



Artificial Intelligence Threat Reporting and Incident Response System

D8.5 Final 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:	31/8/2024
Deliverable Submission Date:	3/9/2024
Deliverable Version:	v1.0
Main author(s) and Organisation:	Maria Tsirigoti, ICCS
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	03/09/2024
Peer Review 1	Sebastijan Čutura	ECSO	29/08/2024
Peer Review 2	Javier Gil-Quijano Michaël Marcozzi	CEA	30/08/2024
Submitted by (Project Coordinator)	Gonçalo Cadete	INOV	03/09/2024

Contributors

Organization
Sofia Tsekeridou (INTRA)
Konstantinos Chisiridis (INTRA)
Roberto Cascella (ECSO)

Document History

Version	Date	Modification	Partner
ToC	09/07/2024	ToC	Maria Tsirigoti (ICCS)
v0.1	20/07/2024	1 st draft ready (dissemination, communication and clustering activities)	Maria Tsirigoti (ICCS)
v0.2	24/07/2024	Input for the exploitation section	Sofia Tsekeridou, Konstantinos Chisiridis (INTRA)
v0.3	29/07/2024	Input for standardization section	Roberto Cascella (ECSO)
v0.4	01/08/2024	Semi-final version for internal review (after the implementation of the exploitation and standardization input)	Maria Tsirigoti (ICCS)
v0.5	30/08/2024	Reviewed version (implementation of ECSO's comments)	Maria Tsirigoti (ICCS)
v0.6	02/09/2024	Reviewed version (implementation of CEA's comments)	Maria Tsirigoti (ICCS)
v1.0	03/09/2024	Final version	Maria Tsirigoti (ICCS) Gonçalo Cadete (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

1	INTRODUCTION.....	9
1.1	Project Introduction	9
1.2	Deliverable purpose.....	9
1.3	Intended readership.....	9
1.4	Relationship with other deliverables and tasks	9
2	DISSEMINATION AND COMMUNICATION CHANNELS AND ACTIVITIES FROM M24 UNTIL M36	11
2.1	Online Tools	11
2.1.1	Website	11
2.1.2	Social Media	11
2.1.3	Zenodo Community	14
2.2	Dissemination Material	14
2.3	Newsletters.....	15
2.4	Press Releases & Press Activities	16
2.5	Videos	17
2.6	Events	18
2.7	Publications.....	20
2.8	Workshops	22
2.8.1	3 rd Stakeholders and Industrial Workshop.....	22
2.8.2	Final Exploitation Workshop	22
2.9	Other Activities	23
2.9.1	IRIS Tools Video Campaign	23
2.9.2	IRIS Blog.....	24
2.9.3	IRIS Training Sessions	24
2.9.4	IRIS Pilot Use Cases	25
3	KEY PERFORMANCE INDICATORS.....	26
4	EXPLOITATION ACTIVITIES FROM M24 UNTIL M36	27
4.1	List of IRIS Key Exploitable Results	29
4.1.1	KER #1: Social Acceptance Framework.....	29
4.1.2	KER #2: Risk and vulnerability assessment module	29
4.1.3	KER #3: AI threat analytics and detection engine	29
4.1.4	KER #4: Risk-based response and self-recovery.....	30
4.1.5	KER #5: Digital twin honeypot detection models.....	30
4.1.6	KER #6: IRIS-enhanced MeliCERTes platform	31
4.1.7	KER #7: APIs for advanced threat intelligence orchestrator	31
4.1.8	KER #8: Collaborative threat intelligence sharing and storage	31
4.1.9	KER #9: DLT-based control services for accountability, traceability, and auditing	32
4.1.10	KER #10: IRIS secure crypto functions for data management.....	32
4.1.11	KER #11: IRIS cybersecurity exercises and training scenarios	32
4.1.12	KER #12: IRIS Lab Pods	33
4.1.13	KER #13 : IRIS cyber range environment platform	33
4.1.14	KER #14: IRIS smart city IoT and control system pilot.....	33



4.1.15	KER #15: IRIS smart city autonomous transport system pilot.....	34
4.1.16	KER #16: IRIS cross-border smart grid pilot	34
4.1.17	KER #17: Integrated IRIS Platform.....	34
4.1.18	KER #18: Autonomous Threat Analytics (ATA) Service Bundle	35
4.1.19	KER #19: Enhanced MeliCERTes Ecosystem (EME) Service Bundle	35
4.1.20	KER #20: Virtual Cyber Range training (VCR) Service Bundle.....	36
4.1.21	KER #21: Add-ons Services Service Bundle.....	36
4.1.22	KER #22: Algorithms for Adversarial Attack Detection.....	37
4.2	Exploitation Strategy of the IRIS cybersecurity platform.....	37
4.3	The IRIS Exploitation Workshop as part of the Cybersec Expo& Forum in Krakow, Poland.....	38
5	<i>CLUSTERING ACTIVITIES FROM M24 UNTIL M36</i>	<i>41</i>
5.1	Secure Cyber Cluster.....	41
5.1.1	Secure Cyber Cluster logo & brand book	41
5.1.2	Secure Cyber Cluster e-newsletters.....	41
5.1.3	Secure Cyber Cluster LinkedIn.....	42
5.1.4	Secure Cyber Cluster workshops	43
5.1.5	Secure Cyber Cluster press release and policy brief	43
5.2	Stakeholders and Industrial Workshops	44
5.3	ECSCI workshops	45
5.4	Other events	46
6	<i>POLICY AND STANDARDISATION ACTIVITIES FROM M24 UNTIL M36</i>	<i>47</i>
6.1	Potential contribution to standards	55
7	<i>CONCLUSION</i>	<i>56</i>
8	<i>ANNEXES.....</i>	<i>57</i>
8.1	Annex 1: Updated Dissemination Material	57
8.2	Annex 2: Secure Cyber Cluster brand book.....	64



List of Figures

Figure 1: Google analytics screenshot	11
Figure 2: IRIS X (Twitter).....	12
Figure 3:IRIS LinkedIn.....	12
Figure 4:IRIS Mastodon	13
Figure 5:IRIS YouTube channel	13
Figure 6: IRIS Zenodo Community	14
Figure 7: Newsletters No 5 & 6.....	15
Figure 8: IRIS press releases (3rd year).....	16
Figure 9: Screenshot from the IRIS general video	17
Figure 10: 3rd IRIS Stakeholders and Industrial Workshop	22
Figure 11:IRIS Final Exploitation Workshop	23
Figure 12: IRIS Tools Video Campaign	23
Figure 13:IRIS blog	24
Figure 14: Training session at Cisco Madrid Innovation Center.....	24
Figure 15: IRIS PUCs.....	25
Figure 16: IRIS Exploitation Workshop in Krakow, Poland.....	39
Figure 17:Secure Cyber Cluster logo	41
Figure 18: Secure Cyber Cluster e-newsletter No 5	42
Figure 19:Secure Cyber Cluster LinkedIn page	42
Figure 20: Cluster's joint workshops	43
Figure 21: Screenshots of the Secure Cyber Cluster's press release and policy brief	44
Figure 22: 3rd IRIS Stakeholders and Industrial Workshop	44
Figure 23: ECSCI workshops	45
Figure 24: Workshops organized by other H2020 projects	46
Figure 25: 2 nd IRIS brochure (Cover)_ Pilot Use Cases	57
Figure 26: 2nd IRIS brochure (Inside)_ Pilot Use Cases	58
Figure 27: 5 th IRIS roll up banner_ Pilot Use Cases.....	59
Figure 28: 3rd IRIS brochure _ IRIS Components	60
Figure 29: 4th IRIS brochure _ Service Bundles & Components.....	63
Figure 30: Secure Cyber Cluster brand book	65

List of Tables

Table 1: List of events (M24-M36)	19
Table 2: List of the project's publications (M24-M36)	21
Table 3: IRIS KPIs.....	26
Table 4: Standards and the relevance for IRIS.....	53
Table 5: Well established, used or under development standards	55
Table 1: List of events (M24-M36)	19
Table 2: List of the project's publications (M24-M36)	21
Table 3: IRIS KPIs.....	26
Table 4: Standards and the relevance for IRIS.....	53
Table 5: Well established, used or under development standards	55



LIST OF ABBREVIATIONS AND ACRONYMS

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



EXECUTIVE SUMMARY

The purpose of this deliverable entitled D8.5 “Final report on dissemination, communication, standardisation and exploitation” is to provide a report of the activities performed in the IRIS project in the last project year (M24-M36), regarding the dissemination, communication, standardisation and exploitation activities of the project. Deliverable D8.5 is the continuation of the D8.3 “Initial report on dissemination, communication, standardisation and exploitation” and D8.4 “Interim report on dissemination, communication, standardisation and exploitation” and presents the activities and related impacts of initiatives undertaken by the IRIS project partners.

The first section of the document delivers an overview of our activities relating dissemination and communication, presented per channel and tool used. The document presents, in detail, all the progress that has been made in dissemination and communication of the project’s results and in engaging the target audiences and stakeholders, through tables presenting their expected and current performance. Then, there is a dedicated chapter which presents in detail the exploitation and business modelling activities of IRIS project implemented during the third year of the project (from M24 until M36) along with the planned future steps. The next chapter showcases all the clustering and liaising activities held with relevant stakeholders and similar H2020 projects in the past 12 months. Finally, there is an overview of the work performed regarding the standardisation activities in the third project year.

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



1 INTRODUCTION

1.1 Project Introduction

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

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

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

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

1.2 Deliverable purpose

The document includes all the activities on dissemination, communication, standardisation and exploitation that have been undertaken by the consortium partners during the third and last year of the project (M24-M36).

1.3 Intended readership

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

1.4 Relationship with other deliverables and tasks

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

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

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

D8.3: Initial report on dissemination, communication, standardisation and exploitation, which includes all dissemination and communication activities, the exploitation and standardization activities as well as the clustering and community building activities with relevant



stakeholders' that have been undertaken, during the first twelve (12) months of the project, and those still planned. The deliverable will also include the analysis of the standardization landscape and policies relevant to IRIS. The deliverable 8.3 also serves as a guiding document for the deliverables 8.4 and 8.5.

D8.4: Interim report on dissemination, communication, standardization and exploitation, which will include all dissemination and communication activities, the exploitation and standardization activities as well as the clustering and community building activities with relevant stakeholders' that have been undertaken, during the first two years of the project, and those still planned.



2 DISSEMINATION AND COMMUNICATION CHANNELS AND ACTIVITIES FROM M24 UNTIL M36

2.1 Online Tools

2.1.1 Website

The IRIS website www.iris-h2020.eu went live in November 2021 (M2 of the project life span). Its concept, objectives, design, and many more details are presented in the deliverable D8.1 “Project Website” submitted in M3. Since then, the website has been continuously updated with the consortium activities, the project’s achievements and new engaging sections.

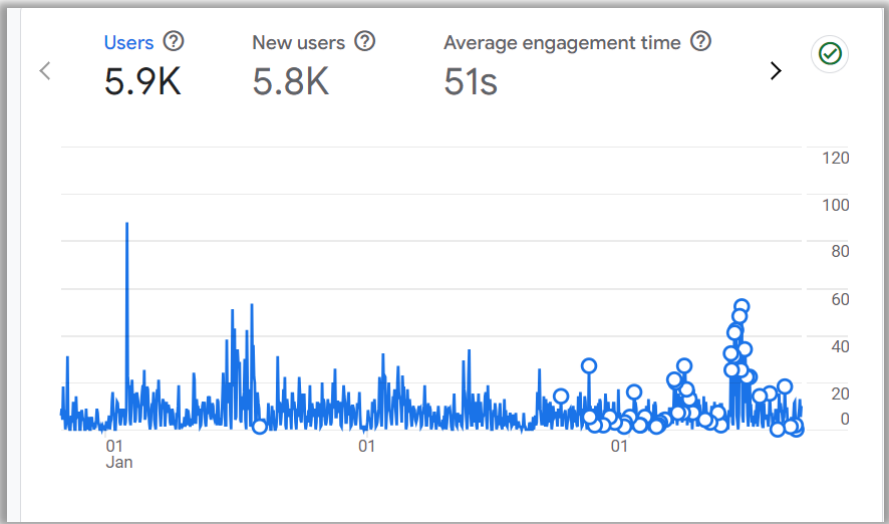


Figure 1: Google analytics screenshot

Activity	Expected KPI	Current Status M24
www.iris.eu	5000 per year	5,9 K (total)
	Ready by M2	accomplished

2.1.2 Social Media

X (former Twitter) and LinkedIn accounts were set up before the official launch of the project to raise awareness. In a later stage, the project’s YouTube channel was created to host all the project’s promo videos and finally, we created a Mastodon account to support the audiences’ engagement. During the last year of the project and in order to present the project’s innovations to non-technical audience, we launched a video campaign presenting the IRIS tools through our social media.

The project’s social media accounts are very active and have exceeded by far the expected 3rd year results.



Figure 2: IRIS X (Twitter)

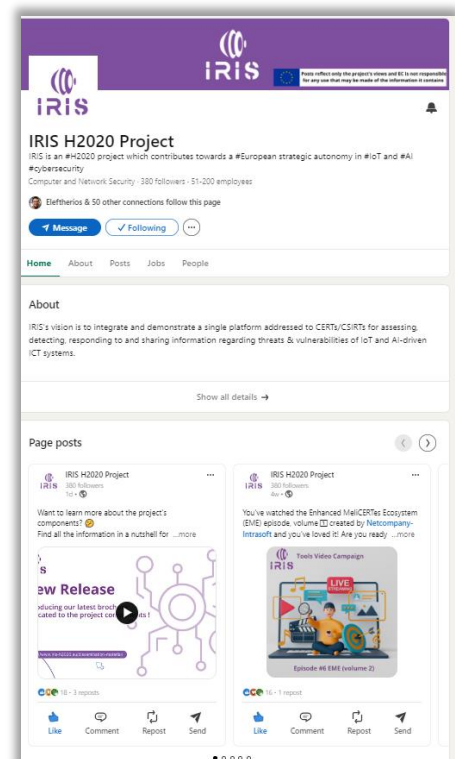


Figure 3: IRIS LinkedIn

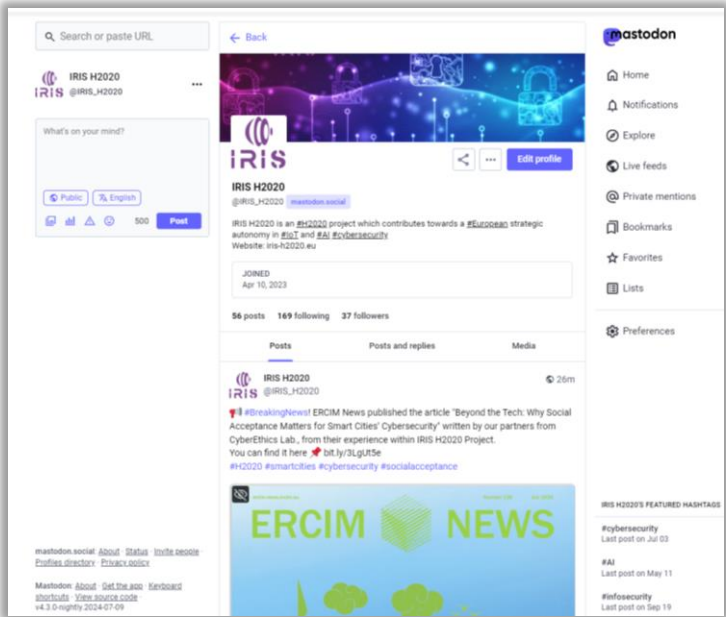


Figure 4:IRIS Mastodon

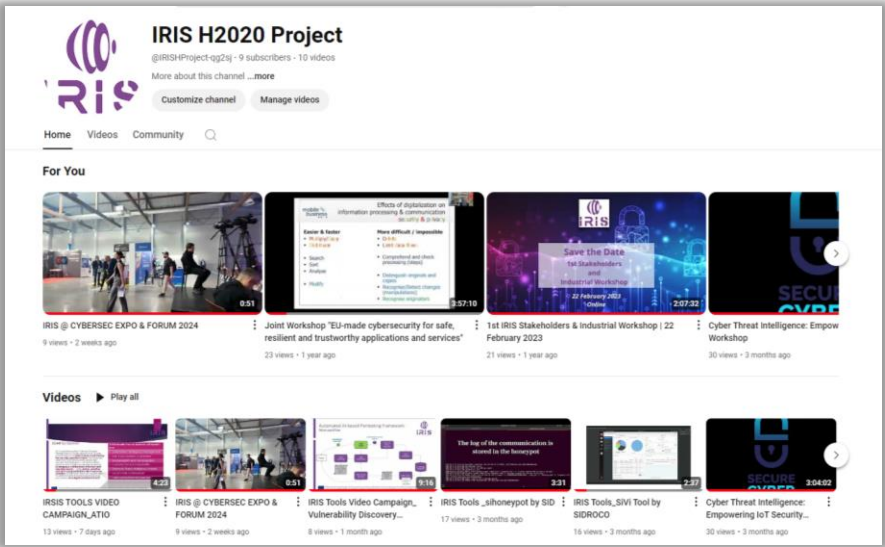


Figure 5:IRIS YouTube channel

Activity	Expected KPI	Current Status M36
X (former Twitter)	300 followers	967 followers
LinkedIn	300 followers	380 followers
YouTube	N/A	13 videos, 250 views
Mastodon	N/A	37 followers



2.1.3 Zenodo Community

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

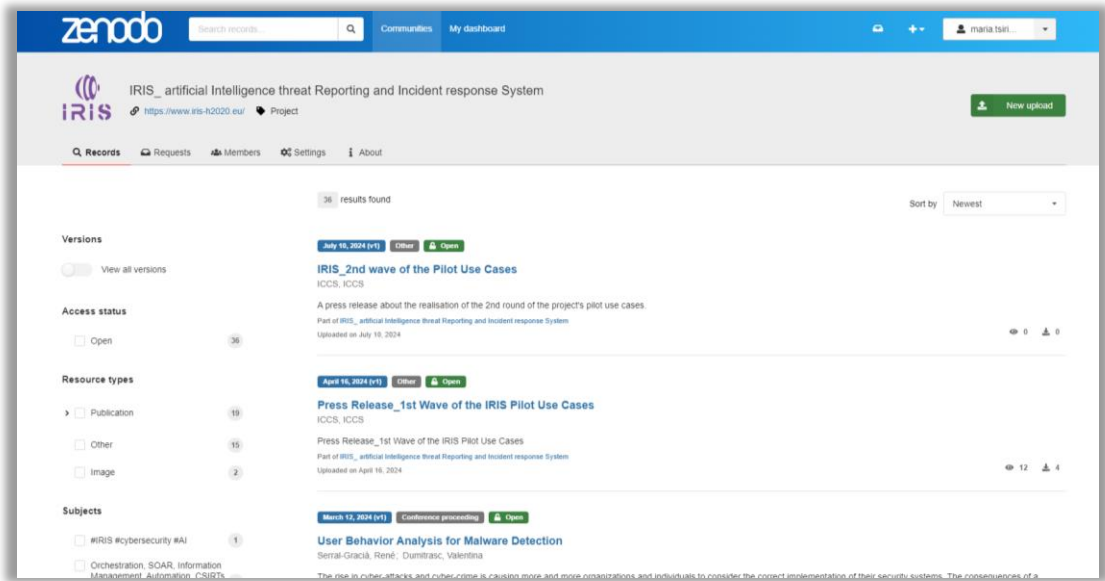


Figure 6: IRIS Zenodo Community

2.2 Dissemination Material

The initial version of the project’s brochure and roll up banner were created in M03 and they are presented in D9.3 Initial report on dissemination, communication, standardization and exploitation that was submitted in the first half of the project’s life span and is now available on the project’s website along with all the [public deliverables](#). The updated version of the dissemination material (brochure and roll up banner) was created in the second half of the project to promote the three Pilot Use Cases.

During the 2nd review meeting, it was suggested that IRIS should have another brochure more marketing oriented that will present its innovations and components in a clear and easy to understand manner. Therefore, a 3rd IRIS brochure, presenting the IRIS components, and a 4th IRIS brochure focused on the exploitable assets and the Service Bundles were created.

The project’s promotional material is available on the project’s [website](#) and the [Zenodo community](#) in downloadable format. In [Annex 1](#) of this document, you can find the updated IRIS roll up banner (focused on the Pilot Use Cases) and all the brochure versions (one focused on the Pilot Use Cases, one focused on the project’s components and one focused on the service bundles & the components) created since M24.

Activity	Expected KPI	Current Status M36
Dissemination material	2 brochures 3 roll up banners	4 brochures 5 roll up banners



2.3 Newsletters

Within the third year of the project (M24-M36), another two issues of the IRIS newsletter have been published ([newsletter #5](#) and [newsletter #6](#)) reaching the six (6) issues in total. The newsletters are sent to the people that have registered through the [website](#), they are circulated through the social media and they are available both on the [website](#) and the [Zenodo community](#). Beside the IRIS newsletters, the project has also contributed to the five (5) Secure Cyber Cluster newsletters which are also available on the IRIS [website](#).

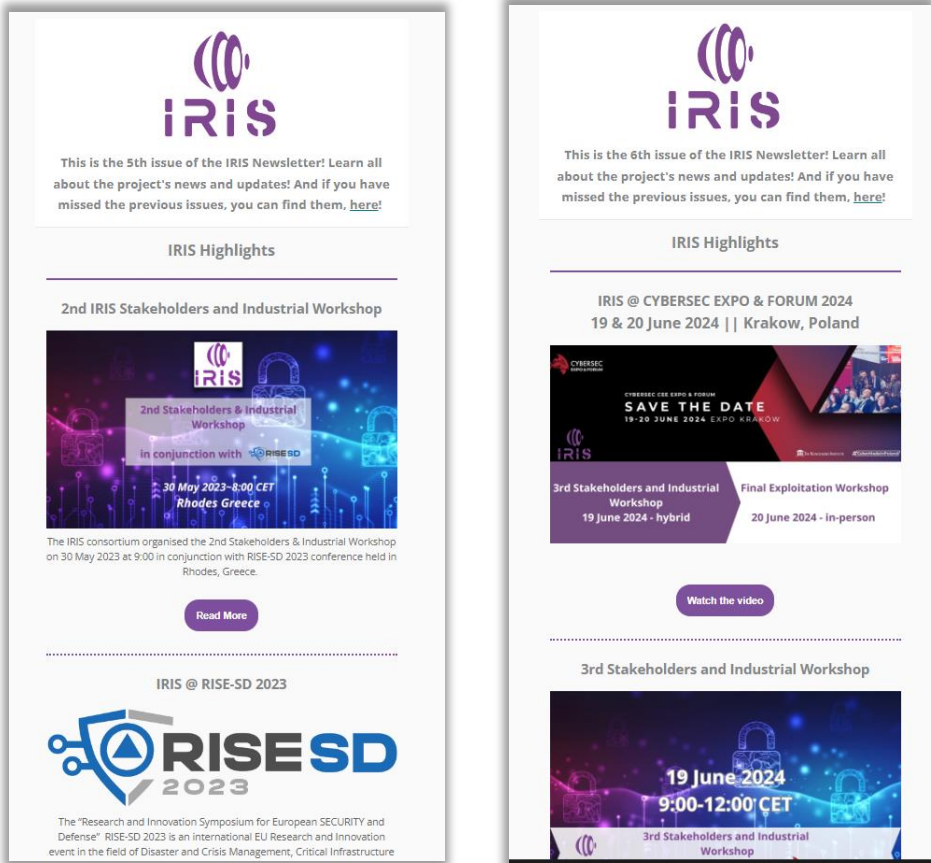


Figure 7: Newsletters No 5 & 6

Activity	Expected KPI	Current Status M36
Newsletters	6 e-newsletters	11 e-newsletters (6 IRIS e-newsletters, 5 joint newsletters with Cyber Secure Cluster)

2.4 Press Releases & Press Activities

During the second half of the project three press releases were published. One describing the joint activities performed within the Secure Cyber Cluster and two describing the first and second successful rounds of the project's Pilot Use Cases' realisation. Also, [ERCIM News](#) hosted an article about IRIS in the special Issue: "Sustainable Cities" (July 2024) under the title "[Beyond the Tech: Why Social Acceptance Matters for Smart Cities' Cybersecurity](#)". All the press activities and press releases are available on [the Media section](#) of the IRIS website.



Figure 8: IRIS press releases (3rd year)

Activity	Expected KPI	Current Status M36
Press releases	6 press releases	6 press releases (+ 4 republications + 11 press clippings based on the press releases)
Press activities	3 media appearances	5 media appearances

2.5 Videos

A general IRIS video depicting the project's aim and the solutions in a simple yet informative way was created to promote the project. The project is available on the project's [YouTube channel](#) and [website](#) and was communicated through the project's and partners' social media and websites.



Figure 9: Screenshot from the IRIS general video



2.6 Events

IRIS participated in several events and conferences in the 3rd year of the project lifespan. Consortium representatives have networked and engaged with relevant stakeholders, as well as presented some of the core objectives of the project. The events concerning the 1st year of the project are available in the deliverable D8.3 Initial report on dissemination, communication, standardisation and exploitation, those of the 2nd year are presented in the deliverable D8.4 Interim report on dissemination, communication, standardisation and exploitation. The table below presents in short, a list with the events of the 3rd project's year. All the events are also available on the IRIS [website](#) in detail:

Partner	Date	Activity	Website
INTRA	20-21 September 2023	Project presentation	1st Annual Conference on Critical Infrastructure Resilience
UPC	25-29 September 2023	Paper presentation	CPS4CIP 2023
INOV	16-17 October 2023	Project presentation, clustering activity	Joint Cluster Meeting “Cyber Security and Data Protection Synergies”
TUD, INOV	1-3 November 2024	Paper presentation	22nd IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom-2023)
CERTH	30 Nov- 1 Dec 2023	Project presentation	CONVERGENCE 2023
INTRA	5 December 2023	Project presentation, clustering activity	Collaborative Standardization and Policy Making For Greater CI Resilience in Europe Workshop



Partner	Date	Activity	Website
ATOS	12 January 2024	Project presentation, clustering activity	Security Services for Connected Devices Workshop
INTRA, CERTH, ICCS	6 March 2024	Project presentation, clustering activity	CTI Workshop
TalTech	25-27 March 2024	Paper presentation	ASD - Initiative on Autonomous Systems Design DATE 2024
KEMEA	24 May 2024	Project presentation	Geneva Centre for Security Policy's Critical Incident Management Course.
TUD	27-31 May 2024	Paper presentation	IEEE International Conference on Blockchain and Cryptocurrency - ICBC 2024
INOV	19-20 June 2024	Booth	CYBERSEC EXPO & FORUM
SID	26-28 June 2024	Paper presentation	MOCACT 2024
CEL	16-19 July 2024	Paper presentation	EASST-4S 2024 Amsterdam: Making and Doing Transformations.
ICCS	30 July 2024	Paper presentation	ARES 2024

Table 1: List of events (M24-M36)

Activity	Expected KPI	Current Status M36
Presentations in conferences	18 oral presentations	23 oral presentations (1 keynote presentation, 22 paper presentations)
Project presentations	7 project presentations	28 project presentations
Booths	3 booths or demos	5 booths



2.7 Publications

IRIS consortium partners have published peer-reviewed scientific papers in high-impact factor peer-reviewed journals and conference proceedings. The table below presents a list of the scientific papers of the third project year. All the publications, once they get published, are available on the IRIS [website](#) and the [Zenodo Community](#).

Scientific paper	Conference / event / journal	Partner	Status
Threat intelligence using Digital Twin Honeypots in Cybersecurity	IEEE-CSR 2023	SID	Published
Accelerating Blockchain Applications on IoT Architecture Models – Solutions and Drawbacks	ACM journal	TUD	Published
Towards the conception of a multi-chain to meet users' future needs: A design science research approach to digital servitization in the automotive industry	IEEE Xplore	TUD	Published
User Behavior analysis for Malware detection	CPS4CIP 2023	UPC	Published
A New Design for Self-Encryption	22nd IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom-2023)	TUD, INOV	Published
Fear of Missing Out: Constrained Trial of Blockchain in Supply Chain	MDPI	TUD	Published
ADAssure: Debugging Methodology for Autonomous Driving Control Algorithms	ASD - Initiative on Autonomous Systems Design DATE 2024	TalTech	Published
Completely FROST-ed: IoT issued FROST signature for Hyperledger Fabric blockchain	IEEE International Conference on Blockchain and Cryptocurrency - ICBC 2024	TUD	Presented / not published yet
SiHoneypot: a Digital Twin-based honeypot for Autonomous Vehicles	MOCAST 2024	SID	Presented / not published yet
Acceptance and acceptability – challenges and opportunities for	EASST-4S 2024 Amsterdam: Making and Doing Transformations	CEL	Presented / not published yet



Scientific paper	Conference / event / journal	Partner	Status
transformative and sustainable technologies			
A SOAR platform for standardizing and automating operational processes among IoT trustworthy environments	ARES 2024	ICCS	Presented / not published yet
A Comprehensive Survey of Manual and Dynamic Approaches for Cybersecurity Taxonomy Generation	Knowledge and Information Systems (Springer)	CERTH	Submitted

Table 2: List of the project's publications (M24-M36)

Activity	Expected KPI	Current Status M36
Journal Publications/ Conferences Proceedings	3 scientific papers	27 scientific publications (21 papers conference proceedings, 4 paper published in scientific journals 1 submitted in a journal, expecting approval soon)

2.8 Workshops

2.8.1 3rd Stakeholders and Industrial Workshop

The 3rd Stakeholders and Industrial Workshop was held successfully on 19 June 2024 in conjunction with the CYBERSEC EXPO and FORUM in Krakow, Poland. More details are presented in [chapter 5](#) of this document.

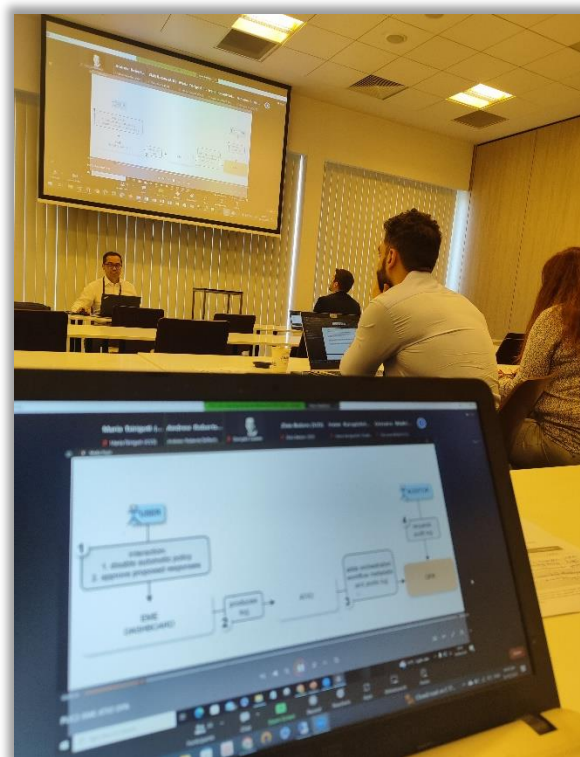


Figure 10: 3rd IRIS Stakeholders and Industrial Workshop

2.8.2 Final Exploitation Workshop

The IRIS Final Exploitation Workshop was held physically in conjunction with CYBERSEC FORUM & EXPO in Krakow, Poland on 20 June 2024. The workshop presented valuable insights into the complexities of incident reporting, the crucial functions of SOC's, and the strategic advantages of cross-border information sharing. The agenda and all the information about the Final Exploitation Workshop can be found either on the [event's website](#) or on the [project's website](#).

All the relevant activities about community building and liaison activities with relevant stakeholders that are also under T8.5 and led by ECSO, like the organization of the IRIS Final Exploitation Workshop, are presented in detail in the public deliverable D8.8 Report on connection with stakeholders that will be also be submitted in M36.



Figure 11: IRIS Final Exploitation Workshop

2.9 Other Activities

2.9.1 IRIS Tools Video Campaign

During the third project year, IRIS launched a video campaign so that we could engage even more people and promote the work performed within the project. The IRIS Tools video campaign includes simple short videos presenting the project's tools. The videos are available on the project's [YouTube channel](#) and the [website](#).



Figure 12: IRIS Tools Video Campaign

2.9.2 IRIS Blog

IRIS partners had committed to contribute to the project's blog so that the project's progress and the consortium work could be communicated to the IRIS target audiences. The IRIS blog was updated almost every two months with informative yet easy-to-read articles. The 25 blog articles are available on the [website](#).

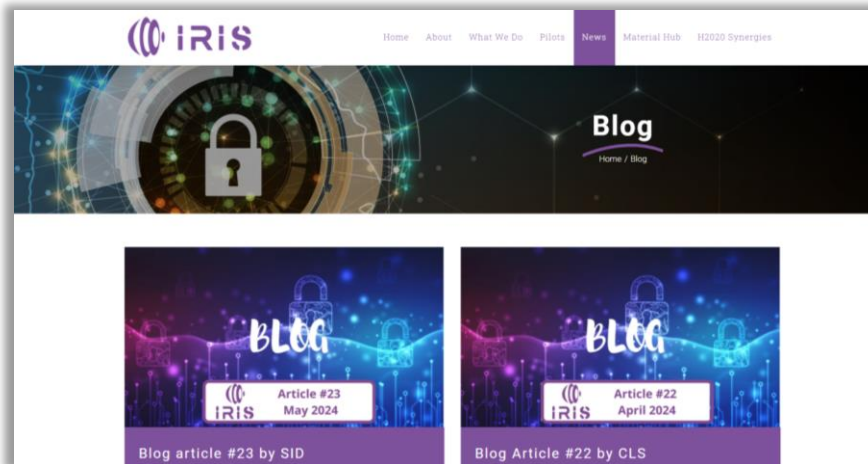


Figure 13: IRIS blog

2.9.3 IRIS Training Sessions

Two training sessions were organized and performed by IRIS consortium partners in order to inform trainees about the IRIS platform and innovations. The 1st training session was held in May 2024 at the CISCO Madrid Innovation Center, where an overview of the project and details of the project's Pilot Use Case 1 were presented and the 2nd was held on 24 July 2024 in THALES premises with the participation of 15 participants who were presented the PUC3 scenario and how the VCR is working.

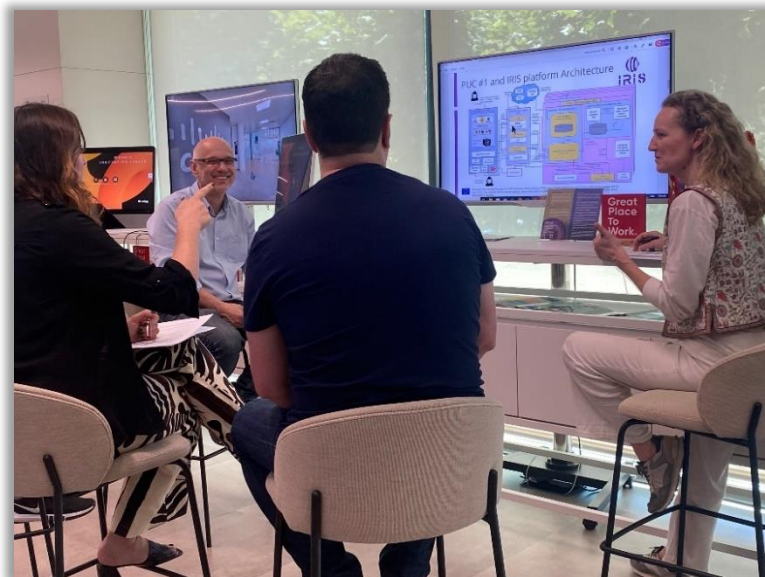


Figure 14: Training session at Cisco Madrid Innovation Center

2.9.4 IRIS Pilot Use Cases

IRIS has completed its three Pilot Use Cases (PUCs) in two rounds. The first held in March 2024 and the second in June 2024. The three project PUCs were fully supported in terms of communication and dissemination. The dissemination material was updated with information about the PUCs, there was a social media campaign with posts about the PUCs before and after their realization, the dedicated website sections were updated and finally two press releases were published.



Figure 15: IRIS PUCs



3 KEY PERFORMANCE INDICATORS

Action	Expected KPI	Current Status M36
Website	5000 visitors per year	5,9 K visitors total
Social media	Twitter: 300 followers in total LinkedIn: 100 followers in total	967 followers ✓ 380 followers ✓
Dissemination material	2 brochures 3 roll up banners	4 brochures ✓ 5 roll up banners ✓
Video	1 general video	1 general video (<i>12 promo videos</i>) ✓
Press Activities	6 press releases 3 media appearances	6 press releases ✓ 4 media appearances ✓
E-newsletters	6 e-newsletters	11 newsletters ✓ (<i>6 IRIS issues, 5 Secure Cyber Cluster issues</i>)
Journal Publications/ Conferences Proceedings	3 scientific papers	27 scientific publications ✓ (<i>21 papers conference proceedings & 4 paper published in scientific journals</i>)
Conferences/Events	<ul style="list-style-type: none"> 18 oral presentations in conferences 7 project presentations 3 booth demonstrations 	<ul style="list-style-type: none"> 23 oral presentations ✓ (<i>1 keynote speech, 22 paper presentations</i>) 28 project presentations ✓ 5 booths ✓
Training	<ul style="list-style-type: none"> 3 training sessions 2 MSc & 4 PhD students' supervision 	<ul style="list-style-type: none"> 2 training sessions 2 MSc & 5 PhD students' supervision ✓
Project code repository	2 contributions to open source projects	In progress
International Standards	2 standards contributions	2 identified potential contributions (CACAO OASIS and Smart Cities architecture)
Workshops/Webinars	3 workshops & 3 webinars	11 workshops/webinars ✓ (<i>3 Stakeholders & Industrial Workshops, 1 Advisory board Workshop, 1 Validation Workshop, 1 Launch event, 1 Final Exploitation Workshop, 4 Cluster Workshops</i>)

Table 3: IRIS KPIs



4 EXPLOITATION ACTIVITIES FROM M24 UNTIL M36

The IRIS exploitation team, along with project partners, performed several exploitation activities from M24 to M36 of the project, with a view to delivering concrete results and forming a strategy on how the various Key Exploitable Results (KER) of the project will be commercialized or will be used for further research purposes. The various activities performed are analyzed in further detail in the sub-sections that follow.

In summary, the key exploitation activities performed these months are:

- Identification of the Final IRIS list of Key Exploitable Results (KER), presented in detail in Section 4.1.
- Identification of the IRIS Results Ownership List (ROL - in alignment with the IRIS IPR Management Strategy), presented in detail in Section 4.1.
- For each of the KER, the target markets, value proposition, TRL, exploitation strategy and path, licensing, delivery model, pricing and time-to-market have been identified and described, in Section 4.1 of this deliverable, as well as in further detail in D8.6.
- The latter, helps IRIS partners to have a clear exploitation strategy per KER, meaning that for each KER the project identified (i) who is going to exploit the result, (ii) who can use the result and what concrete benefits can get out of this result, (iii) how the result will be delivered to its stakeholder groups, via which channel, (iv) what are the conditions of using the result and how the results will be marketised to engage stakeholders in using the IRIS KER.
- An exploitation strategy for the integrated IRIS cybersecurity platform has been developed. The platform will be offered to the market via 4 service bundles, each of one addressing specific technical segments of the IRIS architecture.
- An updated market analysis has been performed, investigating the market niche of the IRIS platform, and focusing on the segments of IoT and AI cybersecurity solutions, trends and needs, as well as analysing the pertinent competition. We also analyse the segment of the existing CERT/CSIRT teams and critical infrastructure operators in the EU who could use the IRIS KER.
- The exploitation strategy of the Service Bundles was also supported and validated by an expert of the [Horizon Results Booster](#) services, from which IRIS received valuable support. In summary, 2 exploitation workshops were organized (lasting 3 hours each), which were managed by the HRB expert and the exploitation leader of IRIS (INTRA), along with the participation of most project partners, and the owners of the service bundles. The scope of these workshops was to design and validate the final exploitation strategy and business models of the IRIS service bundles, based on a tailored methodology and predefined templates. The exploitation seminars with the HRB were organized in two consecutive days, on:
 - 27th of June, 2024, where the HRB expert introduced some aspects of exploitation strategies and terms in Horizon Projects and then partners discussed the business models of the Autonomous Threat Analytics (ATA) service Bundle.



- 28th of June, 2024, were the HRB expert and the exploitation leader facilitated discussions to design the business plans of the Enhanced MeliCERTes Ecosystem (EME) and the Virtual Cyber-range (VCR) service bundles.
- Detailed business plans and delivery models for the IRIS Platform Service Bundles have been created addressing the problem each bundle solves, tailored market research, unique selling points and value propositions, background and foreground IP, alternative solutions and competition analysis, as well as the models for going to the market and the use models (presented in D8.6).
- The IRIS Exploitation Workshop was organized as part of the [Cybersec Expo & Forum](#) in Krakow, Poland on the 20th of June 2024. During the workshop, the IRIS marketable results and the service bundles were presented to various stakeholders to enhance their adoption and promote their exploitation after the end of the project. Stakeholder groups that were engaged involve CISOs, CERT experts, owners of start-ups and small businesses, as well as operators of smart infrastructures in the EU.
- To enhance the visibility of the IRIS service bundles and provide concrete channels of engagement with potential stakeholders and customers, IRIS will use the [Horizon Results Platform](#) to promote the service bundles, while the EME service bundle will be an opensource project with dedicated Github page to engage the broader community of EU CERTs/CSIRTs.

More information and details on the exploitation activities and their outcomes, as well as the detailed exploitation strategy of IRIS, and the business plans per IRIS service bundle is provided in **D8.6 “Market analysis, roadmapping and business modelling report”**, which is a confidential report.



4.1 List of IRIS Key Exploitable Results

During the last months of IRIS, the final list of the marketable assets of the project, namely the Key Exploitable Results have been identified, along with the owner(s) of these results, in alignment with the IRIS management strategy of Intellectual Property. In total, 21 marketable assets have been identified as presented in the sub-sections that follow. We also analyse their target stakeholders, value proposition and time-to-market.

4.1.1 KER #1: Social Acceptance Framework

Name	Social Acceptance Framework
Owner(s)	CEL (Individual exploitation)
Description	Evaluates technology acceptability across six dimensions using questionnaires and sentiment analysis.
Target Stakeholders	Chief Information Security Officers, National CERTs/CSIRTs, National Authorities.
Value proposition	Increases the likelihood of successful technology adoption by ensuring alignment with social acceptance criteria.
Time-to-market	Less than 1 year after the end of the project

4.1.2 KER #2: Risk and vulnerability assessment module

Name	Risk and vulnerability assessment module
Owner(s)	ATOS, CEA (Joint exploitation)
Description	Identifies and analyzes vulnerabilities and potential risks in infrastructures using IoT and AI.
Target Stakeholders	CSIRT/CERT teams, Critical infrastructure operators, Companies needing cybersecurity products
Value proposition	Provides a comprehensive and proactive approach to identifying and mitigating vulnerabilities.
Time-to-market	1 to 2 years after the end of the project

4.1.3 KER #3: AI threat analytics and detection engine

Name	AI threat analytics and detection engine
Owner(s)	CLS, SID, CEA (Joint exploitation)
Description	Enhances threat detection systems for IoT and AI using machine learning anomaly classifiers.



Name	AI threat analytics and detection engine
Target Stakeholders	CSIRT/CERT teams, Critical infrastructure operators, SOCs
Value proposition	Enhances the detection and mitigation of sophisticated threats through advanced analytics.
Time-to-market	Less than 1 year after the end of the project

4.1.4 KER #4: Risk-based response and self-recovery

Name	Risk-based response and self-recovery
Owner(s)	CLS (individual exploitation)
Description	Uses game-theoretic strategies for optimal threat response and supports self-recovery policies.
Target Stakeholders	CSIRT/CERT teams, Critical infrastructure operators, SOCs
Value proposition	Provides an intelligent approach to threat response and self-recovery.
Time-to-market	1 to 2 years after the end of the project

4.1.5 KER #5: Digital twin honeypot detection models

Name	Digital twin honeypot detection models
Owner(s)	SID
Description	Uses digital twins for IoT and AI to analyze and predict threats through AI algorithms.
Target Stakeholders	Organizations seeking enhanced threat detection capabilities.
Value proposition	Enhances threat detection and predictive analysis using innovative digital twin technology.
Time-to-market	1 to 2 years after the end of the project



4.1.6 KER #6: IRIS-enhanced MeliCERTes platform

Name	IRIS-enhanced MeliCERTes platform
Owner(s)	INTRA
Description	Extends a secure platform for threat intelligence and incident sharing with enhanced features.
Target Stakeholders	CERTs/CSIRTs in the EU, Critical infrastructure operators, SOCs
Value proposition	Enhances incident response through secure, standardized threat intelligence sharing.
Time-to-market	Less than 1 year after the end of the project

4.1.7 KER #7: APIs for advanced threat intelligence orchestrator

Name	APIs for advanced threat intelligence orchestrator
Owner(s)	ICCS (individual exploitation)
Description	Integrates components for cyber-incident detection, reporting, and response.
Target Stakeholders	CERTs/CSIRTs in the EU, Critical infrastructure operators
Value proposition	Streamlines threat intelligence orchestration and incident response through advanced APIs.
Time-to-market	Less than 1 year after the end of the project

4.1.8 KER #8: Collaborative threat intelligence sharing and storage

Name	Collaborative threat intelligence sharing and storage
Owner(s)	CERTH (individual exploitation)
Description	Connects platform components and repositories for collaborative threat intelligence sharing.
Target Stakeholders	CERTs/CSIRTs in the EU, Critical infrastructure operators
Value proposition	Facilitates efficient and secure threat intelligence sharing.
Time-to-market	Less than 1 year after the end of the project



4.1.9 KER #9: DLT-based control services for accountability, traceability, and auditing

Name	DLT-based control services for accountability, traceability, and auditing
Owner(s)	INOV, TUD (joint exploitation)
Description	Uses DLT for secure threat intelligence with immutable event logging.
Target Stakeholders	Financial institutions, Healthcare providers, Critical infrastructure operators, Cybersecurity authorities
Value proposition	Ensures secure and immutable logging and auditing for enhanced accountability.
Time-to-market	Less than 1 year after the end of the project

4.1.10 KER #10: IRIS secure crypto functions for data management

Name	IRIS secure crypto functions for data management
Owner(s)	INOV, TUD (joint exploitation)
Description	Employs advanced encryption techniques to protect ICT data from network attackers.
Target Stakeholders	Financial institutions, Healthcare providers, Critical infrastructure operators, Cybersecurity authorities
Value proposition	Provides robust data protection through advanced cryptographic techniques.
Time-to-market	Less than 1 year after the end of the project

4.1.11 KER #11: IRIS cybersecurity exercises and training scenarios

Name	IRIS cybersecurity exercises and training scenarios
Owner(s)	KEMEA (individual exploitation)
Description	Includes virtual exercises with red and blue teams to enhance cybersecurity skills.
Target Stakeholders	CERTs/CSIRTs, Critical infrastructure operators, SOC's
Value proposition	Enhances cybersecurity skills through practical, scenario-based training.
Time-to-market	Less than 1 year after the end of the project



4.1.12 KER #12: IRIS Lab Pods

Name	IRIS Lab Pods
Owner(s)	THALES, CLS, CERTH, ICCS, KEMEA (joint exploitation)
Description	Standalone pod versions for testing, validation, and training in the VCR environment.
Target Stakeholders	CERTs/CSIRTs, critical infrastructure operators, SOCs
Value proposition	Provides flexible testing and training environments for cybersecurity measures.
Time-to-market	Less than 1 year after the end of the project

4.1.13 KER #13 : IRIS cyber range environment platform

Name	IRIS cyber range environment platform
Owner(s)	THALES (individual exploitation)
Description	A virtual platform for collaborative CERTs/CSIRTs training with multiple user support.
Target Stakeholders	CERTs/CSIRTs, critical infrastructure operators, SOCs
Value proposition	Provides a realistic environment for training and testing cybersecurity response strategies.
Time-to-market	Less than 1 year after the end of the project

4.1.14 KER #14: IRIS smart city IoT and control system pilot

Name	IRIS smart city IoT and control system pilot
Owner(s)	IMI (individual exploitation)
Description	Monitors IoT control systems and gateways to detect and report threats in urban environments.
Target Stakeholders	Smart city operators, urban infrastructure managers, CERTs/CSIRTs
Value proposition	Enhances the security of urban IoT systems against cyber threats.
Time-to-market	N/A



4.1.15 KER #15: IRIS smart city autonomous transport system pilot

Name	IRIS smart city autonomous transport system pilot
Owner(s)	Taltech (individual exploitation)
Description	Protects autonomous vehicle infrastructure from cyberattacks, identifying breaches and sharing signatures.
Target Stakeholders	Smart city transport operators, autonomous vehicle manufacturers, CERTs/CSIRTs
Value proposition	Ensures the security and reliability of autonomous transport systems.
Time-to-market	N/A

4.1.16 KER #16: IRIS cross-border smart grid pilot

Name	IRIS cross-border smart grid pilot
Owner(s)	FVH (individual exploitation)
Description	Reduces risks in smart grid components through anomaly detection and threat data sharing.
Target Stakeholders	Smart grid operators, Energy sector stakeholders, CERTs/CSIRTs
Value proposition	Enhances the security and resilience of cross-border smart grid systems.
Time-to-market	Less than 1 year after the end of the project

4.1.17 KER #17: Integrated IRIS Platform

Name	Integrated IRIS Platform
Owner(s)	INTRA, ATOS, CEA, CLS, SID, THALES, KEMEA, LCCS, CERN
Description	The full version of the IRIS cybersecurity platform integrating advanced threat detection, encryption, and DLT technologies.
Target Stakeholders	Critical infrastructure operators in the EU, CERT/CSIRTs
Value proposition	Offers a holistic approach to cybersecurity by integrating multiple advanced tools.
Time-to-market	Less than 1 year after the end of the project



4.1.18 KER #18: Autonomous Threat Analytics (ATA) Service Bundle

Name	Autonomous Threat Analytics (ATA) Service Bundle
Owner(s)	ATOS, CEA, CLS, SID
Description	The IRIS ATA Service Bundle offers a cybersecurity solution tailored for IoT and AI systems, combining advanced capabilities in vulnerability management, binary analysis, intrusion detection, and honeypot operations. The bundle's integrated components deliver protection and response strategies, ensuring the security and resilience of complex ICT environments.
Target Stakeholders	IoT device manufacturers, AI system developers, critical infrastructure operators, cybersecurity service providers, enterprise IT departments
Value proposition	Provides comprehensive, integrated cybersecurity for IoT and AI systems, reducing vulnerability exposure and enhancing threat detection and response capabilities.
Time-to-market	Less than 1 year after the end of the project

4.1.19 KER #19: Enhanced MeliCERTes Ecosystem (EME) Service Bundle

Name	Enhanced MeliCERTes Ecosystem (EME) Service Bundle
Owner(s)	INTRA (leading the open-source project and commercialization), ICCS and CERTH (supporting the open-source project and commercialization)
Description	The IRIS Enhanced MeliCERTes Ecosystem (EME) is an open-source platform designed to facilitate secure communication, collaboration, and cyber threat intelligence (CTI) sharing among cybersecurity authorities, incident response teams, and critical infrastructure operators. It integrates various advanced tools and technologies to enhance the management of cybersecurity incidents and the structured communication of threat intelligence, thereby bolstering situational awareness and response capabilities.
Target Stakeholders	Cybersecurity authorities, CERT/CSIRT teams, critical infrastructure operators, government agencies
Value proposition	<ul style="list-style-type: none"> • Enhances collaboration and information sharing among cybersecurity stakeholders. • Improving incident response times and situational awareness. • Interoperable with most of the existing solutions in the market. • Leverages open-source tools to provide a cost-effective, flexible, and extensible platform.
Time-to-market	Less than 1 year after the end of the project



4.1.20 KER #20: Virtual Cyber Range training (VCR) Service Bundle

Name	Virtual Cyber Range training (VCR) Service Bundle
Owner(s)	THALES, KEMEA
Description	The IRIS Virtual Cyber Range (VCR) Service Bundle offers an advanced platform for immersive and realistic cybersecurity training simulations. This service bundle is specifically designed to enhance the effectiveness of cybersecurity training for both end-users and professionals by providing engaging, scenario-based exercises that simulate targeted attacks of varying complexity.
Target Stakeholders	CERT/CSIRT analysts, cybersecurity professionals, enterprise IT security teams, academic institutions offering cybersecurity programs.
Value proposition	Provides hands-on, practical training to improve technical skills, risk awareness, and process adoption. Enhances the preparedness and resilience of cybersecurity teams against evolving threats.
Time-to-market	Less than 1 year after the end of the project

4.1.21 KER #21: Add-ons Services Service Bundle

Name	Add-ons Services Service Bundle (DPA module)
Owner(s)	INOV, TUD
Description	A service that provides secure, immutable, and traceable logging and auditing functionalities, ensuring robust accountability in collaborative incident response workflows.
Target Stakeholders	Enterprises with high compliance requirements, cybersecurity service providers, incident response teams.
Value proposition	Enhances accountability and traceability in incident response workflows, supporting compliance with regulatory requirements and improving overall incident response effectiveness.
Time-to-market	Less than 1 year after the end of the project



4.1.22 KER #22: Algorithms for Adversarial Attack Detection

Name	Algorithms for Adversarial Attacks Detection
Owner(s)	CEA (individual exploitation)
Description	The MAI-GUARD tool developed by CEA has been enhanced with new algorithms and models for detecting adversarial attacks.
Target Stakeholders	Providers and/or integrators of artificial vision systems, particularly for autonomous vehicles.
Value proposition	Detection of gradient-based attacks on images.
Time-to-market	1 to 2 years after the end of the project

4.2 Exploitation Strategy of the IRIS cybersecurity platform

The IRIS cybersecurity platform integrates multiple service bundles to address diverse security challenges. With a Technology Readiness Level (TRL) of 7, it showcases a prototype platform featuring integrated cybersecurity services, demonstrated in operational environments under three distinct use cases. The platform's architecture is modular and flexible, allowing organizations to deploy individual service bundles or combinations tailored to their specific needs. This modular approach ensures that entities such as critical infrastructure operators, CERTs/CSIRTs, and national cybersecurity authorities can customize the platform to address their unique security requirements. The IRIS platform has been designed from inception to function as a threat intelligence system, capable of automated threat analytics, detection, response, and recovery. From a marketing perspective, the platform is divided into four primary service bundles: the Automated Threat Analytics (ATA) Service Bundle, the Enhanced MeliCERTes Ecosystem (EME) Service Bundle, the Virtual Cyber Range (VCR) Service Bundle, and the Add-on Services (DPA) Service Bundle. Each bundle offers distinct functionalities suited to different aspects of cybersecurity.

Service Bundle 1: The ATA Service Bundle focuses on protecting IoT and AI systems, providing advanced vulnerability management, binary analysis, intrusion detection, and honeypot capabilities. It is designed to manage risks associated with smart cities and critical infrastructures, incorporating machine learning for anomaly detection and Digital Twin Honeypots for proactive threat analysis.

Service Bundle 2: The Enhanced MeliCERTes Ecosystem (EME) Service Bundle provides a suite of integrated and interoperable functionalities targeted at critical infrastructure operators and CERT/CSIRT authorities. It combines several open-source tools, including MeliCERTes, MISP, and Shuffle, to facilitate threat intelligence sharing, operational workflow automation, and secure collaboration. This bundle acts as a central hub for information sharing and incident response, enhancing collective cyber resilience through standardized threat taxonomies and integrated CTI sharing and storage tools. It is important to note that the EME Service Bundle will be offered as an open-source project in Github, maximizing its exploitation potential and engaging further the open-source community.



Service Bundle 3: The Virtual Cyber Range (VCR) Service Bundle offers an immersive platform for realistic cybersecurity training simulations. It enables organizations to conduct scenario-based exercises, simulating targeted attacks to improve the practical skills of cybersecurity professionals. This bundle is particularly valuable for CERT/CSIRT analysts and other cybersecurity personnel, providing hands-on experience that complements theoretical training and enhances the overall effectiveness of cybersecurity training programs.

Service Bundle 4: The Add-on Services (DPA) Service Bundle delivers secure, immutable, and traceable logging and auditing capabilities. Utilizing advanced self-encryption and secret key sharing technologies, it ensures the integrity and transparency of incident response processes. This bundle is integrated with the EME platform to support secure incident response workflows, offering enhanced accountability through decentralized logging mechanisms. The DPA module will be available for European CERTs/CSIRTs at no cost, accessible via the EME GitHub page.

The IRIS platform's exploitation model offers three distinct usage options to accommodate to varying customer needs.

Usage Model 1 allows customers to exploit individual components of the IRIS platform, such as the AI threat analytics engine or Digital Twin Honeypots, on a standalone basis. This model is suitable for customers who require specific functionalities and prefer to integrate them into their existing systems.

Usage Model 2 enables customers to deploy one of the four service bundles independently, addressing specific requirements without adopting the entire platform. For instance, an electricity grid operator might opt for the ATA Service Bundle to safeguard their infrastructure.

Usage Model 3 offers the flexibility to combine multiple service bundles based on specific use cases, allowing customers to tailor their deployment for broad cybersecurity solutions. For example, a critical infrastructure operator might combine the ATA and VCR Service Bundles to enhance both threat detection and training capabilities. Each model supports tailored deployment strategies, ensuring that organizations can select and integrate the components that best align with their cybersecurity objectives.

4.3 The IRIS Exploitation Workshop as part of the Cybersec Expo& Forum in Krakow, Poland

To enhance the exploitation activities of the project and present the service bundles to key stakeholders, IRIS organized a dedicated exploitation workshop as part of [the Cybersec Expo& Forum](#) in Krakow, Poland. The IRIS Workshop was designed to highlight and explore the capabilities of the IRIS platform. It focused on demonstrating the platform's various service bundles and their practical applications in enhancing cybersecurity measures. Participants gained an in-depth understanding of how the IRIS platform integrates its service components, including Automated Threat Analytics (ATA), Enhanced MeliCERTes Ecosystem (EME), Virtual Cyber Range (VCR), and Add-on Services (DPA).

The workshop also featured **live demonstrations of the platform's functionalities**, showcasing real-world applications and the benefits of its threat analytics, incident response capabilities, and cybersecurity training simulations. Attendees were also engaged in discussions about practical use cases and success stories from the deployment of IRIS service bundles in operational environments, illustrating their impact on improving cybersecurity resilience.



Figure 16: IRIS Exploitation Workshop in Krakow, Poland



Interactive sessions provided opportunities for participants to interact with platform experts, ask questions, and explore how the IRIS platform can be customized to address specific organizational needs and challenges. Additionally, the workshop facilitated networking among cybersecurity professionals, stakeholders, and potential collaborators, promoting discussions on emerging trends and solutions in the cybersecurity field.



Exploitation Workshop Outcomes and Engagement of Stakeholders

The IRIS Workshop at the CSCE24 Cybersecurity Forum yielded significant benefits for the IRIS platform, both in terms of stakeholder engagement and feedback. The event effectively showcased the platform's diverse capabilities, leading to heightened interest from various stakeholders, including critical infrastructure operators, national cybersecurity authorities, CISOs in the EU, and cybersecurity professionals. These participants were particularly engaged by the platform's modular approach, which allows for tailored solutions to specific cybersecurity challenges, and the real-world applications demonstrated during the workshop. For instance, a specific exploitation case also arose from a municipality in Portugal, which wants to use some of the IRIS cybersecurity tools in its processes and operations, to enhance its cybersecurity posture. Discussions with IRIS partners are in place to further promote this exploitation opportunity and decide on the specific tools and service bundles of IRIS that could be used by the municipality.

In parallel, the interactive sessions facilitated valuable discussions on how the IRIS platform's service bundles could be integrated into existing security infrastructures, generating interest in potential collaborations and deployments. The workshop also provided feedback that will guide future exploitation of the IRIS platform. Comments were made regarding the platform's usability and interoperability, particularly that the IRIS integration of many technologies and cybersecurity tools is novel and that the platform benefits by using the service bundles, since it could be more easily adapted to various operational environments. Additionally, attendees highlighted the need for expanded training and support resources to maximize the platform's effectiveness. These insights will be helpful in refining the platform's exploitation strategy and ensuring it meets the evolving needs of its diverse user base, thereby strengthening its position in the cybersecurity market.

5 CLUSTERING ACTIVITIES FROM M24 UNTIL M36

5.1 Secure Cyber Cluster

The IRIS project has built strong synergies with other similar H2020 projects since its launch. EU funded projects ARCADIAN, SECANT, SENTINEL, IDUNN, ELECTRON, TRUST aWARE, SPATIAL, ERATOSTHENES and, of course, IRIS had created a Communication Task Force (CTF) which met monthly to exchange information and ideas and plan clustering activities. This CTF joint forces and got developed into a cluster with a joint logo, brand identity, social media under the title “Secure Cyber Cluster”.

5.1.1 Secure Cyber Cluster logo & brand book

After discussing it for a while and after voting among several logos, the project cluster concluded to the option that was the most popular. The logo was used in all the jointly organised activities and became the cluster’s trademark. Besides the logo, we have also created a brand book, which describes the proper use of the logo, colours and font and also explains the idea behind the Secure Cyber Cluster. The brand book is available in [Annex 2](#) of this document.



Figure 17: Secure Cyber Cluster logo

5.1.2 Secure Cyber Cluster e-newsletters

The projects’ cluster prepared and circulated five e-newsletters which included all joint activities as well as the projects’ individual activities and achievements. The e-newsletters were available on the cluster’s LinkedIn page and the projects’ websites (eg [IRIS website](#)).



Figure 18: Secure Cyber Cluster e-newsletter No 5

5.1.3 Secure Cyber Cluster LinkedIn

A dedicated [LinkedIn page](#) was created to share the joint activities and also those of each project. The page has 130 followers and many posts and reposts.



Figure 19: Secure Cyber Cluster LinkedIn page

5.1.4 Secure Cyber Cluster workshops

The cluster organized and held four joint workshops in total. Since M24 of the IRIS project, there were two jointly organized workshops: The [Joint Cluster Physical Event](#), held in Lisbon, Portugal on 16 & 17 October 2023 in which IRIS was represented by our coordinator INOV and the online [Cyber Threat Intelligence: Empowering IoT Security workshop](#), held on 6 March 2024, where the project was represented by INTRA, ICCS and CERTH. Each workshop had more than 40 participants.



Figure 20: Cluster's joint workshops

5.1.5 Secure Cyber Cluster press release and policy brief

The projects of the Secure Cyber Cluster published a joint press release to share their goals and performed activities. The press release was promoted through the projects' social media and the cluster's LinkedIn page. It is also available on [IRIS website](#), in downloadable format. A very important

joint activity was the creation of a joint policy brief that was sent to the EC representatives, after the conclusion of one of the joint workshops.



Figure 21: Screenshots of the Secure Cyber Cluster's press release and policy brief

5.2 Stakeholders and Industrial Workshops

The IRIS consortium organized the 3rd Stakeholders & Industrial Workshop on 19 June 2024 in Krakow, Poland in conjunction with the CYBERSEC EXPO & FORUM 2024. The workshop's participants had the chance to watch demonstrations of the project's solutions and tools and connect with industry professionals, stakeholders, and experts in a hybrid setting. The workshop was intended for representatives from the CERT/CSIRT community, members of the European Commission, security operators, distributors, cybersecurity service providers, cybersecurity professionals and researchers. The agenda and the project's details and logo were presented on the [event's website](#), providing a huge promotion.



Figure 22: 3rd IRIS Stakeholders and Industrial Workshop

5.3 ECSCI workshops

IRIS has been member of the European Cluster of Securing Critical Infrastructure (ECSCI) since May 2023. IRIS has participated in two workshops organized by the cluster. The [1st Annual Conference on Critical Infrastructure Resilience](#), held on 20-21 September 2023 and the [Collaborative Standardization and Policy Making for Greater CI Resilience in Europe Workshop](#), held on 5 December 2023. In both events, the project was represented by INTRA. Besides the events, ECSCI members had constant communication through emails and online meetings.



Figure 23: ECSCI workshops

5.4 Other events

IRIS participated in two workshops organized by other H2020 projects. [ERATOSTHENES “Trust and Identity Management for IoT” 2nd Workshop](#) showcased how Europe’s Research and Innovation community is addressing the issues of identity, trust, security, and privacy for IoT devices and network systems. The workshop was organized by ERATOSTHENES project as part of its 2nd formal workshop and its primal focus is on the presentation of recent technologies and outcomes as well as identification of synergies between the projects.

IRIS was among the H2020 & Horizon Europe projects that participated in a clustering workshop organised by CROSSCON project with the aim to discuss the major cybersecurity aspects in connected devices and ecosystems. The workshop “Security Services for Connected Devices”, held on 12 January 2024, was organized in conjunction with the [European Network for Cybersecurity \(NeCS\) PhD School – PhD Winter School 2024](#), hosted in Cortina d’Ampezzo (BL), on the 8th-12th of January 2024.

The projects that participated were CROSSCON, ORSHIN, SecOPERA, CERTIFY Project, ERATOSTHENES, ENTRUST, REWIRE, TRUSTaWARE, ENCRYPT Project, and CyberSEAS Project.

IRIS was represented by ATOS in both events.



Figure 24: Workshops organized by other H2020 projects



6 POLICY AND STANDARDISATION ACTIVITIES FROM M24 UNTIL M36

This section updates the analysis presented in D8.4 and it is also part of D8.7 “Report on policy recommendations”. Standards play a key role in ensuring inter-dependency and interoperability of technical solutions across different geographical regions and communities. As such, IRIS takes specific actions to ensure reference and integration of standards to ease the reuse and uptake of the tools and implemented solutions. The standardisation effort in IRIS is a joint activity with other work packages meant to analyse the standard landscape, orchestrate the cooperation with international organisations, and define a roadmap.

In previous deliverables we reported the relevant standards identified by the IRIS partners, herein briefly reminded. The IRIS platform should support existing technical standards (MISP, STIX/TAXII etc.) and processes (RFC formats for incident response reports etc.). In particular, the IRIS Platform will contain a standardised taxonomy/ontology which is mapped to widely used, e.g. existing ENISA and/or NIST taxonomies/ontologies (STIX 2.1, MISP Standards etc.). The Structured Threat Information Expression (STIX™), defined by the OASIS Cyber Threat Intelligence (CTI) Technical Committee, is a programming language and serialization format for exchanging cyber threat intelligence (CTI). STIX allows organisations to share CTI in a consistent and machine-readable manner, in a way which improves capabilities such as collaborative threat analysis, automated threat exchange, automated detection and response, and others.

In IRIS, the CTI threat analysis and sharing techniques will be driven by secure and efficient security information representation in standardised formats, e.g., STIX or JSON, being able to provide sharing mechanisms with external entities using standard. More specifically, the AI/IoT CTI relevant information, generated within WP3 cybersecurity threat/attack detection modules, will be structured in a standardised format. These standardized and secure CTI representation ontology (e.g. STIX v2.1, MISP Standards) will be considered in the IRIS Enhanced MeliCERTes platform, currently under development in WP4. The WP4 plans to develop a distributed ledger that provides dynamic accountability, auditing and traceability to threat intelligence publication, consumption and access control with self-encryption and recovery capabilities. Standards in this domain are under development by ISO/TC 307 and other technical groups such as CEN-CENELEC JTC19, ETSI ISG PDL, ITU-T Groups and IEEE¹.

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.

Below we present an update of the involvement of the IRIS partners in the standardisation committees and the relevant standards for IRIS.

¹ European Cyber Security Organisation. ECSO Technical Paper on Distributed Ledger Technologies. June 2022



IRIS partner	Standard Organisations	Technical Committee / Working Group	Standard	Relevance for IRIS
ICCS	CEN/CENELEC	TC CEN/WS DIV	Requirements for acquiring digital information from victims during search and rescue operations	
ICCS	CEN/CENELEC	TC CEN/WS DigScen	Specifications for Digital Scenarios for Search and Rescue Exercises	
IMI	UNE	CTN178	Several with focus on Smart Cities ICT Architectures and in particular 178104	Cybersecurity modules in Smart City Platform
SID	ISO/IEC	TS 27008:2019	"information security management systems controls"	Relevant for WP3/T3.2/SiVi Risk-based selection is utilised for security management. As a consequence, the information risk management provided by the tool is enchanting.
SID	ISO/IEC		27032:2012	Relevant for WP3/T3.2/SiVi SiVi can manage many types of data, including cybersecurity events, and it follows the instructions to improve the status of cybersecurity and the services it delivers. SiVi bolsters the security domains, including information security, network security, internet security, and protection of vital information infrastructure, by these actions.
SID	ISO/IEC		27034-5:2017	Relevant for WP3/T3.2/SiVi Throughout the Systems Development Life Cycle, precise



IRIS partner	Standard Organisations	Technical Committee / Working Group	Standard	Relevance for IRIS
				direction was provided for the development of the tool (SDLC)
SID	ISO/IEC		27035-1:2016	<p>Relevant for WP3/T3.2/SiVi</p> <p>SiVi's approach to security was impacted by ISO/IEC 27035-1:2016, including basic ideas linked to information security management, efficient incident response, effective detection of information security events, and suitable assessment of such occurrences. ISO/IEC 27035-2:2016 was used to plan the tool's incident response function. SiVi and its sensors provide a full Intrusion Detection System (IDS) that follows ISO/IEC 27039:2015 for deployment and operating guidelines.</p>
SID	ISO/IEC		27042:201	<p>Relevant for WP3/T3.2/SiVi</p> <p>Security incidents require additional analysis to interpret, identify, or collect information. SiVi follows ISO/IEC 27042:2015, ISO/IEC 27037:2012, and ISO/IEC 27043:2015 for digital evidence gathering and preservation.</p>
ICCS	N/A	Network Working Group	IETF HTTP standard	<p>Relevance for WP4: T4.3-Advanced Threat Intelligence Orchestrator.</p> <p>HTTP functions as a request-response protocol in the client-server model. Moreover, is an application layer protocol designed within the framework of the Internet protocol suite. Its definition presumes an underlying and reliable transport layer protocol</p>
ICCS	N/A	ECMA-404, ISO/IEC 21778:2017, IETF STD 90 RFC 8259	JSON Data Interchange Standard. JSON Schema	<p>Relevance for "WP4: T4.3-Advanced Threat Intelligence Orchestrator" and "WP6: T6.1- APIs for integration with the smart city's IoT- and AI-enabled infrastructures".</p>



IRIS partner	Standard Organisations	Technical Committee / Working Group	Standard	Relevance for IRIS
				<p>JSON (JavaScript Object Notation) is a lightweight, text-based, language-independent syntax for defining data interchange formats. JSON Schema is a vocabulary that allows you to annotate and validate JSON documents, says json-schema.org. A language and platform agnostic tool, JSON describes a set of constraints for interaction between JSON documents. Since JSON is a common REST API data format, JSON Schema has been growing in use and importance.</p>
ICCS	N/A	Technical Steering Committee (TSC), Technical Oversight Board ("TOB")	OpenAPI Specification (OAS)	<p>Relevance for "WP6: T6.1- APIs for integration with the smart city's IoT- and AI-enabled infrastructures"</p> <p>The OpenAPI Specification (OAS) defines a standard, language-agnostic interface to HTTP APIs which allows both humans and computers to discover and understand the capabilities of the service without access to source code, documentation, or through network traffic inspection.</p>
UPC	MISP Standard		https://www.misp-standard.org/standards/	<p>Relevance for WP4</p> <p>It is necessary for the exchange of information with different CERTs that the project needs</p>
UPC	ENISA		https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool/results#Smart%20Cities	<p>Relevance for WP7</p> <p>Good practices for IoT infrastructures, smart cities</p>



IRIS partner	Standard Organisations	Technical Committee / Working Group	Standard	Relevance for IRIS
UPC	MITRE		https://attack.mitre.org/	Relevance for WP7 Possibility to use some of the techniques defined here to perform some of the attacks on the pilots
CERTH	ISO		ISO/IEC/IEEE 29119-1:2022: Software Testing	Relevance for WP3, WP4, and WP5. To test the developed components
CERTH	ISO		ISO/IEC 27001:2013 — Information security management	Relevance for WP3, WP4, and WP5. To secure any kind of digital information
CERTH	ISO		ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls	Relevance for WP4/T4.1, T4.2/CTI Sharing and Storing To collect and analyse information relating to information security threats.
TUD	Hyperledger Foundation an open source project from the Linux Foundation		Hyperledger Fabric	Relevant for WP4 – DPA. Provides the distributed ledger software (standard for enterprise blockchain)
TUD	SAFE NETWORK	MaidSafe	Self-Encryption	Relevant for WP4 – DPA. Provides the robust encryption of the data
TUD	ISO/IEC 19592-2:2017		Secret sharing	Relevant for WP4 – DPA. Provides the basic principles of secret sharing.
CISCO	ISA/IEC	ISA99/IEC6 2443	Security for industrial automation and control systems	Cisco Cybervision which is part of the infrastructure of PUC1 in WP7 allows to implement ISA/IEC 62443 by providing asset visibility, defining zones and conduits and assigning controls to zones. As described here:



IRIS partner	Standard Organisations	Technical Committee / Working Group	Standard	Relevance for IRIS
				https://blogs.cisco.com/security/it-and-ot-cybersecurity-united-we-stand-divided-we-fall?dtid=oblqcdc000651
CLS	ISA/IEC	ISA99/IEC 62443	Security for industrial automation and controls systems	CLS's Nightwatch which is part of the infrastructure of PUC1 aligns to and supports the implementation of the ISA/IEC 62443 by providing OT & IoT asset visibility as well as AI monitoring, threat detection and response for industrial systems.
INTRA	ISO	ISO/IEC/IE EE 29119-1:2022	Software Testing	Relevance for WP6 To test the developed components and integrated IRIS platform
INTRA	ISO	ISO/IEC 27001:2013	Information security management	Relevance for WP4, and WP6. To secure any kind of digital information
INTRA	ISO	ISO/IEC 27002:2022	Information security, cybersecurity and privacy protection — Information security controls	Relevance for WP4/T4.7, WP6 and WP7 To collect, manage and share information relating to information security threats.
INTRA	MISP Standard	CIRCL, MISP Community	https://www.misp-standard.org/standards/	Relevance for WP4 and WP6 CTI information exchange with different CERTs/EME deployments
INTRA	STIX 2.1	OASIS Open	https://oasis-open.github.io/cti-documentation/stix/intro.html	Relevance for WP3, WP4 and WP6 Standardized description of detected threats, vulnerabilities, attacks (CTI information) and interoperable exchange within/across IRIS platform



IRIS partner	Standard Organisations	Technical Committee / Working Group	Standard	Relevance for IRIS
INTRA	CACAO security playbooks	OASIS Open	https://docs.oasis-open.org/cacao/security-playbooks/v2.0/security-playbooks-v2.0.html	Relevance for WP3, WP4 and WP6 Standardized description of response actions and interoperable exchange within/across IRIS platform
ICCS	MISP Standard	CIRCL, MISP Community	https://www.misp-project.org/openapi/	Relevance for WP3, WP4, Usage of the MISP OPEN API for establishing communication between ATIO and MISP of CTI module

Table 4: Standards and the relevance for IRIS

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

Standard Organisations	Technical Committee / Working Group	Standard	Why this is relevant ?	Usage in WP / Task / Component
OASIS	OASIS Cyber Threat Intelligence (CTI) Technical Committee.	Structured Threat Information Expression (STIX™)	STIX is a programming language and serialisation format for exchanging cyber threat intelligence (CTI). Allows organizations to share CTI in a consistent and machine-readable manner, in a way which improves capabilities such as collaborative threat analysis, automated threat exchange, automated detection and response, and others.	Related with WP4 in total and the total scope of the project.



Standard Organisations	Technical Committee / Working Group	Standard	Why this is relevant ?	Usage in WP / Task / Component
ISO/IEC JTC 1	SC 42 has established the five working groups of Foundational Standards (WG 1), Big Data (WG 2), Trustworthiness (WG 3), Use Cases and Applications (WG 4), and Computational Approaches and Computational Characteristics of AI Systems (WG 5)	AI standardization.	The SC 42 WG 3 Trustworthiness Working Group is concerned with AI's dependability and ethics. It has conducted research and development on AI credibility, robustness evaluations, algorithm bias, and ethics, among other areas.	WP3
ISO/IEC TR 24027 Information technology		Artificial Intelligence (AI) — Bias in AI systems and AI-aided decision making	It focuses mostly on algorithmic bias in AI systems and AI-assisted decision systems.	WP3
ISO/IEC TR 24368:2022		TR Information Technology — Artificial Intelligence — Overview of Ethics and Social Concern	It focuses on AI research from the ethical and social aspects.	WP3
ISO/IEC/IEEE 29119-11		Software and Systems Engineering — Software Testing — Testing of AI-Based System	It intends to standardise testing of artificial intelligence systems.	WP3
OASIS Open		CACAO: Collaborative Automated Course of Action Operations for Cyber Security	It could be relevant to Task 3.3 to potentially establish standardised response actions within the risk-based response and self-recovery	WP3, WP4, WP6



Standard Organisations	Technical Committee / Working Group	Standard	Why this is relevant ?	Usage in WP / Task / Component
			module based on CACAO or to support the Permissible Actions Protocol (PAP).	
UNE	Spanish agency of normalisation	CTN178	Several with focus on Smart Cities ICT Architectures and in particular 178104	WP7

Table 5: Well established, used or under development standards

6.1 Potential contribution to standards

OASIS CACAO

With respect to OASIS CACAO the project has identified potential gaps and extension to the standard.

Based on the experience utilizing the CACAO standard within the IRIS project, one notable area for potential extension is the execution capability of the CACAO playbook. While the standard does mention the concept of an "executable playbook", which should be immediately actionable within an organization's security infrastructure without necessitating modifications or updates to the workflow and commands, the project partners have encountered issues in utilizing this capability.

As such, when deploying the response_API, the RRR module necessitates the use of an external bash script for executing the response workflow reported in the generated CACAO playbook. This introduces a dependency on external tools and adds complexity to the process. The project partners believe that enhancing the CACAO standard to incorporate advanced execution capabilities directly within the playbook itself, would significantly streamline any deployment process.

For the CACAO standard, the project sees the contribution mostly a recommendation that can be seen as "lessons learnt" still having an impact and still potentially benefitting the broader CACAO community.

Smart Cities' System Architecture

Another potential contribution refers to the ITUY4000 family and CTN178104 standards that define systems architecture for Smart Cities. The contribution will come mostly from the IRIS modules in Smart Cities System Architecture and could be potentially done via the UNE national organisation



7 CONCLUSION

The current document delivers a complete overview of the dissemination, communication, standardisation and exploitation activities that have been conducted during the last year of IRIS.

The document presented an overview of the activities relating dissemination and communication of the project performed in the third year of the project, the exploitation and business modelling activities of IRIS project implemented, all the clustering and liaising activities held with relevant stakeholders and similar H2020 projects in the past 12 months and the work performed regarding the standardisation activities in the last project year.

The high performance of the dissemination, communication, standardisation, and exploitation activities demonstrates a fruitful and productive last project year, setting the conditions for the successful market exploitation of the project.

8 ANNEXES

8.1 Annex 1: Updated Dissemination Material



Figure 25: 2nd IRIS brochure (Cover)_ Pilot Use Cases

IRIS Vision

IRIS project aims to deliver a framework that will support European CERT and CSIRT networks detecting, sharing, responding and recovering from cybersecurity threats and vulnerabilities of IoT and AI-driven systems.

Project Facts


Duration: 36 months (September 2021-August 2024)
EU funding: 4 918 790.00

Pilots:
#1 **Barcelona**, Spain
#2 **Tallinn**, Estonia
#3 **Helsinki**, Finland and **Tallinn**, Estonia

Project Coordinator:
INOV - Instituto de Engenharia de Sistemas e Computadores, Inovacao, (INOV), Portugal

Pilot Use Cases

Pilot Use Case #1



Securing the smart city's IoT and control systems against confidentiality & integrity breaches

Focus: Securing the IoT and control system infrastructure deployed in a tramway station against confidentiality and integrity breaches.


Place: Barcelona, Spain

Expected outcomes:

- Safer environment where tramways, pedestrians and bikes may coexist safely
- Less safety issues and accidents stemming from man-made cyber-attacks

End Users: CERTs/CSIRTs, transport operators

Pilot Use Case #2



Securing AI-enabled infrastructure of autonomous transport systems in a smart city

Focus: Protection of the AI-enabled infrastructure of the autonomous transport system (AV shuttle and the Remote Operation Centre) available in Tallinn against potential orchestrated attacks.


Place: Tallinn, Estonia

Expected outcomes:

- Minimization of the impact of the attack by identifying the threat, self-recovering from it and sharing the corresponding intelligence with other related system operators and platforms
- Assisting system operators to identify if specially crafted data, designed to confuse AI-based decision making, (e.g., spoofed/fuzzed) are received from onboard vehicle sensors, or injected directly to APIs

End Users: CERTs/CSIRTs, CI security operators

Pilot Use Case #3



Effective incident response and threat intelligence collaboration for critical cross-border smart grid threats

Focus: Education of CERTs/CSIRTs on effective incident response and threat intelligence collaboration in cross-border cyber-attacks.

Place: Tallinn, Estonia and Helsinki, Finland

Expected outcomes:

- Safer services and more protected components of the smart grid to the building residents
- Better decision-making for the energy operators
- Secure energy infrastructure

End Users: CERTs/CSIRTs, Energy infrastructure stakeholders

Figure 26: 2nd IRIS brochure (Inside)_ Pilot Use Cases

IRIS

@iris_h2020
 IRIS H2020 Project
 @IRIS_H2020
 IRIS H2020 Project

coordinator@iris-h2020.eu
 www.iris-h2020.eu

IRIS Vision

IRIS project aims to deliver a framework that will support European CERT and CSIRT networks detecting, sharing, responding and recovering from cybersecurity threats and vulnerabilities of IoT and AI-driven systems.

Project Facts

Duration: 36 months (September 2021-August 2024)

EU funding: 4 918 790.00

Pilots:

- #1 **Barcelona**, Spain
- #2 **Tallinn**, Estonia
- #3 **Helsinki**, Finland and **Tallinn**, Estonia

Project Coordinator:
INOV - Instituto de Engenharia de Sistemas e Computadores, Inovação, Portugal

Pilot Use Cases

Pilot Use Case #1

Securing the smart city's IoT and control systems against confidentiality & integrity breaches

Focus: Securing the IoT and control system infrastructure deployed in a tramway station against confidentiality and integrity breaches.

Place: Barcelona, Spain

Expected outcomes:

- Safer environment where tramways, pedestrians and bikes may coexist safely
- Less safety issues and accidents stemming from man-made cyber-attacks

End Users: CERTs/CSIRTs, transport operators

Pilot Use Case #2

Securing AI-enabled infrastructure of autonomous transport systems in a smart city

Focus: Protection of the AI-enabled infrastructure of the autonomous transport system (AV shuttle and the Remote Operation Centre) available in Tallinn against potential orchestrated attacks.

Place: Tallinn, Estonia

Expected outcomes:

- Minimization of the impact of the attack by identifying the threat, self-recovering from it and sharing the corresponding intelligence with other related system operators and platforms
- Assisting system operators to identify if specially crafted data, designed to confuse AI-based decision making, (e.g., spoofed/fuzzed) are received from onboard vehicle sensors, or injected directly to APIs

End Users: CERTs/CSIRTs, CI security operators

Pilot Use Case #3

Effective incident response and threat intelligence collaboration for critical cross-border smart grid threats

Focus: Education of CERTs/CSIRTs on effective incident response and threat intelligence collaboration in cross-border cyber-attacks.

Place: Tallinn, Estonia and Helsinki, Finland

Expected outcomes:

- Safer services and more protected components of the smart grid to the building residents
- Better decision-making for the energy operators
- Secure energy infrastructure

End Users: CERTs/CSIRTs, Energy infrastructure stakeholders

Consortium

Figure 27: 5th IRIS roll up banner_ Pilot Use Cases

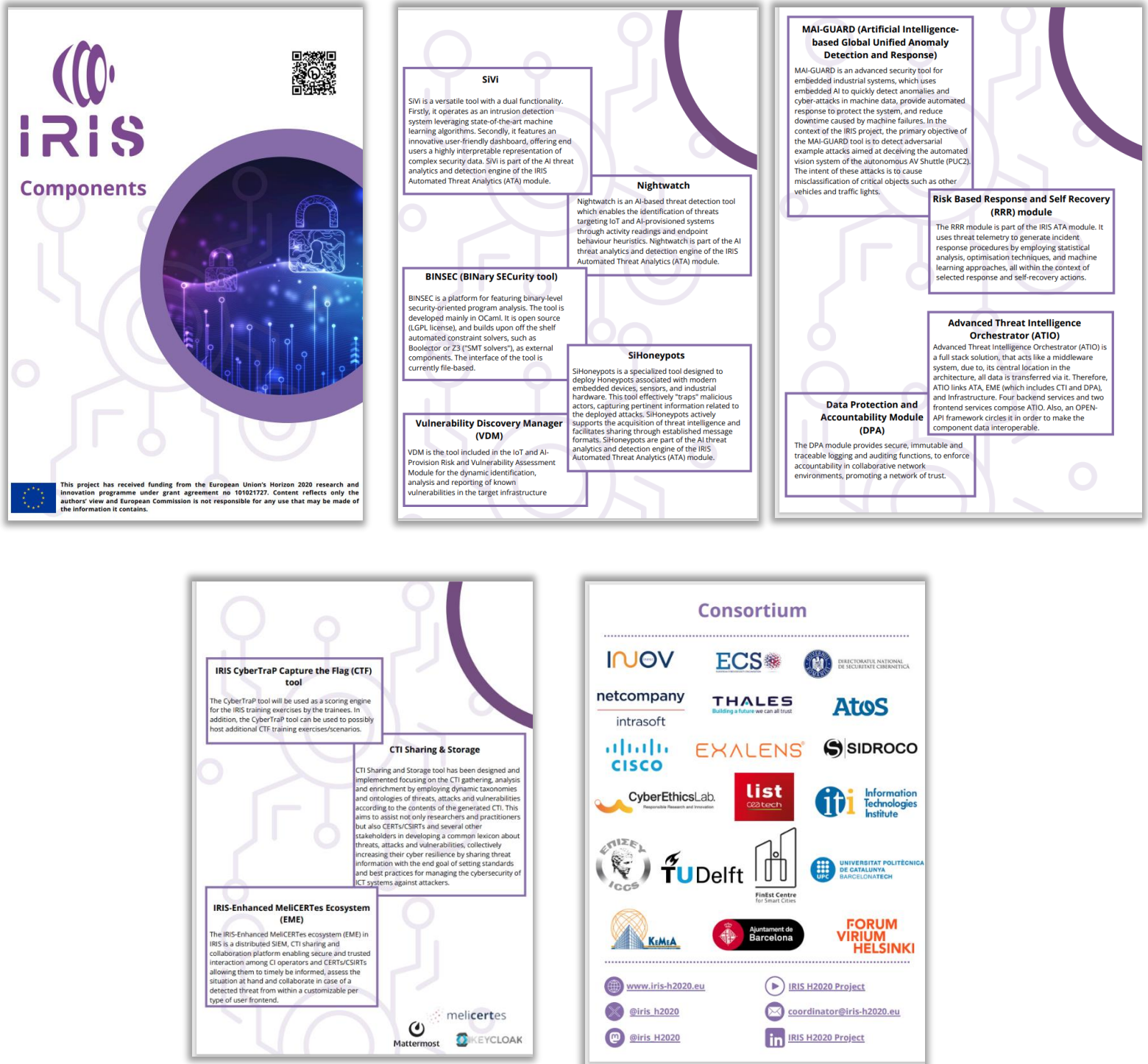


Figure 28: 3rd IRIS brochure – IRIS Components

IRIS

artificial intelligence threat Reporting and Incident response System

As existing and emerging smart cities continue to expand their IoT and AI-enabled platforms, this introduces novel and complex challenges to the threat intelligence landscape linked with identifying, responding and sharing data related to attack vectors, targetting emerging IoT and AI technologies. IRIS is a Horizon 2020 project that integrates and demonstrates a single platform addressed to CERTs/CSIRTs and Critical Infrastructure Operators for assessing, detecting, responding to and sharing information regarding threats & vulnerabilities of IoT and AI-driven ICT systems within smart cities. To achieve this, IRIS brings together experts in cybersecurity, IoT, AI explainability, automated threat detection, response, and recovery.

IRIS helps European CERTs/CSIRTs and Critical Infrastructure Operators 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 has been demonstrated and validated in 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.

The project duration extended from September 2021 to August 2024. Its resulting offerings to the Cybersecurity market are four Service Bundles that can be used either individually or together according to the needs of the target end user:

- the Automated Threat Analytics
- the Enhanced MeliCERTes ecosystem
- the Virtual Cyber Range
- the Add-on Services

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.

IRIS

Automated Threat Analytics Service Bundle

The Automated Threat Analytics (ATA) Service Bundle is a novel cybersecurity solution designed to protect IoT and AI systems. This integrated service offers advanced vulnerability management, binary analysis, intrusion detection, and honeypot capabilities tailored specifically for the complexities of smart city environments and critical infrastructures.

ATA Service Bundle can be used to enhance their cybersecurity by evaluating and managing IoT/AI system risks. It facilitates threat intelligence sharing with standardized formats, enriches knowledge bases like MISP, and monitors for abnormal behavior using machine learning. Additionally, Digital Twin Honeypots enable proactive threat analysis and prediction, ensuring an adaptive security framework.

Target:

- Smart city operators (local governments, utility providers, transportation authorities)
- National and regional cybersecurity authorities (CERTs/CSIRTs)
- Businesses of all sizes across various industries utilizing IoT/AI technologies
- Critical Service/Infrastructure operators

Benefits:

- Proactively address emerging threats with tailored IoT/AI security measures
- Reduce the burden on security teams through automation and orchestration
- Facilitates compliance with cybersecurity regulations that focus on risk management and incident response

Partners and contact people:

IRIS

AtoS

Susana Gonzalez Zarzosa: susana.garzosa@eviden.com
Rodrigo Diaz: rodrigo.diaz@eviden.com

EXALENS

Irene Karapistoli: irene.karapistoli@exalens.com

CyberEthicsLab.
Responsible Research and Innovation

Lorena Volpini: lvolpini@cyberethicslab.com

list
co2 tech

Michael Marcozzi: michael.marcozzi@cea.fr
Sebastien Bardin: sebastien.bardin@cea.fr

IRIS

Enhanced MeliCERTes Ecosystem (EME) Service Bundle

The IRIS-Enhanced MeliCERTes ecosystem (EME) is a distributed SIEM, CTI sharing and collaboration platform enabling secure and trusted interaction among CI operators and CERTs/CSIRTs allowing them to timely be informed, assess the situation at hand and collaborate in case of a detected threat from within a customizable per type of user web frontend.

EME serves as a single hub for cybersecurity stakeholders to coordinate their efforts, share critical information, and optimize their incident response capabilities in the face of evolving cyber threats concerning primarily IoT and AI-driven platforms. The EME's information sharing, visual analytics, secure communication and collaboration features allow national CSIRTs, cybersecurity authorities, and critical infrastructure operators to be timely and fully informed, assess the situation and work together in real-time during critical incidents to effectively respond and minimize their impact. Its integrated CTI Sharing and Storage tool facilitates the development of standardized threat taxonomies, enhancing collective cyber resilience.

Target:

- National/Regional Computer Security Incident Response Teams (CSIRTs) or CERTs (Computer Emergency Response Teams)
- Cybersecurity authorities and agencies (e.g., ENISA, NCCs, EU-CERT, Europol)
- Critical infrastructure operators (focusing on smart cities) / Operators of Essential Services (OESs)
- Security Operations Centers (SOCs)

Benefits:

- Facilitates timely, interoperable sharing of incident data and cyber threat intelligence (CTI) among all relevant stakeholders



Enhanced MeliCERTes Ecosystem (EME) Service Bundle

- Improved incident response times by streamlining communication and information sharing
- Interoperable, integrates with existing cybersecurity tools and systems, leveraging previous investments
- User-friendly interface reduces the need to switch between multiple systems
- Helps organizations comply with relevant EC cybersecurity regulations and reporting requirements, such as the NIS Directive

Partners and contact people:

intrasoftware
Sofia Tsekeridou: sofia.tsekeridou@netcompany.com

Information Technologies Institute
Eleni Darra: e.darra@iti.gr

Dr Angelos Amiditis: a.amiditis@iccs.gr
Giovana Bilali: giovana.bilali@iccs.gr

Virtual Cyber-Range Service Bundle

The Virtual Cyber Range (VCR) Service Bundle is a platform for immersive and realistic cybersecurity training simulations. It creates engaging, scenario-based exercises that enhance the effectiveness of cybersecurity training for both end-users and professionals. The VCR features highly realistic simulations of targeted attacks, enabling hands-on, practical training that complements theoretical knowledge. The VCR is designed to train CERT/CSIRT analysts and cybersecurity professionals, empowering organizations to develop a skilled, resilient workforce capable of defending against evolving cyber threats.

The VCR enables organizations to engage in hands-on training with immersive scenarios that simulate targeted cyber-attacks and security breaches.

Target:

- Critical infrastructure operators (e.g., energy, transportation, telecom)
- Government agencies (e.g., CERTs, CSIRTs)
- Cybersecurity service providers

Benefits:

- Realistic and immersive simulations improve learning outcomes
- Rapid development and deployment of new training scenarios

Partners and contact people:

Building a better world, one idea at a time
Lorens Barraud: lorens.barraud@thalesgroup.com
Bruno Vidalenc: bruno.vidalenc@thalesgroup.com

Nikos Kapsalis: n.kapsalis@kemea-research.gr
Sotirios Spantideas: s.spantideas@kemea-research.gr

Add-on Services Service Bundle (Data Protection and Accountability (DPA) module)

The Add-on Services Bundle provides a decentralized, secure solution for logging and auditing critical decisions and changes during collaborative incident response workflows. Unlike traditional centralized logging services, DPA uses advanced self-encryption and secret key sharing technologies to ensure that logs are immutable, traceable, and managed by the collaborating parties themselves. This enhances accountability and trust in incident response processes by offering a transparent logging mechanism.

Add-on Services (DPA) can be used to enhance the integrity and transparency of their incident response processes. By securely logging and auditing critical decisions and changes in an immutable manner, organizations can ensure a reliable record of their actions.

Target:

- EU CERTs/CSIRT Teams
- National Authorities
- Organizations engaged in collaborative incident response workflows

Benefits:

- Provides a clear, immutable record of actions and decisions
- Ensures that all parties involved in incident response can access and verify logs independently

Partners and contact people:

Goncalo Cadete: goncalo.cadete@inov.pt

Roland Kromes: R.G.Kromes@tudelft.nl

IRIS Components

SIVI
SIVI is a versatile tool with a dual functionality. Firstly, it operates as an intrusion detection system, leveraging state-of-the-art machine learning algorithms. Secondly, it features an innovative user-friendly dashboard, offering end users a highly interpretable representation of complex security data. SIVI is part of the AI threat analytics and detection engine of the IRIS Automated Threat Analytics (ATA) module.

SIHoneypots
SIHoneypots is a specialized tool designed to deploy Honeypots associated with modern embedded devices, sensors, and industrial hardware. This tool effectively "traps" malicious actors, capturing pertinent information related to the deployed attacks. SIHoneypots actively supports the acquisition of threat intelligence and facilitates sharing through established message formats. SIHoneypots are part of the AI threat analytics and detection engine of the IRIS Automated Threat Analytics (ATA) module.

Nightwatch
Nightwatch is an AI-based threat detection tool which enables the identification of threats targeting IoT and AI-provisioned systems through activity readings and endpoint behaviour heuristics. Nightwatch is part of the AI threat analytics and detection engine of the IRIS Automated Threat Analytics (ATA) module.

Risk Based Response and Self Recovery (RRR) module
The RRR module is part of the IRIS ATA module. It uses threat telemetry to generate incident response procedures by employing statistical analysis, optimisation techniques, and machine learning approaches, all within the context of selected response and self-recovery actions.

Charalampos Eleftheriadis: celeftheriadis@sidroco.com
Zisis Batzos: zbatzos@sidroco.com
Harris Saoulidis: hsaoulidis@sidroco.com

Irene Karapistoli: irene.karapistoli@exalens.com

The figure displays four brochures related to the IRIS project. The top-left brochure, titled 'IRIS Components', details the BINSEC platform, the MAI-GUARD tool for anomaly detection, and the Vulnerability Discovery Manager (VDM). The top-right brochure, also titled 'IRIS Components', describes the Advanced Threat Intelligence Orchestrator (ATIO), the Data Protection and Accountability Module (DPA), and the IRIS CyberTraP tool. The bottom-left brochure, titled 'IRIS Components', focuses on CTI Sharing & Storage, the IRIS-Enhanced MeliCERTes Ecosystem (EME), and contact information for the project. The bottom-right brochure, titled 'Consortium', lists the participating organizations, including INOV, ECS, netcompany, intrasoft, CISCO, EXALENS, SIDROCO, CyberEthicsLab, list, iti, TU Delft, FinEst, KEMEA, Ajuntament de Barcelona, and FORUM VIRIUM HELSINKI. It also provides contact information for the IRIS H2020 Project.

IRIS Components

BINSEC
BINSEC is a platform for featuring binary-level security-oriented program analysis. The tool is developed mainly in OCaml. It is open source (LGPL license), and builds upon off the shelf automated constraint solvers, such as Boolelector or Z3 ("SMT solvers"), as external components. The interface of the tool is currently file-based.

MAI-GUARD (Artificial Intelligence-based Global Unified Anomaly Detection and Response)
MAI-GUARD is an advanced security tool for embedded industrial systems, which uses embedded AI to quickly detect anomalies and cyber-attacks in machine data, provide automated response to protect the system, and reduce downtime caused by machine failures. In the context of the IRIS project, the primary objective of the MAI-GUARD tool is to detect adversarial example attacks aimed at deceiving the automated vision system of the autonomous AV Shuttle (PUC2). The intent of these attacks is to cause misclassification of critical objects such as other vehicles and traffic lights.

Michael Marozzi: michael.marozzi@cea.fr
Sebastien Bardin: sebastien.bardin@cea.fr

Vulnerability Discovery Manager (VDM)
VDM is the tool included in the IoT and AI-Provision Risk and Vulnerability Assessment Module for the dynamic identification, analysis and reporting of known vulnerabilities in the target infrastructure.

Susana Gonzalez Zarzosa: susana.gzarzosa@eviden.com
Rodrigo Diaz: rodrigo.diaz@eviden.com

IRIS Components

Advanced Threat Intelligence Orchestrator (ATIO)
Advanced Threat Intelligence Orchestrator (ATIO) is a full stack solution, that acts like a middleware system, due to, its central location in the architecture, all data is transferred via it. Therefore, ATIO links ATA, EME (which includes CTI and DPA), and Infrastructure. Four backend services and two frontend services compose ATIO. Also, an OPEN-API framework circles it in order to make the component data interoperable.

Dr Angelos Amiditis: a.amiditis@iccs.gr
Giovana Bilali: giovana.bilali@iccs.gr

Data Protection and Accountability Module (DPA)
The DPA module provides secure, immutable and traceable logging and auditing functions, to enforce accountability in collaborative network environments, promoting a network of trust.

Goncalo Cadete: goncalo.cadete@inov.pt
Katali Liang: katali.liang@tudelft.nl

IRIS CyberTraP Capture the Flag (CTF) tool
The CyberTraP tool will be used as a scoring engine for the IRIS training exercises by the trainees. In addition, the CyberTraP tool can be used to possibly host additional CTF training exercises/scenarios.

Nikos Kapsalis: n.kapsalis@kemea-research.gr
Sotiris Spantideas: s.spantideas@kemea-research.gr

IRIS Components

CTI Sharing & Storage
CTI Sharing and Storage tool has been designed and implemented focusing on the CTI gathering, analysis and enrichment by employing dynamic taxonomies and ontologies of threats, attacks and vulnerabilities according to the contents of the generated CTI. This aims to assist not only researchers and practitioners but also CERTS/CSIRTs and several other stakeholders in developing a common lexicon about threats, attacks and vulnerabilities, collectively increasing their cyber resilience by sharing threat information with the end goal of setting standards and best practices for managing the cybersecurity of ICT systems against attackers.

Eleni Darra: e.darra@iti.gr
Dimitris Kavallieros: dimitris.kavallieros@gmail.com

IRIS-Enhanced MeliCERTes Ecosystem (EME)
The IRIS-Enhanced MeliCERTes ecosystem (EME) in IRIS is a distributed SIEM, CTI sharing and collaboration platform enabling secure and trusted interaction among CI operators and CERTS/CSIRTs allowing them to timely be informed, assess the situation at hand and collaborate in case of a detected threat from within a customizable per type of user frontend.

Sofia Tsekeridou: sofia.tsekeridou@netcompany.com
Kostas Chisiridis: konstantinos.chisiridis@netcompany.com

Watch the demo videos on our YouTube channel:
[IRIS H2020 Project](https://www.youtube.com/channel/UCIRIS_H2020)

Consortium

INOV, ECS, netcompany, intrasoft, CISCO, EXALENS, SIDROCO, CyberEthicsLab, list, iti, TU Delft, FinEst, KEMEA, Ajuntament de Barcelona, FORUM VIRIUM HELSINKI, DIRECTORATUL NATIONAL DE SECURITATE CIBERNETICA, UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

www.iris-h2020.eu
[@iris_h2020](https://twitter.com/iris_h2020)
[@iris_h2020](https://www.linkedin.com/company/iris-h2020-project)

IRIS H2020 Project
coordinator@iris-h2020.eu
IRIS H2020 Project

Figure 29: 4th IRIS brochure _ Service Bundles & Components

8.2 Annex 2: Secure Cyber Cluster brand book

Branding Elements

The Vision

SecureCyber Cluster envisions a digitally integrated Europe, where businesses, governments, and individuals operate in a cyber environment that is secure, resilient, and invulnerable to threats.

We aim to be the cornerstone of cybersecurity, ensuring that European digital assets are protected and trusted.

The Mission

SecureCyber's mission is to enhance cybersecurity across Europe by fostering collaboration among H2020 funded projects. The commitment is to developing innovative solutions through synergies created in our cluster.

By facilitating monthly meetings, policy briefs, white papers, workshops and webinars we aim to advance the field of cybersecurity.

Target Audience

Target Persona 1

Gender: Female
Age: 30-35
Profession: Cybersecurity Analyst
Education: Master's Degree in Information Security
Project: Developing AI-based threat detection systems

Target Persona 2

Gender: Male
Age: 40-45
Profession: IT Project Manager
Education: Bachelor's Degree in Computer Science with certifications in cybersecurity
Project: Implementing a comprehensive security protocol for financial institutions

Personality

The archetypes

Let's talk about the archetypes incarnated by the brand. Archetypes are a way to understand the personality of a brand. Here is a brief introduction followed by a chapter for each archetype.

SecureCyber Cluster is a brand that embodies the archetype of the **Sage**, the **Explorer**, and the **Innovator**.

The Sage represents the brand's commitment to knowledge, wisdom, and expertise in the field of cybersecurity. The Explorer represents the brand's adventurous spirit and willingness to explore new frontiers in cybersecurity. The Innovator represents the brand's commitment to innovation and creativity in developing new cybersecurity solutions.

The Sage

The Sage archetype represents the brand's commitment to knowledge, wisdom, and expertise in the field of cybersecurity.

SecureCyber Cluster is a brand that values expertise and knowledge in the field of cybersecurity. Our team of experts is dedicated to staying up-to-date with the latest trends and developments in cybersecurity.

We believe that knowledge is power, and we strive to share our knowledge with our clients and partners to help them stay ahead of the curve.

The Explorer

The Explorer archetype represents the brand's adventurous spirit and willingness to explore new frontiers in cybersecurity.

SecureCyber Cluster is a brand that is always looking for new and innovative ways to enhance cybersecurity.

We are not afraid to take risks and explore new frontiers in cybersecurity. The team of experts is always looking for new and innovative solutions to help our clients stay ahead of the curve.

Visual Tools

TYPOGRAPHY

Titles
Railway ExtraBold
abcdefghijklmnopqrstuvwxyz
123456789
Download the font family [here](#)

Subtitles
Railway ExtraLight
abcdefghijklmnopqrstuvwxyz
123456789
Download the font family [here](#)

Longer texts
Railway Regular
abcdefghijklmnopqrstuvwxyz
123456789
Download the font family [here](#)

COLOR PALETTE

Primary

Space Cadet #2E3192 HEX #2E3192 HEX #2E3192 HEX	Vivid Sky Blue #00AEEF HEX #00AEEF HEX #00AEEF HEX
--	---

Secondary

Midnight Aquamarine #008080 HEX #008080 HEX #008080 HEX	Sundarium #FFD700 HEX #FFD700 HEX #FFD700 HEX
--	--

Neutrals

Platinum #E0E0E0 HEX #E0E0E0 HEX #E0E0E0 HEX	Dark Charcoal #333333 HEX #333333 HEX #333333 HEX
---	--

LOGO VARIATIONS

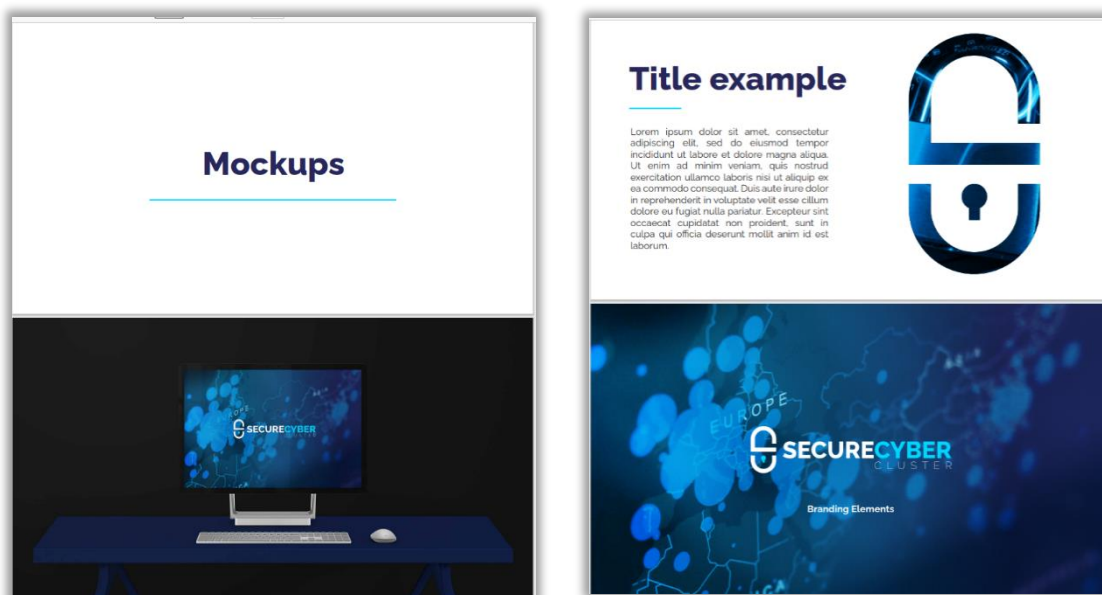


Figure 30: Secure Cyber Cluster brand book