation actions will bring the IRIS project's outcomes to the attention of the Ministry and will promote the project's validated solutions as prototype to the Ministry's supervised and associated entities to enhance and support the First Responders services. KEMEA will exploit the IRIS platform to enhance its research expertise, consultancy services and portfolio in the relevant security domain.

IMI: As a public administration, Institut Municipal d’Informàtica (IMI) will exploit the results of IRIS proposal to impulse new public services and improve the existing ones. Thanks to the knowledge generated during the project and the pilot conducted in Barcelona, IMI will have the opportunity to test new architectures were Cloud and Edge will have a central role.

The information and experience gathered during the project will be useful to inspire and provide orientation to future development of tools that help on the management of increasing municipal resources and generate reporting for services stakeholders (users, contractors, public responsible, infrastructure coordinators and infrastructure contractors). In this domain, the project will help to energize and generate opportunities to the local companies working in the technological domain, helping them to become more competitive.

FVH: FVH will exploit the project results through the Urban Open Platform and Lab, which will design and trial various jointly created smart city pilots, like IRIS, in a real-life environment, such as autonomous cars, smart street lighting etc. also aspires to create smart and sustainable models for future cross-border smart cities.

8 CONCLUSION

The current report provides a complete overview of the dissemination, communication, standardisation, and exploitation activities that have been conducted since the beginning of the project until M12 of the project's lifetime.

The document includes the IRIS dissemination and communication activities and tools used, such as the project website, social media (Twitter, LinkedIn, YouTube Channel) and other online platforms (Zenodo Community, Cyberwatching.eu), the communication material (brochure, roll up banner, general presentation, e-newsletters) as well as the press releases and activities. IRIS consortium partners have been actively engaged and they have been contributing to the dissemination of the project's vision, objectives, and results with their participation in several events. There is also reference to the effort made on establishing strong relations with other H2020 projects and relevant stakeholders.

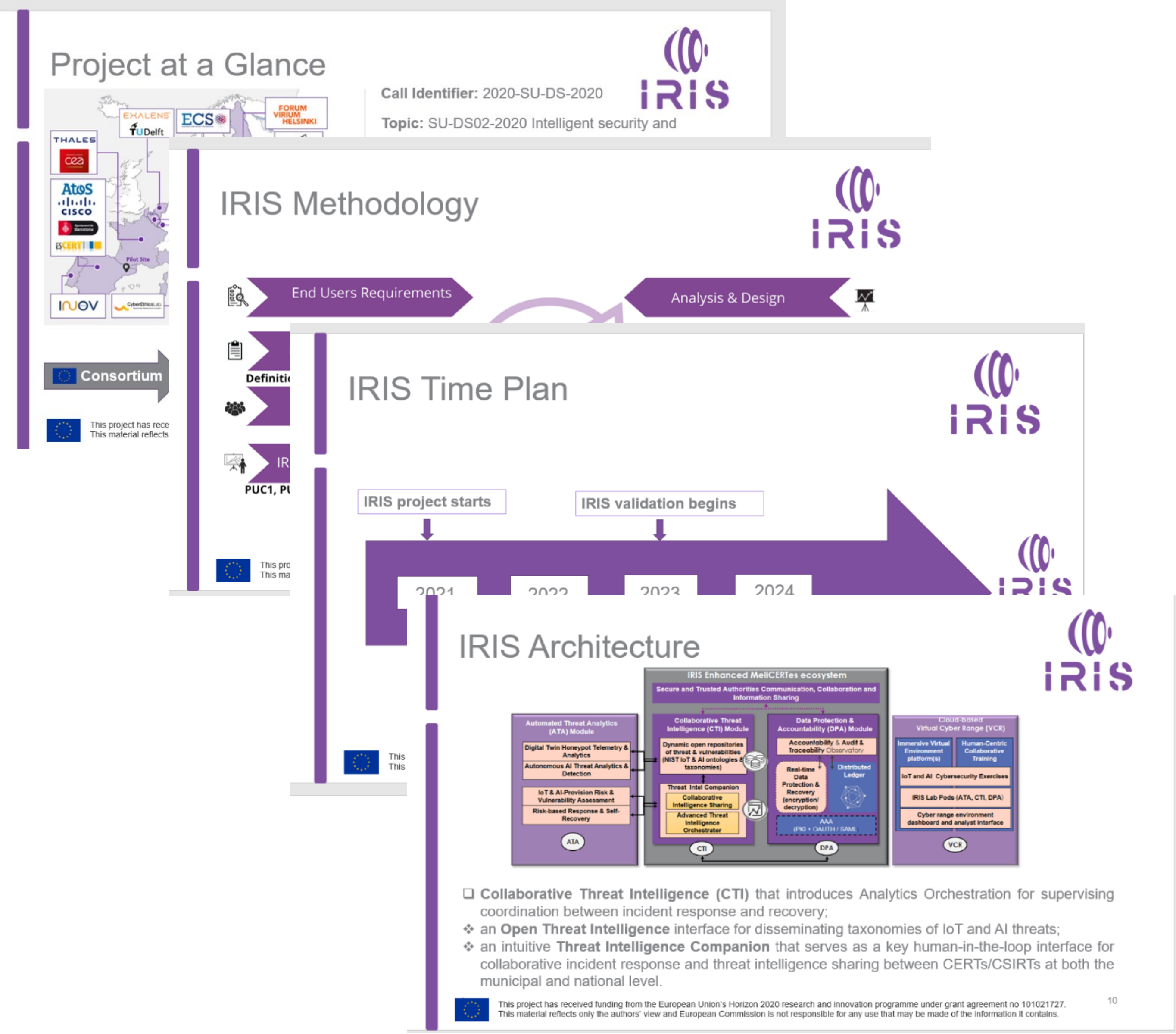
It also describes the internal reporting procedure established to keep a record of the dissemination and communication activities and their evaluation based on the expected Key Performance Indicators mentioned in the Grant Agreement. Moreover, there is a reference on the future dissemination and communication plans and steps. The final sections refer to the standardisation and exploitation activities performed until month 12 of the project.

The activities summarised in this report represent a productive 12-month period of the IRIS project and the high performance of these activities is showing that the second year of the project will be even more fertile.

A further update on the actions discussed and foreseen in this deliverable will be covered in the next report namely the deliverable D8.4 "Interim report on dissemination, communication, standardisation, and exploitation" that will submitted in month 24.

9 APPENDIX

9.1 Appendix I - IRIS general presentation



Project at a Glance

Call Identifier: 2020-SU-DS-2020

Topic: SU-DS02-2020 Intelligent security and

Consortium

This project has rece
This material reflects

IRIS Methodology

End Users Requirements

Analysis & Design

Definiti

IR

PUC1, PU

This pro
This ma

IRIS Time Plan

IRIS project starts

IRIS validation begins

2021

2022

2023

2024

This
This

IRIS Architecture

IRIS Enhanced MeliCERTes ecosystem
Secure and Trusted Authorities Communication, Collaboration and Information Sharing
Automated Threat Analytics (ATA) Module
Digital Twin Honeypot Telemetry & Analytics
Autonomous AI Threat Analytics & Detection
IoT & AI-Provision Risk & Vulnerability Assessment
Risk-based Response & Self-Recovery
ATA
Collaborative Threat Intelligence (CTI) Module
Dynamic open repositories of threat & vulnerabilities (NIST IoT & AI ontologies & taxonomies)
Threat Intel Companion
Collaborative Intelligence Sharing
Advanced Threat Intelligence Orchestrator
CTI
Data Protection & Accountability (DPA) Module
Accountability & Audit & Traceability Observatory
Real-time Data Protection & Recovery (encryption/ decryption)
Distributed Ledger
AAA (PKI + OAUTH / SAML)
DPA
Cloud-based Virtual Cyber Range (VCR)
Immersive Virtual Environment platform(s)
Human-Centric Collaborative Training
IoT and AI Cybersecurity Exercises
IRIS Lab Pods (ATA, CTI, DPA)
Cyber range environment dashboard and analyst interface
VCR

❑ **Collaborative Threat Intelligence (CTI)** that introduces Analytics Orchestration for supervising coordination between incident response and recovery;

❖ an **Open Threat Intelligence** interface for disseminating taxonomies of IoT and AI threats;

❖ an intuitive **Threat Intelligence Companion** that serves as a key human-in-the-loop interface for collaborative incident response and threat intelligence sharing between CERTs/CSIRTs at both the municipal and national level.

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

10