A coordinated framework for cyber resilient supply chain systems over complex ICT infrastructures

D7.4 Report on dissemination, standards and exploitation (Y3)

Document Identification			
Status	Final	**Due Date**	31/08/2023
Version	1.0	**Submission Date**	04/09/2023

Related WP	WP7	**Document Reference**	D7.4
Related Deliverable(s)	D7.5, D7.6, D7.7	**Dissemination Level (*)**	PU
Lead Participant	XLAB	**Lead Author**	Joao Costa
Contributors	ATOS, TUBS, UPC, STS, ALTRAN, SYN, UMINHO, POLITO, TID, SONAE, OPT	**Reviewers**	TID (Antonio Pastor) POLITO (Daniele Canavese) SYN (Nelly Leligou)

Keywords:
Dissemination, activities, standards, exploitation, IPR management, external advisory board, business model, success stories, business case, project.

Document Information

List of Contributors	
Name	Partner
Joao Pita Costa	XLAB
Jan Antić	XLAB
Aleš Černivec	XLAB
Hrvoje Ratkajec	XLAB
Jasenka Dizdarevic	TUBS
Mounir Bensalem	TUBS
Nelly Leligou	SYN
Alexandra Lakka	SYN
Antonio Alvarez Romero	ATOS
Rodrigo Diaz Rodriguez	ATOS
Noel Ruiz López	ALTRAN
Henrique Santos	UMINHO
Pedro Magalhaes	UMINHO
Ana Machado Silva	SONAE
Rui Guilherme Goncalves	SONAE
Antonio Pastor Perales	TID
Diego R. Lopez	TID
Daniele Canavese	POLITO
Aldo Basile	POLITO
Eva Marín Tordera	UPC
Xavi Masip	UPC
Grigorios Kalogiannis	STS
Kostas Poulios	STS
Antonis Gonos	OPT

Document History			
Version	Date	Change editors	Changes
0.1	2022-11-15	Joao Costa (XLAB)	ToC and initial structure
0.2	2022-11-30	Joao Costa (XLAB)	First version of section 4
0.3	2022-12-6	Joao Costa (XLAB)	Inclusion of the concluded IPR management reporting closing the list of IP results built within the project
0.4	2022-12-9	Joao Costa (XLAB)	Inclusion of the final results of the Horizon Results Booster programme on Business Plan Development
0.5	2023-04-05	Joao Costa (XLAB)	Added output of Horizon Results Booster coaching programme
0.6	2023-05-10	Joao Costa (XLAB)	Added community engagement strategy and the KPIs and plans for exploitation
0.7	2023-06-16	Joao Costa (XLAB), Eva Marin (UPC)	Added results of the survey and the analysis of the communication channels
0.8	2023-07-10	Daniele Canavese (POLITO), Jose Manuel Manjón (TID), Joao Costa (XLAB), Antonio Álvarez Romero (ATOS)	Integrated comments from internal review procedure
0.9	2023-07-15	Joao Costa (XLAB), Eva (UPC), Diego R. López (TID)	Internal review process finished and requests addressed.
0.91	2023-08-28	Juan Alonso (ATOS)	Quality Assessment
1.0	2023-08-31	Antonio Alvarez Romero (ATOS)	Final version

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Joao Costa (XLAB)	25/08/2023
Quality manager	Juan Andres Alonso (ATOS)	29/08/2023
Project Coordinator	Antonio Alvarez Romero (ATOS)	04/09/2023

Table of Contents

List of Tables

List of Figures

List of Acronyms

Abbreviation / acronym	Description
AB	Advisory Board
ACME WG	Automated Certificate Management Environment Working Group
BMC	Business Model Canvas
BO	Business Opportunity
BOE	Boletin Oficial del Estado
CNF	Cloud-native Network Function
CNI	Container Network Interface
CPC	Cooperative Patent Classification
DoA	Description of Action
EAB	External Advisory Board
EC	European Commission
EDA	Exploitation Domains of Action
EDC	Enforcement & Dynamic Configuration
EIM	Exploitation and Innovation Manager
EPO	European Patent Office
ER	Exploitable Result
EU	European Union
F2F	Farm to Fork
FRAND	Fair, reasonable, and non-discriminatory
FRF	FISHY Reference Framework
FTE	Full-Time Equivalent
GA	Grant Agreement
GDPR	General Data Protection Regulation
HIDS	Host-based Intrusion Detection System
HPC	High Performance Computing
HRB	Horizon Results Booster
I2NSF WG	Interface to Network Security Functions Working Group
IDS	Intrusion Detection System

Abbreviation / acronym	Description
IETF	Internet Engineering Task Force
IGT	Impact Generation Team
IRTF	Internet Research Task Force
IRO	Intent-based Resilience Orchestration
ITRO	IT Resilience Orchestration
ISO	International Organization for Standardization
IP	Intellectual Property
JSON	JavaScript Object Notation
KER	Key Exploitable Results
KPI	Key Performance Indicators
KR	Key Result
MTRL	Market Technology Readiness Level
NETMOD WG	Network Modeling Working Group
NFV	Network Function Virtualisation
NGFW	Next Generation firewall
NIDS	Network-based Intrusion Detection System
NMRG	Network Management Research Group
OEM	Original Equipment Manufacturer
OPSAWG	Operations and Management Area Working Group
OSM	Open Source MANO
PM	Person-month
PPM WG	Privacy Preserving Measurement Working Group
RATS WG	Remote ATtestation ProcedureS Working Group
SACM	Security Assurance & Certification Manager
SADE	Securing Autonomous Driving Function at the Edge
SDN	Software Defined Networking
SEM	Security Event Management
SFC WG	Service Function Chaining Working Group
SIA	Secure Infrastructure Abstraction
SIEM	Security Information and Event Management

Abbreviation / acronym	Description
SIM	Security Information Management
SNMP	Simple Network Management Protocol
SOAR	Security Orchestration, Automation, and Response
SPI	Security & Privacy Dataspace Infrastructure
SWOT	Strengths, Weaknesses, Opportunities, and Threats
TAL	Technology Adoption Lifecycle
TCO	Total Cost of Ownership
TCP	Transfer Control Protocol
TIM	Trust & Incident Manager
TTO	Technology Transfer Office
UDP	User Datagram Protocol
UTM	Unified Threat Management
UVP	Unique Value Proposition
WBP	Wood-based panels

Executive Summary

As in the preceding deliverables of WP7, this publishable document reports the WP7 activities during the third and final year of the FISHY project; as well as the accumulative work done along the project's lifetime with regards to impact generation. Moreover, the sustainability of the project and the plans beyond its lifetime are also presented. The first section of introduction provides the context on the present document, followed by a section for each task in WP7 summarising the work carried out on each one of them. The information on the dissemination and communication activities in FISHY are detailed in section 2, together with the strategy and metrics on the employed communication tools used in this final stage of the project. The final results of standardisation activities are presented in section 3, together with an analysis of the most salient opportunities for further contribution. The project has actively contributed to upstream open-source projects in its lifetime, and this final activity is reported here together with a discussion of the general open-source and open research strategy. Once again we include a summary of the exploitation activities in section 4 highlighting the key project results, performed throughout the final year of the project as part of its innovation management activity, following the Horizon Results Booster coaching that helped improve the quality of the obtained business models. We also include an analysis of exploitation opportunities, reflecting the exploration of the success stories of the benefits of FISHY as implemented to the project's use cases. Moreover, we include the outcomes of our final meeting with the External Advisory Board.

1 Introduction

1.1 Main achievements in the reporting period

The purpose of this document is to provide a publishable detailed report of the activities related to dissemination, standardisation and exploitation carried during the third and final year of the project. With it, the FISHY consortium reassures the importance of maintaining good monitoring and evaluating practices dedicated to WP7 activities throughout the project lifetime to maximise the impact of its outputs, detailing and analysing already performed and ongoing activities, and using them as input to establish a plan for future actions beyond the project's lifetime. In this last reporting period we have:

- Largely increased the visibility of the project vision and its key exploitable results (KERs) both in the research and scientific community as well as the general public, through top-tier publication venues (including conferences, workshops and peer-reviewed scientific papers, mostly open access), marketing materials, blog posts and white papers. We have organised 4 workshops (one more than defined in the DoA), 1 Demo Day (held at the impactful Barcelona Cybersecurity Congress in 2023 [41]) and 1 Summer Camp (collocated with the DRCN 2023 conference) ensuring the appropriate knowledge transfer to the scientific community.
- Monitored activities of all nature related to relevant standards (SDOs, industry associations, open-source communities) that contribute to the project objectives, and identified needs and opportunities motivating new research paths to provide appropriate technical contributions to publish/influence new standards: e.g., IETF/IRTF groups, ETSI, 3GPP.
- Coordinated knowledge and innovation management seamlessly within the project activities and tasks, ensuring that the consortium members can be well engaged in common exploitation pathways of the defined KERs, and maximise their own exploitation leveraging the innovation and exploitation potential of the project outcomes, contributing to the improvement of business cases in use cases, market positioning of technological developers and recognition of research results within the scientific community.
- Exposed the project's KERs in the industry through industrial event participation and with the collaboration through liaisons with European initiatives engaging with other organisations, key market players and potential users of the FISHY technology.
- Prepared pitch tools (7 pitch decks and pitch canvas for the 7 KERs addressing 7 target audiences) and marketing materials (flyer, poster, presentation, infographics, videos, press release, white paper) to communicate the FISHY value message, and expose the outcomes of the project through the application of its key exploitable results.
- Conducted an appropriate IPR management that ensures the protection of the technology created throughout the project, proceeding with the appropriate innovation log and protection, and performing a white space analysis aligned with the outcomes of the FISHY Radar (and already published in the deliverable D2.4) to identify the technology gap where the FISHY exploitable results can find business opportunity.

Worked under the guidance of the Horizon Results Booster (HRB) to define the KERs of the project in their different exploitation information layers, from problem-solution-value characterisation to the exploration of their value proposition canvas (see [1][2][3]).The impact creation activities within WP7 reported here are horizontal activities within the project, and therefore its results directly impact the success of the overall project. The final status of the R&D and the maturity of the project's technology helped in identifying the opportunities for impact creation and in translating project results into contributions in the areas of communication, standardisation, and further exploitation. The coverage of KERs shown in the chart of Figure 1 reflects the achievements in the project up to the date of

publication of this document, as described in detail in its following sections and appendices. Figure 1 shows the good coverage of the project's KERs over the dissemination channels addressing the scientific community (journal and conference papers as well as the project's blog posts with valuable technical content), the developer community (through well documented open source repositories and public deliverables) and other European initiatives (i.e. liaisons to other EC-funded projects).

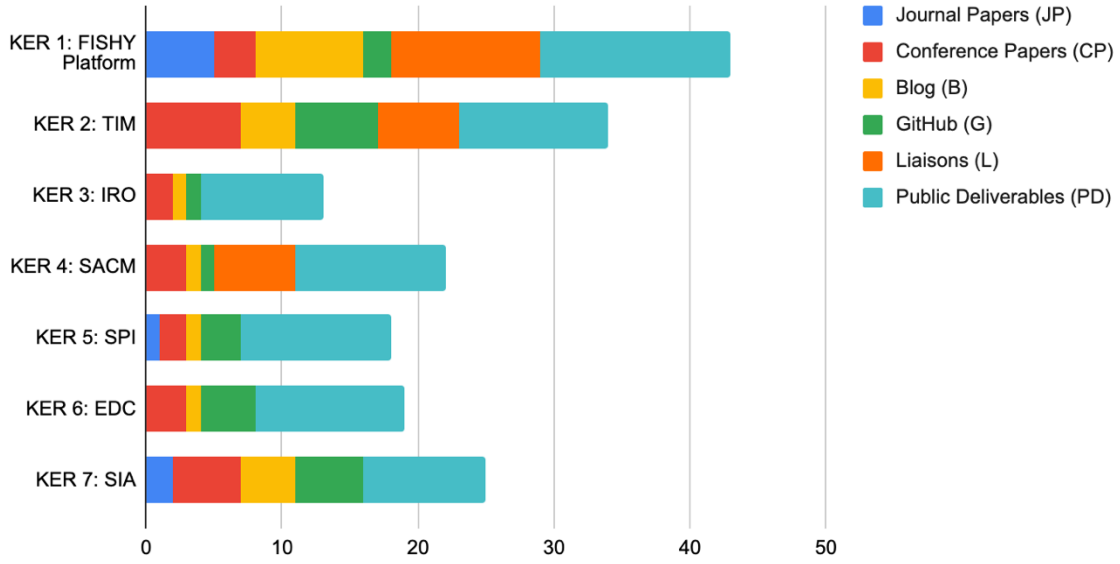


Figure 1 - FISHY KER coverage by research papers, blog posts and public deliverables & repositories

This deliverable constitutes the third of a series of periodic reports, each corresponding to one of the years in the project lifetime. The document is an update of the reports produced in the first and second years of the project [4][5]. D7.4 is the summarised public version of the full document published as deliverable D7.7. D7.4 does not contain much of the exploitation information considered confidential and included in its counterpart D7.7, reporting progress and plan updates for year 3, in the light of the final update of the project.

1.2 Structure of the document

The document is structured according to the three classes of impact creation activities, each one reported in one of the chapters.

Chapter 2 details the communication and dissemination activities, ranging from event participation and organisation to publications of different nature (including research papers and blog posts). The status of the different communication channels (website, social networks, newsletters, YouTube, GitHub and Zenodo) are described and their impact analysed is exposed. This section also includes the different activities in the context of liaisons of different nature between FISHY and other EC-funded initiatives.

Chapter 3 once again summarises the active involvement and the contributions made to different standardisation bodies and industry groups, including the discussion of ongoing activities and further contributions beyond the lifetime of the project. It also lays down the 5-pillar strategy of Community engagement in line with the open source and open research approach in this project.

Chapter 4 reports the exploitation-focused activities, discussing the innovation management of this project in this final reporting period. It elaborates on the 7 KERs that bundle the project's innovation assets, the defined domains of action, and the exploitation framework adopted and shared in the earlier deliverables of the WP7. We also present the different aspects of FISHY's sustainability strategy

and the plan for business development, constructed with the support of the Horizon Results Booster programme. Finally, it presents the outcomes of the last meeting with the project's External Advisory Board.

1.3 Interactions between tasks

It is in the final stage of the project that the interactions between the tasks within WP7 are more visible, allowing for more effective communication of the value message of FISHY, towards the standards bodies and European initiatives that we have been interacting with as well as towards the scientific and open source communities, and the general public. In particular, the interactions between the exploitation task and the other tasks in the WP and in the project is essential to the well-functioning and healthy status of the KERs in the lifetime of the project in respect to their definition, exposure and feedback to product development. In that context, the interactions are as follows:

- FISHY Radar (T2.1): the planned IP results protection and analysis drives the product development to define the exploitable results, their functionality, benefits and differentiators. Deliverable D2.6 has been a relevant input from this task [43]
- Cross-functional platform integration (T5.3): the construction of marketing materials driven by the KER definitions to better expose the value of the functionality of the platform, the co-organisation of joint actions in industrial events to give the appropriate exposure to those KERs and to the FISHY brand in general, and the nurturing of campaigns to highlight the innovation in the project.
- Use case validation (T6.4): following the challenges and the benefits identified by the early technology adopters, we integrated that feedback in the communicated value message and derive the estimates of business case improvement at each use case. Deliverables D6.2 [44] and D6.4 [45] have been the most relevant input for this task.
- Tech coordination (T1.5) - following the latest developments that allowed us to identify the innovation generated by the project and considered in the IP portfolio, we feed the product development of FISHY defining the exploitable results.
- Project steering (T1.1) - overview of the project's objectives and support in the submission of KERs to the Horizon Results Portal, or using the Cyberwatching.eu to expose the sustainability strategy.

There are other (smaller) relations in the project's work programme as, e.g., requirements gathering in T2.2 that also contributed to better understanding the profile of the FISHY user.

1.4 Glossary adopted in this document

The most important terms used in this document and their explanation are listed below.

- **Business Model**. The rationale of a company to generate, deliver and capture value out of their commercial offering and their business relationships.
- **Domain of action.** This is the domain targeted by partners responsible for the KERs.
- **Feature comparison.** The analysis of the competitors based on the comparison with their features and the value they can generate.
- **Key Exploitable Results (KER or plural KERs).** These are the results implying business potential from the technology partners in the project.
- **Legal and Regulatory Landscape.** The legislation basis in relation to the scope of FISHY affecting at international, national and regional levels.

- **Market growth.** The volume and potential of a specific market in the context of the industry and audience it is addressing.
- **Market radar**. Continuous monitoring of relative positioning of the top software vendors within a specific market or niche (or domain of action).
- **Market trend**. The tendencies and dynamics of the market resulting into the attractiveness of the IT and what it relates to.
- **Technological imperatives.** The technologies that translate the necessities to be addressed in a specific industry.

2 Dissemination & Communication

In this chapter, the specific communication and dissemination activities carried out during the third and last year of the project are deeply described. Also, the KPIs related to communication and dissemination are assessed. These activities include, but are not limited to, participation in events/conferences/workshops, published scientific papers, blog entries and other general publications, fostering relationships and synergies with related projects.

2.1 Progress Highlights

2.1.1 Main achievements

During the third and last year of the project, the main achievements of FISHY in terms of communication and dissemination have been:

- Participation in the Cybersecurity Congress in Barcelona(31/01-02/02/2023). This is a joint action framed in the European Research Innovation for Cybersecurity (ERICyB) cluster with other six EU-funded projects (see section 2.4); including the FISHY demo day.
- Organization of a joint workshop, 4th International workshop on Information & Operational Technology (IT & OT) security, with EU-funded projects JCO, PHOENI2X and IntellIoT, in the framework of the DRCN 2023 conference on April 20, 2023 (see section 2.2).
- Organization of the FISHY summer camp on April 20, 2023 in the framework of the DRCN 2023 conference.
- The number of published journals with ACK to FISHY during this period is 1, 7 in total; and the number of published papers in conferences has achieved 17, 7 more than the second year.
- The number of blog posts published during the 3rd and last year of the project is 14, achieving a total number of 23 blog entries in the FISHY website (including 5 video blogs).
- 2 press release and 2 Newsletter have been published during this last year of the project.
- FISHY increases the number of followers in Twitter to 71 new followers.
- FISHY increases the number of followers in LinkedIn to 83 new followers.
- Participation in more than 9 international events.
- Publication of our FISHY KERs.
- Presentation of SIA PoC in the Open Source MANO Ecosystem day.
- Participation in DRCN 2023 panel “Reliability, are you for real?” supported by the EU-funded Projects Phoeni2x and FISHY.

2.1.2 Key Performance Indicators

In the grant agreement, the consortium established several performance indicators about communication and dissemination, shown in Table 1.

Table 1 - Dissemination Activities: KPIs and Targets

KPI description	KPI Target	KPI Achievements in M36
Scientific publication to conferences and journals supporting FISHY approach	At least 9 indexed journals and 20 conference papers	We have 7 published journals (1 more accepted) and expect to have more papers submitted beyond the lifetime of FISHY from final results.
Impact factor of journals considered for FISHY publications	Greater than 2,5 (within JCR Q1 or Q2)	FISHY has published journals of high quality including open source journals.
Number of workshops attended/organised	At least 6/3	We have attended 24 events, 6 of those being conferences and workshops, and organized 4 workshops, one more than the 3 planned initially in the DoA.
Percentage of ISI indexed journal	90% (room for open source journals)	All published journals are indexed, including open source journals.
Ranking of conferences	75% must belong to tier1 or tier 2 conferences	FISHY has achieved a percentage of 59%.

These KPIs proposed in the Grant Agreement were completed with more indicators in the "D7.1. Dissemination, Communication and Impact Creation: Strategy and Plan"[4] to ease the follow up of the communication and dissemination activities. These extra KPIs are shown in Table 2 and Table 3.

Regarding publications, FISHY achieves 7 journal papers published and 14 conference papers presented. Specifically, during the third and last year of the project FISHY published one more journal with ACK to FISHY in IEEE Networks which has an impact factor of 10.294 (JCR 2021 Q1). Then, the summary of all the FISHY journals ordered by JCR ranking is:

- 2 IEEE Network (JCR **10.294** 2021 **Q1**).
- 1 Sensors MDPI (JCR **3.847**, 2021, **Q2**).
- 1 Computer Networks (JCR **5.493**, 2021, **Q1**).
- 2 Electronics MDPI (JCR **2.690**, 2021, Q3).
- 1 ACM Transactions on Modelling and Performance Evaluation of Computing Systems (JCR 0.42, 2021 Q3).

From this list of 7 journal papers 4 are Q1 or Q2, and 5 have an impact factor greater than 2,5; and all of them are indexed journals.

During this last year FISHY added 7 new conference papers to the list of FISHY papers, being in total 17 papers presented in conferences and published. The list of conference papers ordered by ranking:

- 1 IEEE Global Communications Conference, Globecom (rank A[1, 2]).

[1] https://scie.lcc.uma.es/ratingSearch.jsf

[2] https://www.resurchify.com/

- 1 International Conference on Availability, Reliability and Security, ARES conference paper (rank B[1,2]).
- 4 International Conference on Design of Reliable Communication Networks, DRCN conference papers (rank B[1,2]).
- 1 IEEE Symposium on Computers and Communications, ISCC Conference paper (rank B[1]).
- 1 International Conference on Performance Engineering, ICPE Conference paper (rank B[2]).
- 2 International Conference on Network Softwarization, NetSoft conference papers (rank B[2]).
- 1 International Conference on Modelling and Simulation, ECMS conference paper (rank B[1]).
- 4 International Conference on High-Performance Switching and Routing, HPSR conference papers (rank C[2]).
- 1 Jubilee International Convention on Information, Communication and Electronic Technology, MIPRO conference paper (rank C[2]).
- 1 Conference on Innovation in Clouds, Internet and Networks ICIN conference paper (not ranked).

From this list of papers, 10 of them belong to tier1 (A) or tier2(B) conferences (59%).

Finally, in terms of organized and attended workshops the consortium has already accomplished the proposed KPI with 4 organized workshops, and 24 events attended, being 6 of them conferences or workshops (without considering accepted and presented papers).

Table 2 - Dissemination KPIs

KPI	Targets [3]			Expected Impact
	Y1	Y2	Y3	
Number of project-dedicated workshops	1 (2)	2(3)	3(4)	Increased collaboration with other initiatives/projects/programmes for joint research, information exchange and dissemination. Increased awareness. Contact external stakeholders to promote FISHY solutions.
Number of attendees to the FISHY workshops	50 (40)	100 (80)	150 (140)	
Number of FISHY events (Summer Camp/ Demo Day)	0	0	2(2)	
Number of attended events (including 4 exhibitions and industrial events)	10 (5)	20(7)	30 (24)	Ideas' gathering and knowledge exchange with relevant communities, projects and initiatives; Information about latest ICT news; Liaisons; Increased awareness.
Number of scientific publications (90% ISI indexed journals)	1 (1)	5(6)	9(7)	Validation of the project's concept, findings and advantages; Promotion of results to scientific communities; Ideas' gathering and knowledge exchange with relevant communities and initiatives.
Number of articles in general media (at least 20 publications to	2 (1)	10(9)	20 (17)	

[3] In brackets there are detailed the KPIs achieved during this first, second and third year

international conferences and workshops related to cyber resilience)				
Liaisons and joint activities with other projects, communities, initiatives.	5(4)	7(7)	10(10)	Communication of project news, events & results; Validation of project's concept, findings and progress; Ideas' gathering and knowledge exchange; Increased awareness.
Contributions to standardizations	0(15)	2(22)	5 (6)	Submission of at least 4 contributions in relevant industrial bodies and communities

In terms of dissemination KPIs, FISHY has fulfilled almost all these complementary KPIs, especially in terms of organized workshops, and contribution to standards. The number of attended events is below the KPI, but this can be justified by the fact that the project just started in the middle of the pandemic. This pandemic situation also had an impact on the number of conferences where FISHY presented a paper. However, fruit of the joint synergies and also of the final results and prepared demos, FISHY will produce a significant number of scientific publications after the finalization of the project. Currently, 3 conference papers are submitted and 1 journal paper Is in preparation.

Table 3 - Communication KPIs

KPI	Targets			Expected Impact
	Y1	Y2	Y3	
Number of unique website visitors	1,500 (2519)	2,500 (5048)	3,500 (8710)	Main online information channel; Communication of project news, events & results; Liaisons with other initiatives, projects, working groups; Increased awareness. Drive engagement with the project.
Average duration of website visits	2 min (2 min 10 s)	2,5 min (1 min 37 s)	3 min (1 min 12 s)	
Number of website page views	3,000 (9188)	5,000 (14317)	8,000 (19785)	[2]The visibility of the project's progress and achieved results.
Number of references to the project website on search engine (Link Building)	10 (14)	15 (25)	20(20[4])	Liaisons with other initiatives, projects through links; Increased awareness
Number of accumulative followers on Twitter	100 (124)	200 (178)	250 (249)	Increased visibility to stakeholders active on social media; Attainment of interest of stakeholders; Direct communication with followers. Sharing knowledge with other projects and initiatives. Drive engagement with the project
Number of tweets	100 (139)	200 (213)	300 (318)	
Number of LinkedIn members	100 (56)	200 (85)	250 (168)	

[4] First list of followed results in google, July 4th, 2023.

Number of posts, news/ events on the website	15 (>15)	30 (>30)	45 (>45)	
Number of brochures	1 (1)	1(1)	1 (1)	Increased awareness. Drive engagement with the project
Number of infographics	3 (2)	3(4)	3 (5)	Increased awareness on project use cases.
Number of posters	1 (0)	1(0)	1 (2)	Communication of the main project's concepts and advances in a catchy and easily understandable manner. Drive engagement with the project
Number of blog posts	4 (4)	10 (10)	16 (23)	Communication of the main project's concepts and advances in a catchy and easily understandable manner. Drive engagement with the project
Number of project videos	1 (0)	1 (2)	2 (6)	Increase awareness. Reinforcement of the exploitation strategy.
Number of blog videos	2 (0)	4 (0)	6 (5)	Communication of the main project's concepts and advances in a catchy and easily understandable manner. Drive engagement with the project
Number of press releases	1 (1)	1(1)	2 (3)	Communication of project news, events & results; Increased awareness. Unique branding and visual identity of the project; Improves communication of results and information provision during events.

The KPIs related to communication shown in Table 3, are also mostly fulfilled, for instance the number of visitors of our website, number of followers in Twitter and number of tweets, infographics, posters, press releases, blog entries, posts on the website, etc. Nevertheless, some of them are below the corresponding KPI, such as the average duration of website visits and the number of followers on LinkedIn. Regarding this last KPI, number of followers on LinkedIn, it is worth mentioning factors impacting it. On one hand, it is a very ambitious number. In the first part of the project, FISHY had a LinkedIn group. The LinkedIn group was then changed to a LinkedIn profile account to give more visibility to the results and communications of the project. To further improve this number, we are active in republishing FISHY content in the format of LinkedIn articles engaging existing and new users interested in the different KERs of the project.

2.1.3 Dissemination and communication plan beyond Y3

After the finalization of the project, from September 2023, there will still be outcomes of the project in the shape of scientific articles, events, webinars, etc. These outcomes should be still communicated/disseminated. For instances, different papers have already been submitted:

- "Scaling Serverless Functions in Edge Networks: A Reinforcement Learning Approach" by Mounir Bensalem, Erkan Ipek and Admela Jukan from TUBS, submitted to IEEE Globecom 2023 conference.

- "Engineering and Experimentally Benchmarking Open Source MQTT Broker Implementations" by Jasenka Dizdarević, Marc Michalke and Admela Jukan from TUBS, submitted to IEEE Globecom 2023 conference.

And also other papers are now in process of development, most of them being the outcome of the collaboration between 2 or more partners.

On the other hand, FISHY has been invited on 06/06/2023 to a webinar that will be held on 13/09/2023 entitled "Creating cybersecurity awareness in Europe / Can we achieve more together in cybersecurity?" by the Sifis-Home EU project. FISHY and Sifis-Home belong to the European Research Innovation for Cybersecurity (ERICyb), and jointly participated and shared a booth in the Cybersecurity Congress in Barcelona in January 2023.

Apart from the outcomes after the end of the project, ATOS (with the help of UPC) will maintain the FISHY website at least three years after the finalization of the project. UPC will be also in charge of FISHY social media during this period after the lifetime of the project.

2.2 Events

2.2.1 FISHY dedicated events

During the last year of the project the FISHY project has organized 4 General Assemblies:

- 4th General Assembly in Sevilla, October 19-20, 2022. The first face-to-face meeting of the project. This meeting had an important impact on the progress of the project because the partners dealt with specific issues on integration, especially the understanding of the concept of the FISHY Reference Framework.
- 5th General Assembly, online, January 18-19, 2023. This general assembly changed a bit the focus, being organized on workpackages workshops. This approach facilitated technical work and troubleshooting.
- 6th General Assembly in Vilanova i la Geltrú, April 18-19-20, 2023. In this meeting the focus were both, an Integration and a Pilot workshop. Co-located with this assembly FISHY held a 4th workshop, international workshop on Information & Operational Technology (IT & OT) security, in collaboration with 2 more EU funded projects, as well as the FISHY summer camp, with 4 speakers and more than 20 attendants:
    - Raising cybersecurity awareness: practical examples (ATOS – 15 mins)
    - Workshop on next-generation secured communications: Secure Infrastructure Abstraction (TID + UC3M – 35 mins)
    - Workshop on Intent-based networking and practical application (TUBS – 35 mins)
    - Workshop on Wazuh monitoring and detection tool (XLAB – 35 mins)
- 7th General Assembly in Maia Portugal, June 27-28, 2023 (see Figure 2). In this General Assembly partners have worked on some of the pending technical issues, especially for the technical sessions organized in parallel of the plenary meeting. FISHY held also its 3rd EAB meeting on June 27 in a hybrid format.

Figure 2 - 4th General meeting in Sevilla, October 2022

2.2.1.1 FISHY workshops, demo-day and hands-on events

During the last period of the project FISHY has held one demo day, one workshop, as well as a summer camp.

The FISHY demo day was col-located in the FISHY participation in the Barcelona Cybersecurity Congress[5], on January 31st, February 1st, 2nd (see Figure 3). The FISHY participation in the Cybersecurity Congress was in the framework of the European Research Innovation for Cybersecurity (ERICyb) cluster composed of six other European Projects. The seven projects participating in the exhibition were: ASSURED[6], BIECO[7] , CYRENE[8] , FISHY, IoTAC[9], SANCUS[10] and SIFIS-HOME[11].

Previous to this participation the cluster led by IoTAC organized a series of online meetings to agree on the format of the project presentations/demos. The cluster decided to schedule joint presentations each day at 11h and 15h. In these joint presentations with 5 min for each project, the projects demonstrated the state-of-the-art research results in various technical fields of cybersecurity, more specifically IoT security, and how they contribute to the protection of supply chains. Thanks to these presentations the project team managed to, on one hand, receive feedback from the other projects in the booth, discovering synergies and research collaborations; and on the other hand get insights from people external to the cluster of projects. FISHY took advantage of these slots of 5 min each day to present different results of the project, scheduling six different presentations.

- January 31st morning: Technical presentation-SIA/FRF.
- January 31st afternoon: F2F use case video.
- February 1st morning: Technical presentation-TIM.
- February 1st afternoon: WBP use case.
- February 2nd morning: FISHY general presentation and KERs.

[5] https://www.barcelonacybersecuritycongress.com/
[6] https://assured-project.eu/
[7] https://www.bieco.org/
[8] https://www.cyrene.eu/
[9] https://iotac.eu/
[10] https://sancus-project.eu/
[11] https://www.sifis-home.eu/

- February 2nd afternoon: SADE use case.

The event also served to develop our FISHY demo day. Apart from the mentioned presentations in our agenda, also use case demos and specific component demos were prepared to demonstrate the FISHY potential to the event attendees. The demonstrations showed the advantages of the FISHY Platform, and highlighted the trust and incident management capabilities of the technology, as well as the Secure Infrastructure Abstraction (SIA) that brings much novelty to the overall outcomes, opening doors to research paths and to ongoing contribution to related European standards.

Figure 3 - FISHY in the Cybersecurity Congress

As mentioned earlier, on April 20, 2023 FISHY held its 4th workshop: International workshop on Information & Operational Technology (IT & OT) (IoSEC 2023) with the EU-funded projects JCO, PHOENI2X and IntellIoT. IoSEC was framed in the DRCN 2023[12] conference and 6 papers were presented, one of them from XLAB with ACK to FISHY.

Finally, also on April 20, 2023 and co-located with the IoSEC workshop[13] a summer camp[14] was held.

The FISHY Summer Camp brought together experts from the project, PhD students and undergraduate ones. During this event expert talks were on highly innovative topics related to different emerging technologies used in the project. This showed the potential of the research carried out in FISHY, as well as being a great opportunity to receive useful feedback from the audience. The number of participants was 15 (5 undergraduate students), and it was scheduled as follows:

- Raising cybersecurity awareness: practical examples, ATOS.
- Workshop on next-generation secured communications: SIA, TID+UC3M.
- Workshop on Intent-based networking and practical application, TUBS.
- Workshop on Wazuh monitoring and detection tool, XLAB.

[12] https://drcn2023.site.ac.upc.edu/index.html
[13] https://drcn2023.upc.edu/IOSEC2023.html
[14] https://drcn2023.upc.edu/FISHYSummerCamp.html

2.2.2 Participation in Events/conferences/fairs

The participation in events, apart from those organized by FISHY, during the last year can be split into industrial, scientific and EU events. It is worth mentioning that in this summary the activities such as workshops, demo days and summer camps organized by FISHY are not considered, see previous subsection.

Regarding the industrial events, the main events considering both external and company's internal meetings, have been:

- CAPGEMINI participated in the Digital Meeting Telecommunications and Services: "Challenges and objectives 2022" organized by the company's telco division.
- Diego López from TID gave a talk in the ETSI ISG PDL plenary, on November 18-30 2022, online.
- Diego López from TID participated in the webinar: "Making the edge sharp and safe: update on MEC security"[15] on December 1st, 2022.
- Diego López from TID gave a keynote in the Layer123 World Congress[16], "The Impact of Quantum-resistant technologies on network infrastructure & services" on December 6, 2022.
- Luis F. Gonzalez from UC3M showcased a live demonstration about the functionality of the L2S -M component from SIA, in the Open-Source MANO (OSM) 14th meeting in Madrid (Spain). The OSM community had the opportunity to see the advances of this component and move forward the discussion of the feature to be introduced in its source code.
- Luis F. Gonzalez from UC3M participated in the Open Source MANO Mid-Release Meeting 14 (OSM MR14), Ecosystem day[17] on March 8,9 2023.
- XLAB had an Internal XTeam Meeting about AI-based anomaly detection including results from FISHY (TIM), on April 19, 2023.
- CAPGEMINI presented FISHY in the SPARK Europe 2023 - Capgemini's CxO Forum (Technology Leaders and innovators from across the private and public sectors) Versailles (France), on June 1st, 2nd 2023.[18] The team of specialist consultants from engineering and research discussed "Future of Mobility", "Future of Industry" and "Future of Life". Also, it was joined by data scientists and experts in the field of quantum, robotics, generative AI and green technology.

The summary of scientific events that FISHY has participated in its last year is:

- Xavi Masip from UPC and Rodrigo Díaz from ATOS have taken part of the experts' panel in the DRCN conference in April 2023, entitled: "Reliability, are you for real? "
- Diego López from TID gave a talk in the 19th International Conference onIP/loT& Processing + Optical Network (iPOP 2023)[19]: "A Jabberwocky on Network Transformation: Bringing Cloud Principles to Networking Practice" on May 26, 2023, Tokyo, Japan.
- Diego López from TID also participated with a Keynote at the 5th International Workshop on Cyber-Security in Software-defined and Virtualized Infrastructures (SecSoft)[20] "Network and security in supply chains. A fable of mutual utility", on June 19, 2023, in Madrid (Spain).

Finally, regarding EU events, apart from the jointly organized IoSEC workshop, the main event has been the participation in the Cybersecurity Congress within the framework of the European Research Innovation for Cybersecurity (ERICyb) cluster.

[15] https://www.etsi.org/events/2143-2022-12-webinar-making-the-edge-sharp-and-safe-update-on-mec-security
[16] https://congress.layer123.com/event/a2a9b27d-8b30-4cb1-815d-0e7f8d69affb/summary
[17] https://osm.etsi.org/wikipub/index.php/OSM-MR14_Ecosystem_Day
[18] https://sparkeurope2023reg.com/spark-cxo-forum
[19] http://www.pilab.jp/ipop2023/info/program.html
[20] https://www.secsoft-workshop.org/program.html

2.3 Publications

The publications reported in the last year of FISHY are:

- Conferences and workshops:
  - "Incident Handling for Healthcare Organizations and Supply-Chains" by Eftychia Lakka, George Hatzivasilis, Stylianos Karagiannis, Andreas Alexopoulos, Manos Athanatos, Sotiris Ioannidis, Manolis Chatzimpyrros, Grigoris Kalogiannis and George Spanoudakis from SPHYNX, in the 2022 IEEE Symposium on Computers and Communications (ISCC), in July 2022.
  - "A data infrastructure for heterogeneous telemetry adaptation. Application to Netflow-based cryptojacking detection" by Alejandro Moreno (ATOS), Antonio Pastor (TID), Ignacio D. Martínez-Casanueva (TID), Daniel González-Sánchez and Luis Bellido Triana, in the 26th Conference on Innovation in Clouds, Internet and Networks, ICIN 2023, on March 2023.
  - "Security in DevSecOps: Applying Tools and Machine Learning to Verification and Monitoring Steps" by Matija Cankar, Nenad Petrovic, Joao Pita Costa, Ales Cernivec, Jan Antic, Tomaz Martincic, Dejan Stepec from XLAB, in the ICPE '23: ACM/SPEC International Conference on Performance Engineering, on April 2023.
  - "Runtime Security Monitoring by an Interplay Between Rule Matching and Deep Learning-Based Anomaly Detection on Logs" by Jan Antić (XLAB), Joao Pita Costa (XLAB), Aleš Černivec (XLAB), Matija Cankar (XLAB), Tomaž Martinčič (XLAB), Aljaz Potocnik (XLAB), Hrvoje Ratkajec (XLAB), Gorka Benguria Elguezabal, Nelly Leligou (SYNELISIS), Alexandra Lakka (SYNELISIS) and Ismael Torres Boigues, in the DRCN 2023 conference, in April 2023.
  - "An NIDS for Known and Zero-Day Anomalies" by Ayaz Hussain, Francesc Aguiló-Gost, Ester Simó Mezquita and Xavi Masip, in the DRCN 2023 conference, in April 2023.
  - "MONCHi MONitoring for Cloud-native Hyperconnected Islands", by Dulce N. de M. Artalejo, Ivan Vidal, Francisco Valera, and Borja Nogales from UC3M in the ASMTA and EPEW 2023 (EPEW workshop), in June 2023.
  - "A Model for Automated Cybersecurity Threat Remediation and Sharing", by Francesco Settanni, Leonardo Regano, Cataldo Basile and Antonio Lioy from POLITO in SecSoft 2023, June 2023.
- Posters:
  - "Providing Secure NFV Multi Site Connectivity Services", by Jose Manuel Manjón Cáliz (TID) and Borja Nogales (UC3M), in EuCNC & 6G Summit, June 2023.
  - "A Multi-domain Testbed for Collaborative Research" by Ivan Vidal (UC3M), Luis F. Gonzalez (UC3M), Francisco Valera (UC3M), Borja Nogales (UC3M), Raul Martin (UC3M), Dulce Artalejo (UC3M), Diego R. Lopez (TID), Jose M. Majon(TID) and Antonio Pastor (TID), in the IEEE Conference on Sensing, Communication and networking (SECON) conference.
- Journals:
  - "BenchFaaS: Benchmarking Serverless Functions in an Edge Computing Network Testbed" by Francisco Carpio, Marc Michalke and Admela Jukan from TUBS, in IEEE Networks, in September 2022.

On June 30, 2023, FISHY also has the next papers submitted:

- "Scaling Serverless Functions in Edge Networks: A Reinforcement Learning Approach" by Mounir Bensalem, Erkan Ipek and Admela Jukan from TUBS, submitted to IEEE Globecom 2023 conference.
- "Engineering and Experimentally Benchmarking Open Source MQTT Broker Implementations" by Jasenka Dizdarević, Marc Michalke and Admela Jukan from TUBS, submitted to IEEE Globecom 2023 conference.

In total, at the moment of writing this deliverable the number of published papers is 17 conferences/workshops papers, 7 journal papers and 1 poster.

2.4 Liaison with other projects, initiatives & communities

FISHY has established very fruitful collaborations and liaisons during these 3 years of project. Specifically in this last period the summary of activities is:

- Joint infographic FISHY-CYRENE[21] used in the Barcelona cybersecurity congress and in social media. Both projects aim to offer a solution for the cybersecurity of interconnected supply chains (see Figure 4).
- FISHY has participated in the Cybersecurity congress as part of the he European Research Innovation for Cybersecurity (ERICyb) cluster, held in Barcelona, January 31st - February 2nd, with 6 more EU-funded projects. (see section 2.2.1.1).
- 4th FISHY workshop in April 2023 organized with EU-funded projects JCOP[22], PHOENI2X[23] and IntellIoT[24].
- Conference paper "Incident Handling for Healthcare Organizations and Supply-Chains" done in collaboration with AI4HEALTHSEC[25], CONCORDIA[26] and ASCAPE[27].
- Conference paper "A data infrastructure for heterogeneous telemetry adaptation. Application to Netflow-based cryptojacking detection" with PALANTIR[28].
- Conference paper "Security in DevSecOps: Applying Tools and Machine Learning to Verification and Monitoring Steps" with PIACERE[29], MEDINA[30], ICOS[31], SUNRISE[32] and CYLCOMED[33].
- Conference paper "Runtime Security Monitoring by an Interplay Between Rule Matching and Deep Learning-Based Anomaly Detection on Logs" with PIACERE[28] and MEDINA[29].

In total the number of joint activities during the 3 years of project have been 10, summarized in Table 4, and at least 5 papers (1 journal and 4 conference papers) have been published with ACK to more than one EU-funded projects.

[21] https://fishy-project.eu/promotional-material/joint-cyrene-fishy-infographic
[22] https://jcop.eu/
[23] https://phoenix-h2020.eu/
[24] https://intelliot.eu/
[25] https://www.ai4healthsec.eu/
[26] https://www.concordia-h2020.eu/
[27] https://ascape-project.eu/
[28] https://www.palantir-project.eu/
[29] https://www.piacere-project.eu/
[30] https://medina-project.eu/
[31] https://www.icos-project.eu/
[32] https://cordis.europa.eu/project/id/101073821
[33] https://www.cylcomed.eu/

Table 4 - FISHY Liaison activities

Liaison Activities
UPC and ATOS collaborated in the Open Pilot Stream of CYBERWISER. 3 UPC master students participated in SQL injection, password cracking, phishing and Firewall and Network Filtering online courses in January 2021.
The second FISHY workshop has been held on August 17, 2021, and it has been co-organized with the C4IIoT, COLLABS and CyberSANE and in conjunction with the 16th International Conference on Availability, Reliability and Security (ARES 2021).
FISHY participated in the Clustering workshop, December 13,2021 ”Future Proofing and Certifying Supply Chains” organized by the EU projects Assured and CYRENE.
On Friday April 8, 2022, FISHY participated in the roundtable "The Need for IoT Security Standardization & Certification", with the participation of EU projects: CONCORDIA, IoTAC, CYRENE, BIECO and NGIoT. Henrique Santos from University of Minho presented “The Role of Certification to Leverage Trust level in IoT-based Supply Chains: the FISHY vision”,
3rd FISHY workshop: On March 28,2022, FISHY organized the 1st International Workshop on Key challenges in global cybersecurity: Efforts and trends in EU (KCYEU) organized jointly with H2020 CYRENE and H2020 IoTAC, co-located with the DRCN2022 conference.
ATOS liaised with ECSO so that FISHY is featured in ECSO Cybersecurity Awareness Calendar, June 2022 edition as well as the collaboration with CSA Action SWForum.eu to boost the promotion of FISHY results[34] [35].
FISHY has been included in the SWForum.eu hub in their project radar initiative; and it has been especially promoted during July 2022[36] .
Joint infographic FISHY-CYRENE used in the Barcelona Cybersecurity Congress and on social media.
FISHY has co-organized and participated in the Cybersecurity congress as part of the European Research Innovation for Cybersecurity (ERICyb) cluster, held in Barcelona, January 31st - February 2nd 2023, with 6 more EU-funded projects.
4th FISHY workshop in April 2023 organized with EU-funded projects JCOP[21], PHOENI2X[22] and IntellIoT.

[34] https://www.uc3m.es/master/NFV-SDN-5g-networks
[35] http://l2sm.io
[36] https://swforum.eu/project-hub/coordinated-framework-cyber-resilient-supply-chain-systems-over-complex-ict-0

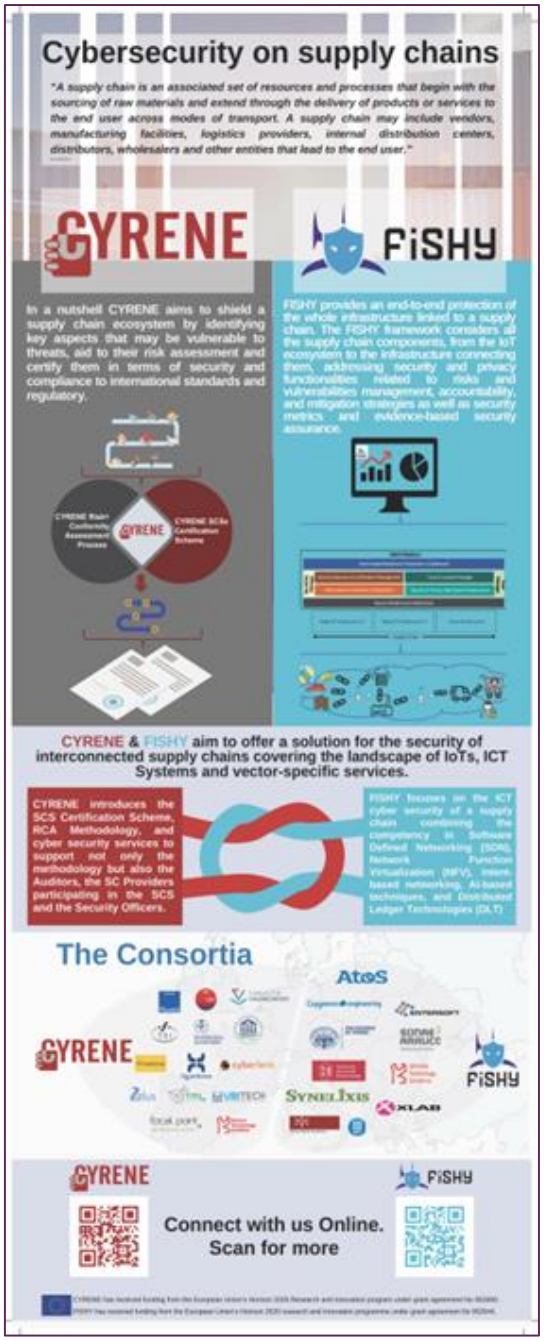


Figure 4 - CYRENE-FISHY infographic

2.5 FISHY Dissemination and Communication Channels/Tools

Table 5 shows the different groups of audience that FISHY is addressed to, as well as which is the specific key message, the tools to address them and the current achievements in each one of the categories.

Table 5 - Groups of audience and tools to reach them

Groups/ categories	Individual actors	Key message	How to address them	Tools	Achievement
General public (GP) and civil society organisations (CSO)	Supply chain, end users	Strong dependence of the whole society on systems built over supply chains	Very accessible language	Social media, website, workshops, fairs, brochures, leaflets, posters	• 8710 visitors to website • 245 Twitter and 160 LinkedIn followers • 4 workshops with 140 attendants, in total • 1 brochure and 5 infographics • 23 blog entries
Industry (I)	Cloud/Edge providers IoT Providers Cybersecurity experts SMEs Large companies	Business benefits of the FISHY framework to address security in ICT infrastructure of large supply chains and ensure cross-resilience	Informative, technical, formal language	Social media, website, workshops, conferences, fairs, brochures, leaflets, posters, Journals/magazines, press release	• 40% of followers on Linkedin come from Industry • Industrial Panel in DRCN 2022 and in DRCN 2023 where 3rd and 4th FISHY workshop were co-located • Participation in 15 industrial events, 3 EU events and 4 scientific events.
Government (G)	Policy makers, decision makers,	Large scale cyber-attacks on supply	Informative, non-technical,	Social media, website,	• 5 Newsletters • Published KERs

Groups/ categories	Individual actors	Key message	How to address them	Tools	Achievement
	national and regional administrations, European Commission services	chains of complex ICT infrastructures can directly or indirectly impact various public services	formal language	workshops, conferences, brochures, leaflets, posters, press release	
Scientific community (SC)	Artificial Intelligence, Cloud & Cybersecurity experts Standardization organisations R&D teams and projects	How findings of the project can contribute on the state-of-the-art of the fields of cybersecurity, AI/ML applications, security assurance, etc.	Technical, formal language	Papers, scientific publications, webinars, conferences, workshops, website, newsletter, open access publications	• 7 journal papers and 17 conference papers with 18 citations[37] • 9 of the 24 papers are open access (6 gold and 3 green access) • 4 workshop with 140 attendants • 5 Newsletters • 23 blog entries

2.5.1 Website

As it has been reported in previous deliverables, the FISHY website, https://fishy-project.eu/, is one of the main ways of communication. All the public content of FISHY is made available on the website, but also because other communication channels, such as blog posts, social networks, and newsletters also use the website as a place to point out. It was designed and implemented jointly by ATOS and UPC. ATOS hosts the website and makes the structural changes, whereas the update of news, publications, events, etc. is led by UPC as leaders of dissemination.

In the last year new changes and updates have been available on the website. First of all, a new item has been added to the menu: Products, including connection to the GitHub repository, the Key Exploitable Results as well as the connection to the FISHY value survey created to assess the FISHY project among our industrial partners (see Figure 5). This FISHY value survey was also sent to projects in the ERICyb cluster, as well as used in our booth in the Cybersecurity congress.

Another change implemented in the last year in the FISHY website was the option to embed videos in our publications, which has been used especially in the FISHY video blogs (see Figure 6).

[37] https://scholar.google.com/

Figure 5 - Products menu in FISHY website

Figure 6 - Embedded videos in FISHY website

Regarding the statistics of our website, in this last year of the project the number of unique website visitors has increased, reaching the number of 8710. The average duration of the visits is 1 min 12 sec, and the number of page views is 19785. More data available about website statistics may be found in Annex, section 7.2.

2.5.2 Social Networks

Social media is used in the FISHY project for disseminating and communicating FISHY results and news. From the beginning of the project a Twitter and a LinkedIn account were created (on LinkedIn at the beginning it was a group as previously reported in past deliverables). In general, the target audience is slightly different from the Twitter audience. Twitter is addressed to a more general audience, but not limited to it; and LinkedIn is focused on a more scientific and companies' audience.

FISHY has also a YouTube account created in September 2020, where general videos of the project have been uploaded, as well as use cases videos and demos. Specifically, on the FISHY YouTube channel there is a general video with the technical and scientific coordinator as well as exploitation leaders describing the project. Three other videos, one per each use case, have been uploaded showing the benefits of FISHY in each one of the use cases. Finally, two videos about technical aspects of the projects have been uploaded giving more technical description for important modules of FISHY. One of these videos describes SIA and the FRF, and another one the TIM module.

The data about these social networks on July 3rd, 2023, is:

- Twitter
  - Link: https://twitter.com/H2020Fishy

- Number of tweets: 318 (+105 during Y3, 9 per month)
- Number of followers: 249 (+71 during Y3)

- LinkedIn
  - Link: https://www.linkedin.com/in/fishy-project-16342920a/
  - Number of posts: 197 (+96 during Y3 8 per month)
  - Number of connections: 168 (+83 during Y3)
- YouTube
  - Link: https://www.youtube.com/channel/UCSDpfCPvFNjRS3RemG0iNQQ
  - Number of videos: 6
  - Visualizations: 598

Most data can be found in Annex 7.2.

2.5.3 FISHY Final Release Campaign

The last mile in terms of communication and dissemination has focused on spreading the FISHY results and achievements.

Product Release Subpage

In the website section it is described a new item on the FISHY website: Products. This new item includes a connection to the FISHY Github repository, the Key Exploitable Results as well as the connection to the FISHY value survey.

Social Media Strategy

To further expose the benefits of FISHY technology adoption, and building on the marketing materials made available, we have campaigned the KERs across social media, in our blog and in external channels. In particular:

- Twitter: short and frequent posts focused on the KER-focused pitch activities to keep the FISHY audience informed of the status and benefits of each KER.
- LinkedIn: a longer social media communication version exposed the KER blog post release and Horizon Result Platform publications.
- Blog: along the project's lifetime we have prepared blog posts to wrap-up each of the KERs elaborating on their technical details in alignment with the exploitation narrative.
- Partners' channels: some of the consortium partners have exposed the KER's in their own internal and external channels exposing their compromise with the described sustainability plan for FISHY.
- Press release: a final press release is being prepared for the end of the project. The idea is to share this press release on the FISHY website, as well as on social media. Also it will be sent to the projects with whom FISHY has established any kind of collaboration. The FISHY partners will adapt this press release to reflect the specific achievements in the company/institution with FISHY.

This communication is a base for the communication with leads and stakeholders, aligned with the consortium's pitch activities at major industrial and community events as discussed in this section.

2.5.4 Newsletters

According to the proposal in previous deliverables and in the project dissemination and communication plan, the main objective of the FISHY newsletter is the direct communications to the targeted stakeholders, such as, the European Commission, researchers and potential interested

investors. The initial Newsletter scheduling has been slightly updated to gather the main achievements as well as the main events in the project (see Table 6). Proposed Newsletter on month 30, #5, was in fact released in Newsletter #4, in month 29 (January 2023); as also details about technical components will be informed in Newsletter #6. This last Newsletter will be released at the end of the project and will also serve to describe the main results/achievements of FISHY in general, but also in the use cases.

Table 6 - FISHY Newsletter scheduling

#	Main Objective	Date planned	Date released
1	To inform about the Project objectives. To involve stakeholders in the project activities and workshops.	M6	M6
2	To report results of the FISHY architecture and achievements in Y1.	M12	M13
3	To involve stakeholders in FISHY project activities and workshops. Describing the results of the 2nd review meeting and the KER.	M18	M22
4	To inform about the achievements in the implementation of the use cases and the participation in the Cybersecurity Congress.	M24	M29
5	To inform about project outcomes and sustainability of these achievements and to provide details about the technical components of the FISHY framework.	M36	M36

2.5.5 Blog

The blog post strategy has been described both in the communication and dissemination project plan, as well as in previous deliverables in WP7. *"The idea of publishing a blog is to spread FISHY to a more general audience and will be shared through a menu option in the Home page of the project website. FISHY blogs will have and extension of one page and the text should be supported by different graphical material, such as pictures, graphs, infographics, etc. Blog posts in FISHY will be published on a bi-monthly basis and will be produced by all partners with the view to communicate project findings as well as ignite interesting conversations. These blogs will be available from the project website. Blogs will be also promoted in the social networks, LinkedIn and Twitter."*

FISHY blogs can be found in https://fishy-project.eu/blog. Table 7 shows the list of blog posts published during the project.

This last year of the project FISHY has published 8 blog posts as well as 5 video-blogs. The blog posts covered topics related to specific modules in FISHY, important events such the Cybersecurity Congress or the meeting with the Horizon Results Booster, as well as liaisons and collaborations. On the other hand, videoblogs have transcribed or described different videos of the project already published in FISHY YouTube channel; 3 of these video-blogs are related to the use cases, and 2 more are devoted to describe more technically two FISHY modules.

Table 7 - Blog posts scheduling

Partner	*Date*	*Titles*
ATOS	*February 28, 2021*	*FISHY: Trustful and smart cybersecurity for supply chains*

UPC	*May 14, 2021*	*Securing IoT nodes in supply of chains*
SYN	*June 30, 2021,*	*Vulnerability Assessment*
SONAE	*August 31, 2021*	*The importance of security in the Industry 4.0 paradigm*
CAPGEMINI	*October 27, 2021*	*FISHY, IoT Security for the automotive Supply Chain*
XLAB	*December 21, 2021*	*The importance of early detection of vulnerabilities and attacks for a healthy supply chain*
POLITO	*March 7, 2022*	*Easing the burden of network configuration: a capability-driven approach*
TID	*May 7, 2022*	*A reference framework for FISHY*
TUBS	*June 30, 2022*	*Intent-based Resilience Orchestration in Supply Chains*
ENTERSOFT/SYN	*September 29, 2022*	*Experiences from validation of FISHY in the Farm to Fork use case*
STS	*October 31, 2022*	*The role of Security Assurance Certification Module on a Supply Chain*
UMINHO	*December 22, 2022*	*Security and Privacy Data Space Infrastructure*
XLAB, UPC, ATOS, UC3M	*January 31, 2023*	*FISHY's Demo & Booth at the Barcelona Cybersecurity Congress 2023*
XLAB	*April 12, 2023*	*Wrapping-up the Horizon Results Booster experience with innovation management training and a hands-on workshop*
CAPGEMINI	*May 15, 2023*	*Video-blog: FISHY SADE use case*
SONAE	*May 15, 2023*	*Video-blog: FISHY SADE use case*
SYN	*May 16, 2023*	*Video-blog: F2F use case demo*
SYN	*May 26, 2023*	*Using blockchain technology to secure security information*
UPC	*July 25, 2023*	*FISHY liaisons and collaborations*
XLAB	*August 16, 2023*	*Key Innovations in Supply Chain Cybersecurity and Resillience that Make Sense in Today's Industry*
XLAB	*August 30, 2023*	*Video-blog: TIM*
UC3M	*To be added*	*Video-blog: SIA-FRF*
ATOS/UPC	*August 31, 2023*	*[to be announced]*

2.5.6 Press releases

The idea of press releases was to inform about how FISHY can produce benefits to the stakeholders' groups, such as: General public and civil society organisations, Industry, Government and Scientific community. At the beginning of the project FISHY established a KPI of 2 press releases along the

project, one at the beginning and another at the end of. The first of them was published on the FISHY website[38] and made available to the FISHY partners to be adapted and published on their websites.

However, the same idea of press release adaptable to different partners was applied in the ERCyB cluster during the preparation of the participation in the Cybersecurity Congress. Led by IoTAC a press releases was prepared and adapted by each one of the EU projects in the cluster, and published in each one the websites as well as disseminated on social networks[39].

Finally, at the moment of writing this deliverable FISHY is preparing a final press release. The FISHY partners will adapt this press release to reflect the specific achievements in the company/institution with FISHY and publish it in their own websites and on social media.

2.5.7 Dissemination & communication toolkit

The following section describes the printed/published online dissemination material prepared in order to spread the message of FISHY. During the first two years of project and due to the pandemic situation the consortium decided to publish only this material on the FISHY website[40] and on social media. Initially this material was: a brochure, a project presentation, a white paper and 4 infographics.

During the last year of the project FISHY had the opportunity to use this material in different face-to-face meetings such as GAs and the Cybersecurity Congress, where FISHY brochures were made available to the public. Moreover, in this last year new material has been produced such as a joint infographic with the H2020 CYRENE project (see Figure 4 - CYRENE-FISHY infographic), as well as a second FISHY poster (see Figure 7 below).

[38] https://fishy-project.eu/promotional-material/press-relase
[39] https://fishy-project.eu/news-events/press-release
[40] https://fishy-project.eu/project/promotional_material

Figure 7 - 2nd FISHY poster

3 Standardisation

3.1 Progress Highlights

During this final period, FISHY partners have continued the activities previously reported, trying to maximise the adoption of project concepts by different work-items and activities, seeking for long-term impact, even beyond the project lifetime.

Beyond direct contributions to relevant standards organisations, especially the IETF, ETSI and 3GPP, these activities have translated into a number of work items in these organisations, as well as open-source projects focused on the convergence of network and cloud technologies. These new work items are specifically related to supply chain support and lifecycle management of ICT services, as detailed in the following sections.

3.2 Contributions to Standards Development Organisations (SDOs)

3.2.1 IETF and IRTF

Within the IETF, and its research branch IRTF, FISHY has focused on the following Working Groups (WG) and Research Groups (RG):

- **OPSAWG** (on general issues regarding network operation), with the approval for publication of the definition of an architecture for service assurance [6], and contributing to a document defining the concepts and data models for network asset lifecycle management [7].
- **NMRG** (on new aspects of network management), with the publication of RFC9316 [8], an analysis of intent declarations and their impact on network management practices.
- **COINRG** (a research group on the convergence of cloud and network technologies), evolving the Cooperating Layered Architecture for SDN (CLAS) [9] to integrate compute and data infrastructure awareness.

As most significant results, the proposal of the **SCITT** (Supply Chain Integrity, Transparency, and Trust) [10] WG, with FISHY SIA included as enabler, was approved by the IESG. And we participated in the chartering and approval of another new Working Group on Network Inventory Model (**IVY**) [11], incorporating some of the asset lifecycle management mechanisms mentioned above.

3.2.2 ETSI

The FISHY team has continued its engagement with the *Network Transformation* initiatives in ETSI, extending its outreach to activities directly related to security. Two specific contributions have been submitted to:

- **ISG ZSM**, on service interfaces for trust management [12].
- **ISG NFV**, introducing the SIA core component L2S-M [13] to the Network Operator Council (**NOC**), as a way to make the network models of Kubernetes and NFV converge.

Regarding the definition of new work-items supported by the results of the project, we participated in the preparation and submission of a set of work-item proposals [14][15][16] for **TC-CYBER**, on testing and assurance verification for optical network devices.

3.2.3 3GPP

The contributions to 3GPP have focused on **SA3** (security aspects), including considerations on zero-trust security for 3GPP 33.894 [17], and proposals for new work items to incorporate IETF ACME in certificate management procedures [18][19], and on the application of zero-trust security principles in mobile network security [20][21][22][23][24][25][26].

3.3 Contribution to open source projects

The project team has continued the activities that were initiated once applicable results became available, and previously reported in D7.3. The original contributions to the OpenConfig [42] project has been followed-up, as well as the interaction with the upstream communities (like Wazuh) that are reported as part of the KER description in the section on exploitation results. In addition to this, three specific activities have results worth highlighting:

- The contributions of the SIA connectivity mechanisms, around L2S-M, is progressing towards its inclusion in OSM Release FOURTEEN, with a demonstration of its capabilities at the OSM MR14 Ecosystem Days in March 2023 [27]. L2S-M is also available as a standalone component at GitHub [28].
- The availability of the FISHY Reference Framework (FRF) central services and the FISHY Sandbox distribution for Iteration 2 [29].

The recent approval of the ETSI Software Development Group [30] *OpenSlice*, focused on the development and demonstration of an open Network Operation Support Systems, incorporating some features based on the FISHY SIA principles.

3.4 Strategy for EU cybersecurity certification

Cybersecurity is an area where, given its nature, there is a vast diversity of possible solutions. These solutions, by definition, impose restrictions on functionality and, therefore, on attractiveness for the end user. That is, from the business point of view there is no desire to implement very secure solutions. On the other hand, there are application areas, such as healthcare, or critical infrastructure, where special consideration with cybersecurity issues must be mandatory. Standards and certification play an exclusive role in this context of non-compulsory versus willingness to promote cybersecurity.

No wonder then that the vast majority of developed countries and the EU, for all the more reason, appear at the forefront of creating strategies to address this fundamental pillar (cybersecurity) of digital transformation. The EU mandated ENISA to lead the definition and implementation of this strategy, which has worked closely with several other institutions dedicated to standardisation (in particular ISO, IEC and CEN). Of this effort, the creation of "The EU cybersecurity certification framework" [31] deserves particular mention. In addition to the political importance of asserting a priority for a technological development ecosystem based on cybersecurity requirements that protect a rapidly developing "digital" Europe, that framework motivated the creation of "the European Cybersecurity Certification Group" (ECCG) [32]. This group brings together standardisation institutions representing the member states and, in coordination with ENISA, has worked towards creating certification frameworks suited to the needs of the EU.

In this sense and continuing the work started in 2017, the "EU Cybersecurity Act"[33] was published. It is a regulatory proposal that aims to harmonise cybersecurity certification activities within the member states. Given the large number of institutions involved and, above all, the differences in maturity levels among the members, it is clear that this will be a long and challenging path but

strategically fundamental to achieving the goals of a consolidated and secure Digital Europe. Under the EU Cybersecurity Act, proposals are being developed for various certification schemes, namely:

- EUCC (Common Criteria based European candidate cybersecurity certification scheme), aimed at product certification and based on the well-known ISO/IEC 15448 and 18045 standards; this scheme has already been published and is at an advanced implementation stage.
- ECCG (Cloud Security Certification), which is in the final publication phase.
- 5G Security Certification, which is in progress.
- IoT Security Certification, which is still in the planning stage.
- Healthcare, Automotive, and Cybersecurity Market, are chosen areas for future developments.

Outside the scope of the EU Cybersecurity Act, but even so, with enormous relevance, the effort to create an education-oriented certification reference, the European Cybersecurity Skills Framework (ECSF), is worth mentioning. This framework has a different purpose than the previous ones. However, by seeking to identify skills, knowledge and capabilities for various professional roles related to cybersecurity and promoting a common education platform, it will enable the efficiencies of the efforts described above.

From this brief introduction to cybersecurity certification efforts in the European Union, the strategic importance attributed to this area is evident, as well as the effort already made in this direction with what remains to be done and which entails essential challenges.

3.5 Community Engagement

The importance of Open Source Software and of the Communities associated with it highly contributes to the excellence of European research and development, and for the health and prosperity of the European industrial landscape. In line with the European Commission's Open Source Software Strategy [34], FISHY contributes to the innovation and autonomy of Europe's digital infrastructure, particularly in the security and resilience of supply chains.

To guide these contributions, we defined the five pillars of open research at FISHY that promotes the collaboration between researchers, the dissemination and reuse of innovation, and the sustainability of the technology developed in this project. To follow the progress of this community engagement, we will be considering several metrics: GitHub contributors to KER; social media followers of lead partner; and research papers and conferences exposing the KER. Some of these are already described in the section 2 in the context of the project's dissemination efforts.

3.5.1 P1. PUBLIC REPOSITORY & DOCUMENTATION

This is a common approach to practical exposure in EC-funded projects complying with the open research directions of EC, as addressed in the DoA. A substantial part of FISHY's technology is made of open source code, shared on the Project's repository: github.com/H2020-FISHY

In this way, we provide the basic functionality of the project's technology on a unique open source repository, with code well documented and licensed mostly through Apache 2.0 or compatible licensing.

3.5.2 P2. KER-SPECIFIC UPSTREAMING

Most FISHY consortium partners that are IP owners and technology providers contribute to several OSS communities. This is directly connected with their internal priorities and reflects in the further development of the code produced in FISHY. Based on that we can consider the contribution to specific communities through the specific KERs that these partners develop. More details can be found in the following section, that discusses these KERs, namely:

- SYN: Smart Contracts with verification and immutability of events and policies produced by the FISHY platform.
- XLAB: contribution to Wazuh based on the extensions of the technology towards the objectives of FISHY's Trust and Incidence Management (KER2), XLAB has dockerized Wazuh deployment and has Ansible deployment scripts available internally, that will be further developed and used in forthcoming projects.
- POLITO: Integrity Assessment Toolkit, Trust monitor extension in OSS.
- TID: Link-Layer Secure connectivity, ETSI Open Source MANO (OSM), CCIPS.
- UPC: PMEM, Trustworthy identification and authentication, Blockchain, improving the IP Background.
- TUBS: IRO mostly from scratch.
- STS: Security Metrics Assurance, Evidence & Certification Management Platform extension and improvement to IP Background.
- UMINHO: Framework for IoT InfSec evaluation, the Zeek log collection and log analysis, the SPI itself and the SPI implementation including Data Management module to provide format conversion (to CEF format) and privacy protection function.
- UC3M: Link-Layer Secure connectivity, ETSI Open Source MANO (OSM).

This is reflected in the project open source contribution page (see the Product/Open FISHY tab at https://fishy-project.eu/ and github.com/H2020-FISHY) and the IP Results assigned with an Open Source license in the list found in the annex of this document.

3.5.3 P3. LOOKING FOR FURTHER OSS OPPORTUNITIES

We are identifying IaC-focused and other FISHY-related communities to engage with from M18 onwards. Highlights are:

- GAIA-X: XLAB has been contributing to the cloud orchestration of GAIA-X and presented the FISHY security solutions in one of the technical meetings.
- OSM: Following-up the ongoing contributions made by UC3M and TID, based on the L2S-M and CCIPS components in SIA.
- OSL: Once this ETSI SGD is formally constituted, TID and UC3M intend to bring the SIA NBI (NorthBound Interface) mechanisms to support network operation and management.
- SWForum.eu: The project was highlighted in the SWForum Spotlight initiative[41] exposing the main vision and technology in the project, as well as some basic information. It was further discussed in the SWForum Discussion "Unbreakable Chains: How AI is Fortifying Cyber Resilience in Supply Chains"[42]
- Cyberwatching.eu: The project is also exposed through its seven KERs at the marketplace of the Cyberwatching.eu initiative[43], where each of the outcomes of the project are exposed and labelled according to the National Institute of Standards and Technology (NIST), highlighting benefits and referencing success stories from the use cases.
- ECSO (European Cyber Security Organisation): The consortium has been investigating the ways of contribution to this initiative, having identified two options that are to be further explored in the near future: (i) the ECSO Marketplace[44] that will have its much awaited global launch in

[41] https://swforum.eu/project-hub/project-spotlight/project-spotlight-fishy
[42] https://swforum.eu/online-sw-forum/cybersecurity/8/unbreakable-chains-how-ai-fortifying-cyber-resilience-supply-chains
[43] https://www.cyberwatching.eu/projects/3097/fishy/products/fishy-cyber-resilient-supply-chain-system
[44] https://ecs-org.eu/activities/ecso-marketplace/

the Q4 of 2023; and (ii) the Cybersecurity Made in Europe label[45] with representants in Spain and other countries of Europe, but that required an annual membership fee that was not planned and will be considered in the context of the further business development beyond the lifetime of the project.

3.5.4 P4. STANDARDS

Project results have been contributed to different standardization efforts to maximize their industrial impact, and more specifically their application to the scenarios identified in the use cases. Standards activities of all nature (SDOs, industry associations, open-source communities) have been tracked, analysing the most relevant opportunities, and bringing not only results as direct contributions to existing activities, but also supporting the emergence of new activities based on relevant FISHY outcomes. The project team has sought the collaboration with other related research projects.

3.5.5 P5. OPEN RESEARCH

As discussed in section 2, the open nature of the research developed in this project is very important for the appropriate dissemination of the project's outcomes, contributing to their sustainability in the hands of other researchers and projects. For these reasons, all open access publications and public deliverables are shared on our Zenodo community page (see zenodo.org/communities/fishy/). The public deliverables and green/gold access research papers are available through Zenodo.

[45] https://www.cybersecurity-label.eu/

4 Exploitation

The following section reports on the activities of Task 7.3 that focus on the exploitation of the project, during the Y3 reporting period of M25-M36. This builds on the first report published within the deliverable D7.2 and includes the IPR management, the business and product development, and the innovation tracking, leveraging other tasks of the project (e.g., the FISHY radar in Task 2.1).

In this section, we discuss the activities towards the maximisation of the industrial impact over targeted verticals and elaborate on the achieved value proposition business models for the stakeholders. Moreover, we describe the exploration of the market positioning building on the FISHY Radar achievements in WP2, as published in the deliverable D2.4.

We also update on the individual and joint exploitation plans by the consortium partners towards the sustainability of the project and summarise the third and final interaction with the FISHY Advisory Board.

4.1 Overview

4.1.1 Highlights

During this final reporting period we have intensified the efforts in exploitation activities, leveraging the final technological releases of FISHY and aligning with the communication strategy to maximise impact also through the joint actions organised in main events (as described in section 2). Bundling the 25 IP results produced and analysed in this project, we have extended the 17 key results identified at the proposal stage, to 20 key results reflecting the R&D in the project (listed in the annex of this deliverable), distributed through 7 Key Exploitable Results (KERs) analysed across 3 phases of the supporting program of the Horizon Results Booster.

Following up on the work developed in the context of the FISHY Radar, particularly regarding the analysis of technological imperatives together with the use case owners of the project, we have explored together the potential of FISHY in boosting their business cases. In that context, we have identified user roles and drafted user stories to prepare the customer journey in a co-creation fashion, to improve the pitch capabilities to these and similar industry sectors and target markets.

In the context of business development and sustainability planning, we have defined the Open FISHY from the OSS IP results, the paid premium features from the commercial IP defined, and the potential for further (paid) customisation. We have also discussed the partner exploitation plans per KER, where we base our sustainability strategy, reflecting both the impact on the consortium's SMEs by the new features made available through the R&D in the lifetime of the project, and the impact in European SMEs outside the consortium that have now access to innovation in the context of supply chain resilience using the FISHY technology flexible to their needs and budget.

4.1.2 Exploitation KPIs

Throughout this final reporting period we have successfully achieved the aims planned in M6 as published in D7.1, together with the overall exploitation roadmap to the lifetime of the project (see Table 8). While the IP Results and exploitable results in this deliverable reached bigger numbers than planned (much related to the unplanned R&D that usually happens in the lifetime), the product development and business development aligns well with the initially planned KRs and KERs. Due to the COVID-19 restrictions in travel and the event cancellation, happening in the first part of the project, the joint actions became easier to organise but less impactful, substituting face-to-face interaction through matchmaking chat rooms that do not favour the lead generation. We have overcome those

difficulties based on the cohesion of the consortium in diversifying these pitch activities and pitch materials. We highlight the joint consortium participation in the Cybersecurity Congress in Barcelona, and in the DRCN Conference in 2023.

Table 8 - Updated KPIs for FISHY's exploitation activities

KPI	Description	Metrics	Target (M36)	Threshold	Status (M36)
IPR Management	Identification, analysis and protection of IP results	# of IP instances logged and analysed	20	15	25
Innovation Management	Analysis of the FISHY innovations with market potential	# of exploitable results analysed	15	10	20
Product Development	Analysis of solutions from FISHY KERs	# of solutions prepared	10	5	10
Business Development	Focused business models based on joint exploitation	# of business tools prepared	5	3	9
Go-to-market	Coordinated communication of the FISHY Key Exploitable Results (KERs)	# of actions	5	1	7

The IPR management results are listed in the annex of this document and discussed in section 4.4.1. The innovation management outcomes, i.e., the exploitable results and domains of action published in earlier deliverables of this WP7 and their final update is also in the annex. The product development reflects the work throughout this project on the 7 KERs (one of them being the platform as a whole), the additional (non-essential) paid services (AI-based anomaly detection by LOMOS, XL-SIEM, the continuous risk assessment engine, an evidence-based data monitoring platform, and the security assurance & certification management platform), and two general purpose services related to the open source offer (training and customisation). In what relates business development, we have prepared 9 business tools for FISHY across the lifetime of the project (BMC, SWOT, lean BMC, risk model, value proposition canvas, Javelin board, MTRL assessment, BOSAT assessment, Technology Adoption Lifecycle), some of which with the supervision of several Horizon Results Booster (HRB) programmes. Moreover, the go-to-market actions include pitch decks and 1-pagers for each KER (with pitch reviewed at the go-to-market coaching programme by the HRB), as well as updated profiling of these in the Horizon Results Platform and Cyberwatching.eu, all of which in use by consortium partners participating in the joint events discussed in section 2.

4.1.3 Plan beyond FISHY's lifetime

In Figure 8 we briefly present the timeline for the project's exploitation activities, with a highlighted third year and a two-year window into the future. In that time beyond the lifetime of the project, the consortium will further implement the go-to-market strategy, analysed in the third and final coaching program of the Horizon Results Booster, leveraging the momentum created by the intense efforts in pitching the value message of the KERs (see section 4.2.2).

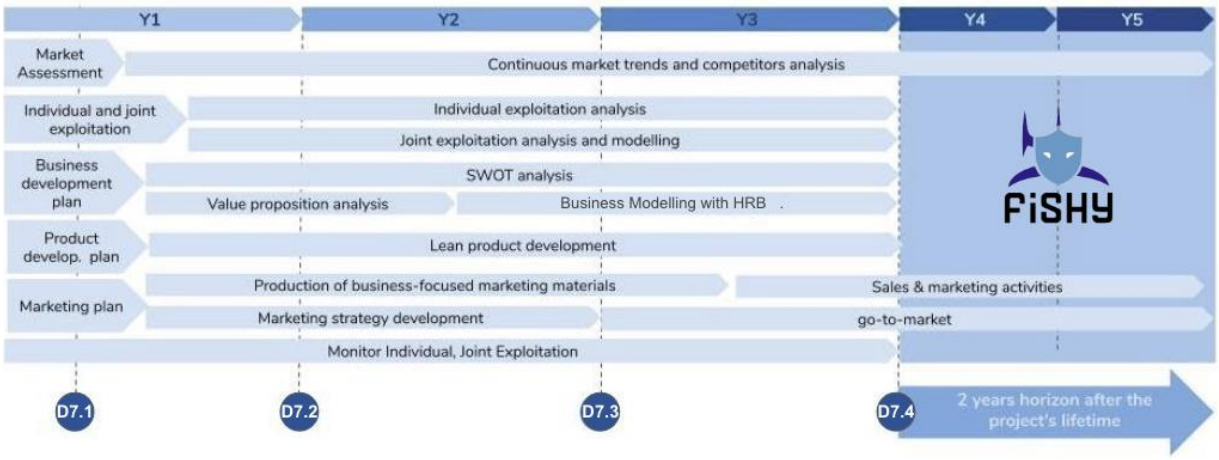


Figure 8 - Updated timeline for FISHY's exploitation activities

The business development (detailed in section 4.3) will follow the opportunities generated in the light of individual and joint exploitation. The sustainability strategy of FISHY includes the maintenance of the code, the development of new features by paid contract or other funding sources (e.g., new projects), and the consulting, training and premium services offered to complement the available OSS contribution.

4.2 Horizon Results Booster

The European Commission's initiative Horizon Results Booster (HRB) has been following the exploitation activities of the project during most of its lifetime, across three coaching programmes. Some of this work was already reported in the deliverables D7.3 and D7.6, and in this section we report the activities that took place and the impact that the program had in the tasks of WP7.

4.2.1 Booster Experience and Coaching Activities

The FISHY team has been leveraging the advantages of the European Commission's initiatives since the start of the project and, in early 2023, we were accepted for a third and final consulting round with the assigned representative of the Horizon Results Booster programme,. On 22/03/2023 and 04/04/2023 we had the introductory call and the hands-on workshop for the 3rd and last session on the Horizon Results Booster (HRB) coaching on Innovation Management under the Go-to-Market service, where we have prepared a series of documents on KER 1 FISHY Platform. This last round focused on innovation management and our goal was to enhance the already mature exploitation work we have been developing so far, as part of the Go-to-Market service. This is an exciting opportunity for us, and we are thrilled to share it with our audiences. This coaching programme follows our previous two rounds on Exploitation Strategy and Business Plan Development, where we analyzed the three main KERs reflecting the FISHY platform, the vulnerability assessment tools, and the IRO. We also delved deep into the business opportunities for the FISHY platform, preparing its value proposition canvas and consequent lean business model canvas.

This intermediate coaching programme was awarded to FISHY in April 2022 and planned to Q4 of 2022, dedicated to the Business Plan Development focusing on the KER 1, i.e., the FISHY Platform Backbone and dashboard. This KER was identified as the one in the ESS analysis with more need of further exploitation work and can be extended to the business model of the full-stack FISHY solution that we are addressing in the last year of the project. The following can summarise the work done in the BPD (not yet reported in the previous deliverables D7.6 and D7.3):

1. Value Proposition Canvas: we listed the FISHY offer based on OSS and premium features/consultancy, identifying the main user activities, pains and gains (later evaluated and ranked by all the use cases), to rewrite the unique value proposition (UVP) from it.
2. Lean Business Model Canvas: based on the information collected at the Business Plan Structure document (following the previous work with HRB earlier in the year), and centred on the rewritten UVP, we prepared the business model that is expressing the realistic joint exploitation taking into consideration the different nature of FISHY partners and the most recent update of their individual exploitation plans.
3. Javelin Board: in this exercise we worked directly with all the use cases to validate hypothesis on how FISHY is solving the problems in the industries where our use case partners are present, and refine the business model based on that.

The partner's active participation was comprehensive, with 9 partners of 6 institutions attending the meetings held on the 22/03 and 04/04.

In this final programme, we started by exploring funding opportunities at national and European levels. Our focus was on the new programme of the European Research Council, EIC Transition [35], which is particularly relevant for the takeover of promising research results. We also looked into the Digital Europe programme, which could complement the opportunities in Horizon Europe innovation action calls. During the second session of this programme, we had a hands-on workshop format. We went through the wide range of exploitation materials we have been preparing in the intense first months of 2023. These ranged from the value proposition canvas and lean business model canvas for each of the seven key exploitable results (KER). We focused on our second KER (TIM - Trust and Incidence Management) to be explored in this coaching session, reflecting the FISHY Open Source Software end-to-end solution, which is provided at the end of the project and complemented by paid features that expand the performance of the open-source technology, making FISHY's business model consistent.

The partner's active participation was comprehensive, with 11 partners of 8 institutions attending the meetings held on the 22/3 and 4/4. After this final session, we reviewed and republished the KER profiles at the Horizon Results Platform and the security-related assets at the Cyberwatching.eu Marketplace. We are proud of what we have accomplished so far and excited to be a part of this cutting-edge work. We are confident that the knowledge and skills we've gained through the Horizon Results Booster programme will be instrumental in taking our innovation management to the next level. We are grateful for the support we have received and look forward to leveraging our new knowledge and skills to continue to innovate and grow.

All the exploitation plans finalised during the workshop were collected by the expert for a further round of comments. Even though elements were clearer and better defined, some elements still need further consideration in the forthcoming work, as actions envisaged, include: (i) the identification of early adopters; (ii) the description of the process to involve decision-makers and other departments within the organisation responsible to take over on the roadmaps; (iii) Milestones and KPIs to be defined and agreed.

4.2.2 Lessons Learned and Fostered Activities

Following a first BOSAT self-assessment (later discussed in detail in section 4.4.3), we were able, as a consortium, to identify the weaknesses and the points to improve in building a robust exploitation for the project's main outcome, the FISHY platform for supply-chain security and resilience. We have prepared its business model based on the lean canvas and the value proposition canvas explored in the second coaching sessions (the *business model development* program), further expanding these business development tools to the KER 2, which was the topic of analysis in the third and final coaching session (under the program *Go-to-market - Innovation Management*).

Based on this knowledge gained, and as a follow-up to the HRB coaching, we have analysed each of the other five KERs under this perspective to generate, during our monthly WP7 workshops, their value proposition canvas and the lean canvas (see section 4.3.1). The usefulness of the exploitation outcomes in the production of these materials is noticeable and, particularly, in the joint exploration of their content. They served us also to improve our pitch deck and other marketing materials with a mature value message for each of the KERs of the project, as exposed by their update in the Horizon Results Platform through the following URLs and corresponding IDs:

- KER1: FISHY Platform [42289] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/horizon-results-platform/42289;keyword=fishy
- KER2: FISHY Trust & Incident Manager [42318] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/horizon-results-platform/42318;keyword=fishy
- KER3: FISHY Intent-based Resilience Orchestration [42320] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/horizon-results-platform/42320;keyword=fishy
- KER4: FISHY Security Assurance & Certification Manager [42333] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/horizon-results-platform/42333;keyword=fishy
- KER5: FISHY Security & Privacy Dataspace Infrastructure [42335] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/horizon-results-platform/42335;keyword=fishy
- KER6: FISHY Enforcement & Dynamic Configuration [42337] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/horizon-results-platform/42337;keyword=fishy
- KER7: FISHY Secure Infrastructure Abstraction [42339] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/horizon-results-platform/42339;keyword=fishy

Moreover, based on the discussions and the documents shared by the HRB expert, we prepared the Technical Adoption Lifecycle for FISHY, based on the expectations of the project's use cases as early adopters, that will help the consortium understand how to engage potential new users in the extended network of the FISHY partners. For that aim we have also circulated a value survey. Understanding the FISHY customer and their needs as well as empathy with the target audience (customers or users) is very important to the success of exploitation activities (following what was done in the value proposition canvas). It is important to avoid tunnel thinking (e.g. get an outside perspective through the mentioned survey).

The Javelin board was prepared with the HRB bringing together KER leaders, IP owners and use case partners. The exercise of specifying different narratives for the different use case domains addressed in the project has shown to be a useful insight on the application of FISHY innovation to the corresponding industrial sectors. Based on that, we have written the success stories of FISHY, and prepared the user roles and user stories for the FISHY platform, exploring which user roles defined will interact with the different functionalities of FISHY. This information also helped identify opportunities at the use case validation stage, contributing to an update to the Horizon Results Platform and Cyberwatching.eu Marketplace public profiles (see section 4.3.3).

The problem is not to fill-in these canvas but to identify the right information and content without using the own opinions but rather to breakdown the specific needs of the target audience. The Porter's 5 forces model, published in the preceding WP7 deliverable, was pointed out by the HRB expert as an important element to approach the audience with the right tools. Similarly, the exploitation efforts and business development methods and tools used by FISHY were much appreciated by the HRB expert providing opportunity for some discussion.

4.3 Innovation Management

This section updates the public deliverable D7.3 and the confidential deliverable D7.6 on the activities of innovation management. We will start by describing the KER positioning regarding the current legal and regulatory framework in the context of the individual exploitation opportunities. Then we describe the progress of the IPR management also reflected in the open source repository structure and the final business model presented later in this section. To close we present the new findings from the perceived value of each KER and summarise their exposure to the scientific community and to the general public.

4.3.1 Innovation Assets and Key Exploitable Results

During this final reporting period we have invested a substantial amount of our time in refining the Key Exploitable Results, their role in the FISHY solution, their business opportunities and their exploitation narrative. These are grouping the 20 exploitable results identified in the FISHY technology development, listed in the annex 7.3 of this report, extending those results reported in the preceding WP7 deliverables. Figure 9 shows those key exploitable results as distributed by domains of action and serving as technological basis to build the project's KERs.

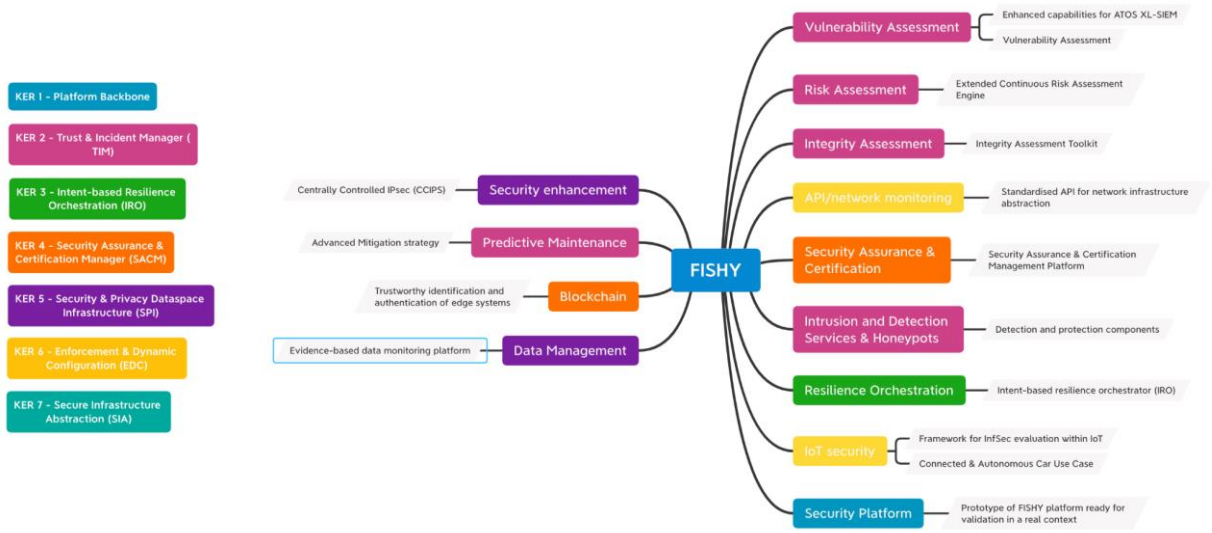


Figure 9 - FISHY's exploitation results distributed by domains of action and KERs

In the process of reorganisation of key results, domains of action, KERs and IP results we have solved some inconsistencies that were related to the timing of desk analysis in the early stage of the project. In that, the "ILT-based warehouse management system" is deleted from IP results and exploitable results lists. At the beginning of the project, the boundaries of the pilot-specific software platforms and of FISHY were not clear, and we now realise that the ILT-based warehouse management system is a pilot specific system and not part of the FISHY platform.

Similarly, XOpera was planned to be used for cloud orchestration at the DoA, but during the early planning stages of the project, the choice of the cloud containerization solution (Kubernetes) and the specifics of the networking configuration needed for proper functioning of inter-domain communication of different FISHY components made the use of xOpera cumbersome. In addition, XLAB was not in charge of the setup and maintenance of the cloud-capable runtime of the FISHY Platform, known as the FISHY Reference Framework (FRF) and also only integrated with the network connectivity component of SIA, NED, which was the main driving force behind the choice of cloud orchestrator and increased demands of networking configuration.

On the other hand, the original plan to apply the "Ordered Proof of Transit (OPoT)", "Netphony" "mcTLS", "MAMI STAR" and "TIB blockchain" features to address network topology was updated, given the evolution of the other SIA components like L2S-M, to support integrity and confidentiality of infrastructure by means of the "Centrally Controlled IPsec (CCIPS)". The combination of L2S-M ad CCIPS allowed us to extend the "Privacy enhancement" to a more general "Security enhancement", as a better description of its exploitation pathway.

During the Horizon Results Booster coaching program *Business Plan Development*, later on refined at the following program *Go2Market - Innovation Management*, we prepared the Value Proposition Canvas and the Lean Canvas for KER 1, the FISHY Platform. This KER was also part of the three KERs in analysis in the initial Exploitation Strategy Seminar, and is representing the full spectrum of the FISHY end-to-end solution that will later (in section 4.3.3) be analysed from a business development perspective.

From the knowledge gained at the Horizon Results Booster, we were able to prepare the value proposition canvas for each of the KERs. This method helps ensure that a product or service is positioned around what the customer values and needs [36]. A characterization table made available at the HRB coaching sessions also helped collect the necessary data to write the lean business model canvas for each of the KERs in the project.

Those outputs (confidential and published in the deliverable D7.7) allowed us for a final update to the Horizon Results Platform public profiles, and can be summarised by the following. The KER 1 comprehends the full spectrum of the FISHY solution where we can expose the following:

Problem: Guaranteeing data security in a supply-chain context, ensuring data sharing with external entities and cybersecurity of IoT devices, as well as edge and cloud infrastructures.

Solution: Easing FISHY platform usability, making the whole system user-friendly and ready to be used for different users according to their expected profile and thus permitted functionalities.

Value: Enhanced customer experience: Easy access to the supply chain cybersecurity in a single window with meaningful and useful output

Innovation: Frontend designed to support the specific needs inherent to the heterogeneous and diverse supply chain scenario also supporting the hybrid model FISHY is envisioned to support.

Usefulness: A single entry point for different actors (users) that will centralise certain security aspects of the supply chain. The different actors can control the security configurations of the domain they administer, with flexible discovery of multiple attacks.

Limitations: non foreseen for the commercial FISHY version (for the current version, see D6.4).

Moreover, we highlighted the value of SIA as recommended by the reviewers, being an essential piece in the discussed FISHY offering based on the FRF capabilities.

4.3.2 FISHY Value Survey

During the final reporting period we have conducted a survey, released at FISHY's joint action event at the Barcelona Cybersecurity Congress, aiming to evaluate the perceived value of the innovation

provided by FISHY. We used our network to invite experts and practitioners to answer 9 questions related to the benefits of each of FISHY's KERs.

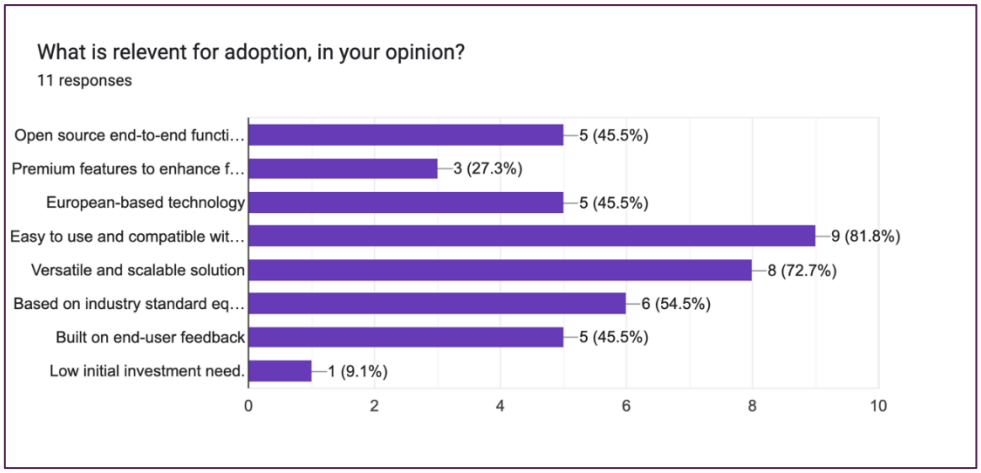
Additionally, we have invited our consortium partners, particularly those holding use cases, and those originated from the liaisons held in the lifetime of the project to ask the staff in positions matching the identified FISHY users to answer the survey. The survey was answered by 11 experts with a variety of roles as follows:

- Owner (of the complete supply-chain)
- Manager (root node of the supply chain)
- Participant (as part of the supply chain)
- Demonstrator (all roles)
- Administrator of the IT platform integrating all supply chain island
- IT Cybersecurity lead

The survey initiates with a short message explaining the aim of the survey, and the project video providing the introduction to the project's main concepts from the point of view of the project's implementation, technical coordination and innovation management. It follows by inquiring on the most relevant priority in supply chain security in resilience, to which we have the following available options:

- Open source end-to-end functionality
- Premium features to enhance functionality
- European-based technology
- Easy to use and compatible with existing systems
- Versatile and scalable solution
- Based on industry standard equipment whilst remaining vendor-independent
- Built on end-user feedback
- (other)

Here, we have obtained the following results highlighting the ease of use and the flexibility/scalability of the FISHY offering, as shown in the following chart:

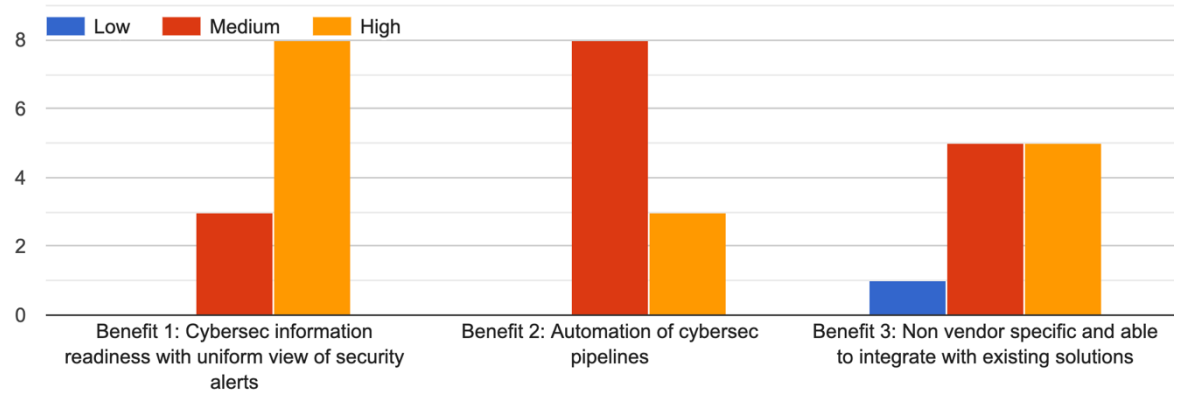


The seven KER-related questions then follow, where the interviewed are to choose between the most relevant of their benefits, as identified by the FISHY team. The results are as follows:

4.3.2.1 KER 1: FISHY Platform

In this first KER, representing the end-to-end solution, there is consensus on the relevance of the readiness of the cybersecurity information with its unified dashboard view. The focus on the automation of cybersecurity pipelines is also seen as important as is the non-vendor lock.

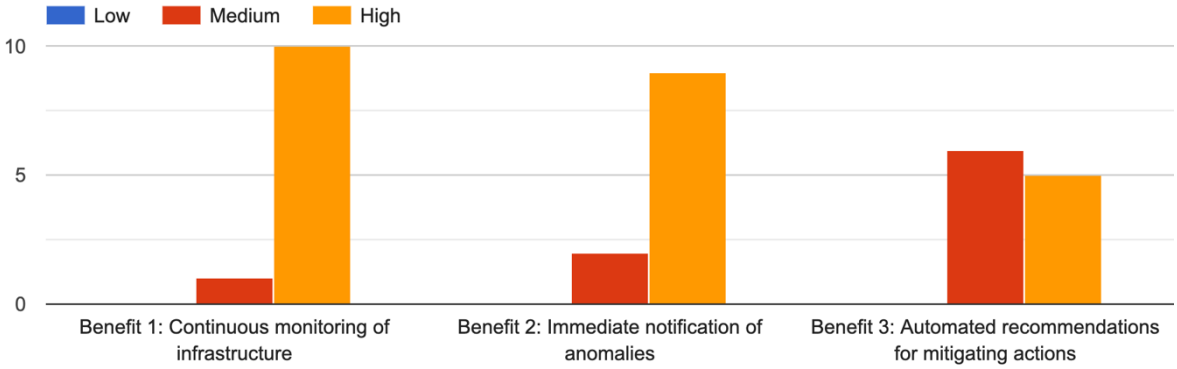
What do you value in a cybersecurity platform protecting your supply chain?



4.3.2.2 KER 2: TIM

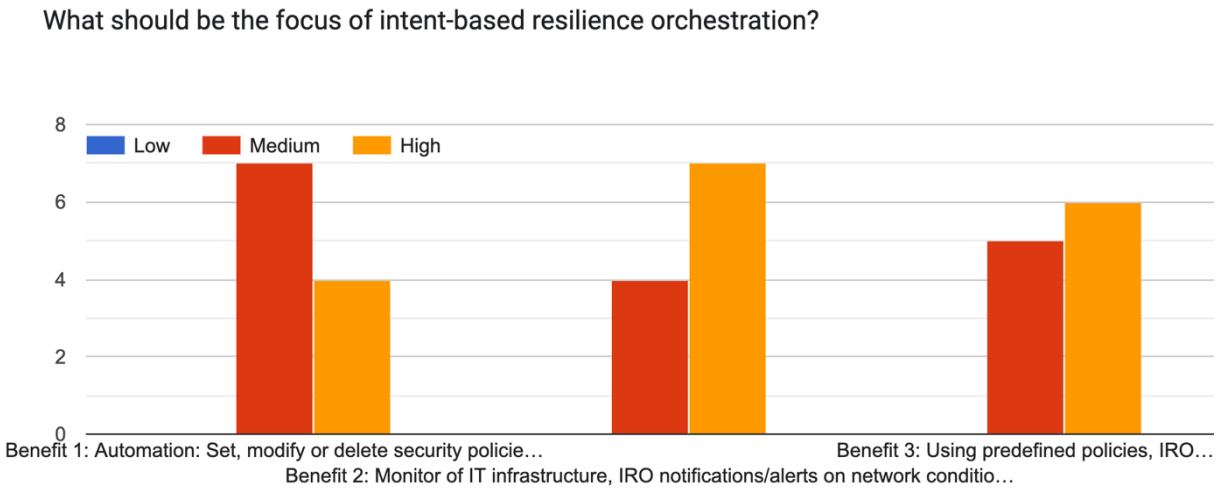
Given the nature of this KER and the current need of better cybersecurity technology, it is predictable that continuous infrastructure monitoring and immediate anomaly notification is well appreciated by potential technology adopters. The automation of mitigation actions through recommendation is also very relevant and will be a point of discussion in pitch activities.

What is more important for you in vulnerability assessment and incident management?



4.3.2.3 KER 3: IRO

In the case of this KER where functionality is more internal to FISHY, the monitoring, notification, recommendation and reaction show to be the most relevant point but might need more detail in the pitch activities. Also much attractive are the use of predefined security policies and the automation.

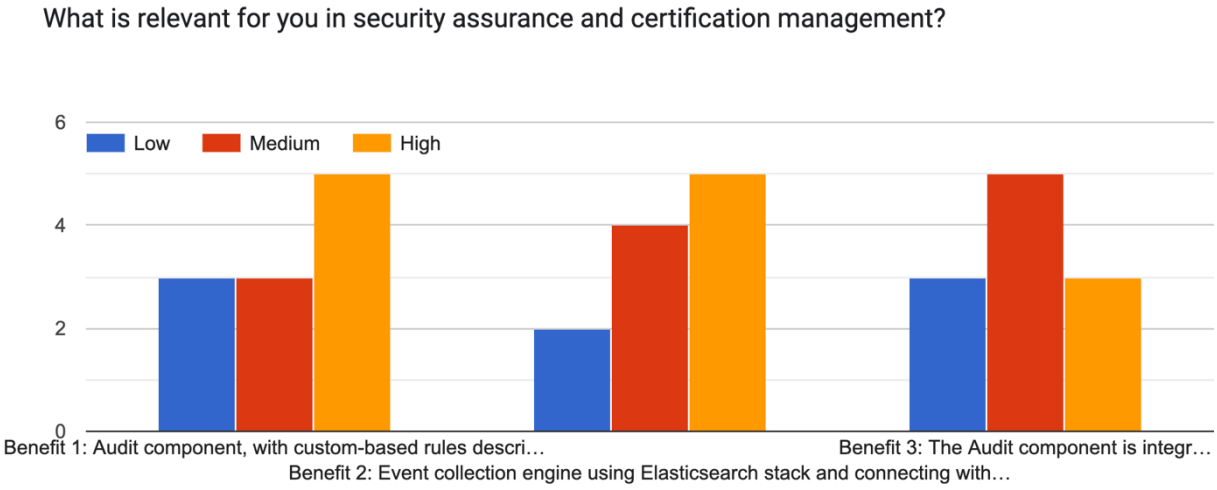


The choice options (benefits of KER 3) are as follows:

- Benefit 1: Automation - Set, modify or delete security policies at scale using high level intent language.
- Benefit 2: Monitor of IT infrastructure, IRO notifications/alerts on network condition, recommended actions, and react based on the situation.
- Benefit 3: Using predefined policies, IRO can react to detected threats automatically or after confirmation from the user, and enforce security rules.

4.3.2.4 KER 4: SACM

This KER gathers less consensus in its selected highlights, although the main point of relevance being the audit component with custom-based rules, followed by the event collection and the use of the Drools rules management system. The discourse when presenting the KER to potential customers needs to be less technical (e.g., explaining the functionality of the Drools system instead of mentioning it, or elaborating on the powerful properties of Elasticsearch that enrich the audit component).

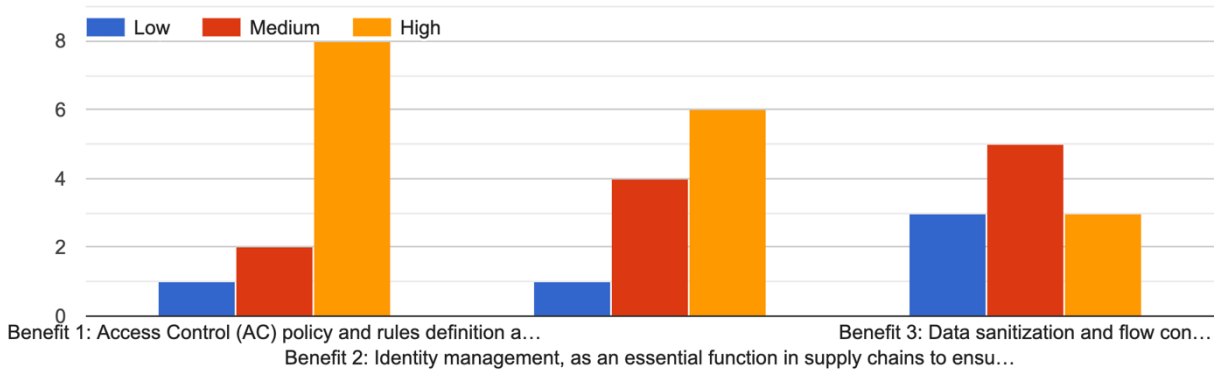


The choice options (benefits of KER 4) are as follows:

- Benefit 1: Audit component, with custom-based rules described using a high level language named Event Calculus logic.
- Benefit 2: Event collection engine using Elasticsearch stack and connecting with other (external) data pools using AMQP technologies (message brokers).
- Benefit 3: The Audit component is integrated in Drools rules management system.

4.3.2.5 KER 5: SPI

In this KER the main focus of interest by potential adopters is the access control of policies and rules, closely followed by the identity management allowing for different access profiles. On the other hand, data sanitization and flow control are perceived with lower interest, and will eventually need more clarification during pitch activities.

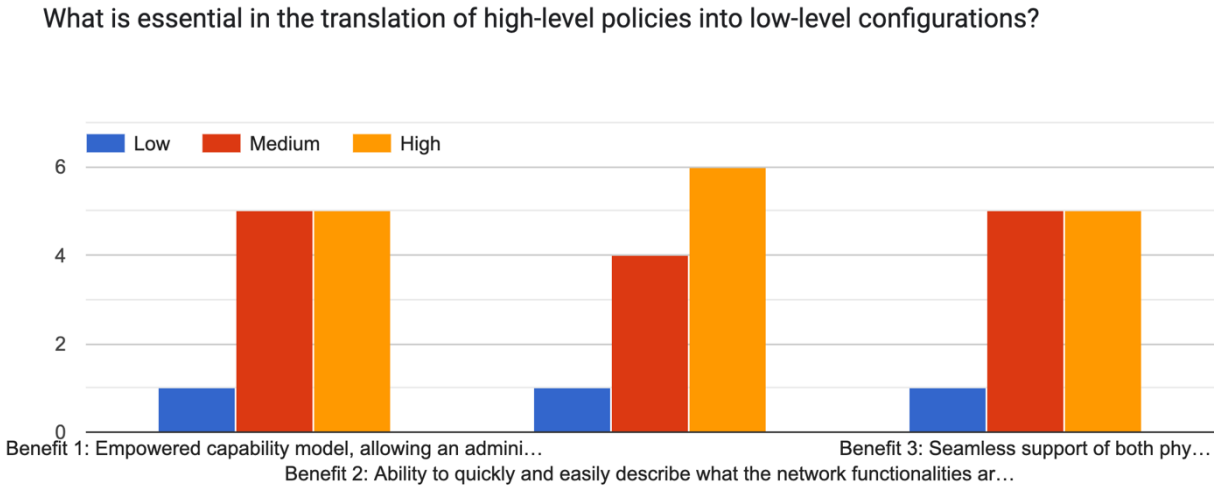


The choice options (benefits of KER 5) are as follows:

- Benefit 1: Access Control (AC) policy and rules definition and enforcement technology.
- Benefit 2: Identity management, as an essential function in supply chains to ensure the coexistence of different access profiles.
- Benefit 3: Data sanitization and flow control from low-level on-premise components, according to previously defined security and privacy rules.

4.3.2.6 KER 6: EDC

In the case of this KER, all of the selected benefits are seen as highly relevant, led by the seamless support of both physical and virtualized security controls, and the ability to quickly and easily describe usage in network functionalities. Also, the ability to add support for new types of security controls is a perceived value that must be taken into account in pitch activities.



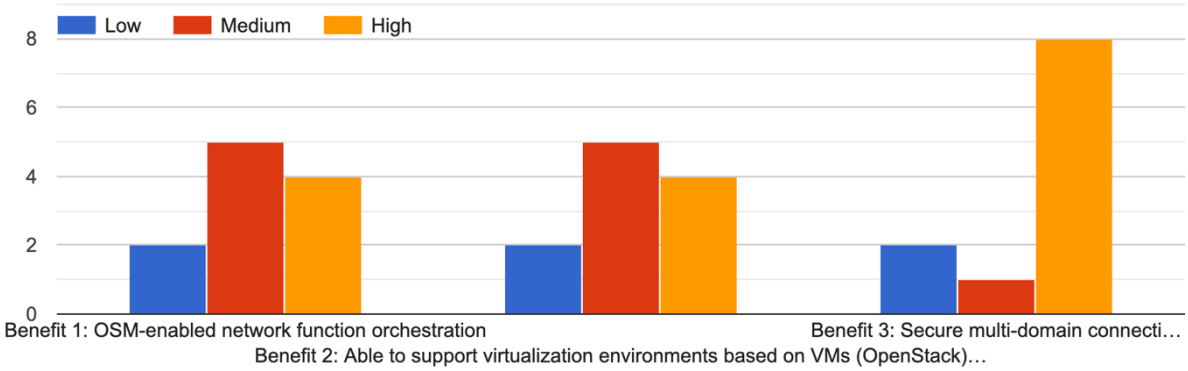
The choice options (benefits of KER 6) are as follows:

- Benefit 1: Empowered capability model, allowing an administrator to add support for new types of security controls with ease.
- Benefit 2: Ability to quickly and easily describe what the network functionalities are using close to human language, independent of implementation.
- Benefit 3: Seamless support of both physical and virtualized security controls, allowing the administrators to configure mixed networks containing both types of devices.

4.3.2.7 KER 7: SIA

Finally, in the case of this KER the benefit perceived as the most valuable is the secure multi-domain connectivity. The OSM enablement and support to virtualisation environments will need to be further elaborated in the context of pitch activities, particularly because they are addressing network functions that might need to be better understood by potential adopters in the context of supply-chain security.

How would you qualify the impact of the potential benefits of being able to apply cross-infrastructure mitigation actions?

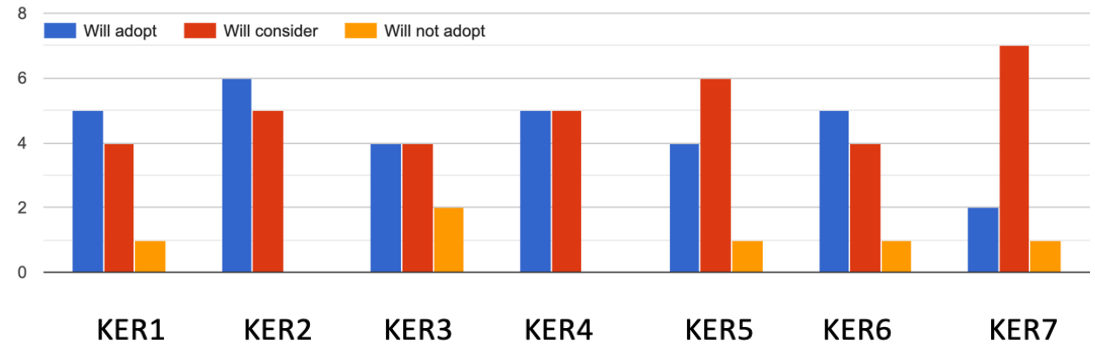


The choice options (benefits of KER 7) are as follows:

- Benefit 1: OSM-enabled network function orchestration.
- Benefit 2: Able to support virtualization environments based on VMs (OpenStack) and containers (Kubernetes).
- Benefit 3: Secure multi-domain connectivity relying on IPsec.

To close this survey analysis, we asked the inquired about the usefulness of the seven innovative outcomes of FISHY in regards to three objective levels of interest: (1) will adopt; (2) will consider; (3) will not adopt. The KERs 2 (TIM) and 4 (SACM) are those that gather more consensus in their adoption, closely followed by KER 1 (the end-to-end solution), 5 (SPI) and 6 (EDC). Risk of either lack of information provided or weakly convincing benefits are shown for the KERs 3 (IRO) and 7 (SIA) that being the core technology of FISHY and essentially a product of research, might have a bigger academic value as well as value in the context of the FISHY Platform itself. The value proposition canvas of the latter has been reworked with the KER leaders (see section 4.3.1) to improve their potential impact.

What is the Value of the Outcomes of FISHY?



4.3.3 KER Exposure & Pitch Materials

Joining efforts with the exploitation task T7.1, we have used the value message of each of the FISHY KERs to further develop the project's marketing materials. In this final reporting period we intensified our activities aiming for the marketing of the FISHY research output, despite the difficulties caused by the COVID-19 restrictions and cancelled events early in the project's lifetime. We put our effort on digital-based marketing materials that can be shared online, and the coordination of the appropriate exposure in digital events where the direct communication with leads can be done before, during or after the event. This was then reused in the major events we were present in as a project. In the following we present the pitch materials prepared to enhance opportunities, and the pitch activities to leverage those in the context of the exploitation of the project's exploitable results. The latter are based on an exploitation perspective and their description will complement but not overlap the discussions in section 4 on the project's exploitation activities.

4.3.3.1 KER-based pitch materials and pitch deck(s)

Following the guiding of the Horizon Results Booster, we have prepared a series of KER-based materials (available directly at the project's website download section at fishy-project.eu/key-exploitable-results) that highlight the benefits and value of functionalities of the full-stack FISHY solution but also to each of the seven KERs..

Building on the available pitch deck used to present the highlights of the project, and on the knowledge acquired with the Horizon Results Booster initiative, we have prepared a pitch deck on the full-stack solution, and seven pitch decks on each of the FISHY KERs that determine its innovation in the main R&D focus (available at the FISHY website here: https://fishy-project.eu/project/promotional_material). The structure of the pitch decks available is as follows:

1. Cover: clear identification of the KER, the project, the consortium and the EC identification, highlighting the unique value proposition is exposed as the vision of the KER we are pitching
2. Benefits: from the 1-pagers we highlight three of the main benefits of the KER in analysis.
3. Problem-Solution-Value: the definition of the addressed problem, the solution that we use to address it and the generated value that serve us as a differentiator on the FISHY solution, highlighting the innovation at each KER.
4. Early adopter/Success stories: the reference statements of each of the use cases and how they benefit from FISHY, allowing for other leads to identify with their objectives and their stories.
5. Team/Contacts: the main contacts

These materials are also available to the consortium in an editable version to allow for the adaptation of their communication potential to the target audience. The content to the presentation of each of the KERs, later used in the presentation of KERs, was made available and is also presented in the annex, based on a modification of the pitch canvas [37].

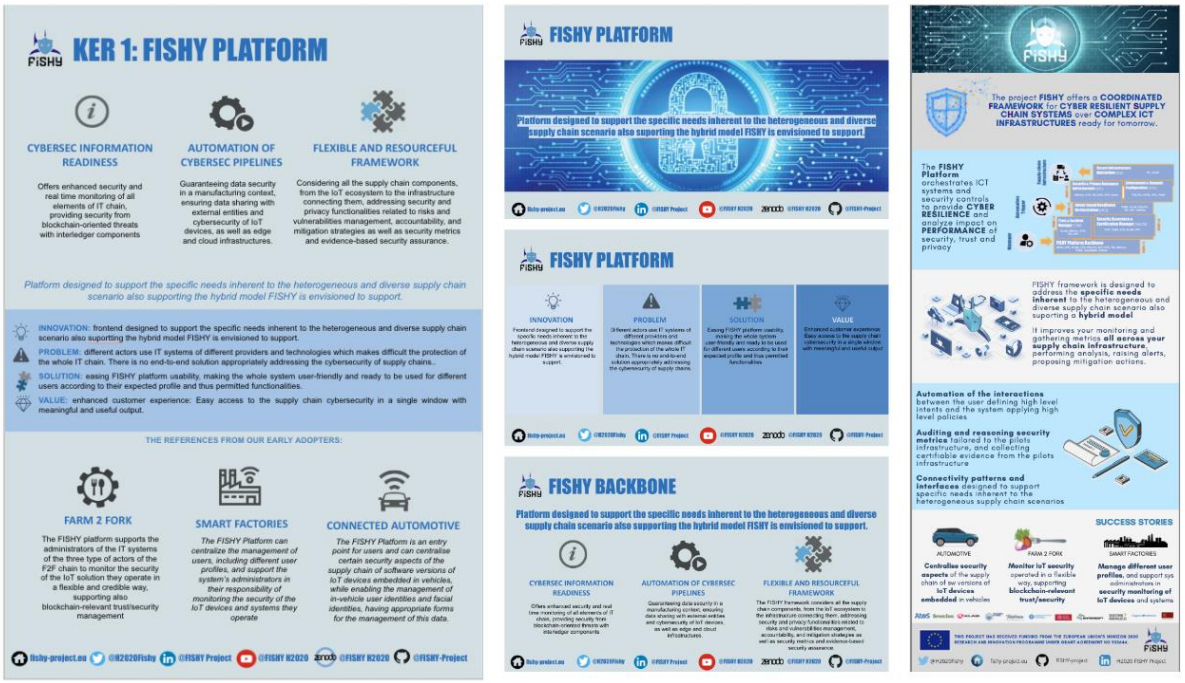


Figure 10 - FISHY's pitch materials focusing each of the KERs

Taking into consideration the changes in the organisation of innovations across KERs, and feeding from the pitch canvas and the latest R&D achievements, we have written seven 1-pager documents that serve as executive summary to present each of the KERs to a decision-maker (see Figure 10).

4.3.3.2 Infographics and Project Roll-up

To follow a common guideline in the communication of the value message of FISHY, they have a simple structure where an initial slogan/vision statement is followed by the benefits of the KER and the problem-solution-value, to close with the reference statements of the use case partners used as success stories highlighting FISHY's innovation.

These documents can be adjusted to better fit the interests of the receiver and thus better capture their interest in the FISHY solution through a better understanding of its generated value. They served the FISHY team having been used by KER leaders, and shared with stakeholders and EAB members.

Moreover, the new FISHY poster wraps-up this business focused communication strategy to better express in a limited timeline the main achievements of the project and their transition to the available exploitable results, also fed by the KER-based communication built as described above. This final project poster was used in the cohesion of the exploitation-focused communication described above, exposed in the landing page which is the KER page of FISHY. See this discussion in more detail in section 2.5.7.

4.3.3.3 KER page

To optimize the exposure of the FISHY offer based on the defined KERs, the consortium prepared business-focused pages as a section on the website that becomes the landing page to optimize their exposure (see https://fishy-project.eu/key-exploitable-results). The landing pages reorder the information modules, and in the same cases restructure those for a better communication over the website. The modules are as follows:

- Expressive title of the KER
- Unique value proposition

- KER video
- Definition of problem, solution and value
- Context in the full-stack
- Top benefits
- Technical schema of the KER
- Main innovations
- Follow-up digital booth

The visitor that is further interested in the technology can then navigate through the available deliverables, research papers, white papers and marketing materials available in the "Downloads" section of the website.

Moreover, to leverage the valuable business information from the FISHY pilots that are the early adopters of the technology, and the rich complexity of their configuration choices according to their priorities, we have published the three success stories in the same KER subpage of the FISHY website based on the exploitation aspects of each of them. These will help us attract potential users that identify with those configuration choices and can better grasp the value of FISHY technology.

4.3.3.4 Final Press Release and White Paper

To wrap-up the highlights of the FISHY's exploitable results in a frame that can be edited and republished in external venues (including the consortium partners' external and internal channels, but also the domain-specific online media as, e.g., cybersecuritynews.com), we have prepared a communication toolkit that elaborates on the available 1-pagers to expose the KERs as innovation-based news for those other venues.

Following the first press release and other promotional materials, and taking a business offer-guided perspective, we describe the highlights of the FISHY research output based on the seven KERs and the innovation assets that they are based on.

To further clarify the overall communication of the value message of FISHY, we prepared the second and final whitepaper providing the KER angle to the FISHY solution presentation, aligned with the new exploitation-focused communication described in the paragraphs above. We have also included the user roles and stories from our use cases, as well as their perspective business case repositioning based on the FISHY advantage. This white paper served us to communicate FISHY to the leads generated at the follow-up conversations, consolidating the effort to expose the benefits of the FISHY technology adoption.

4.4 Business Development

In this final reporting period we have consolidated the business development of FISHY, also elaborating on the KER-specific business plans, that greatly contribute to the overall understanding of the FISHY exploitation strategy. To build over the extensive work done since the early stage of the project's exploitation, taking into consideration the insight from the FISHY Radar (developed in Task 2.1) on the market assessment and on the legal and regulatory landscape, we have advanced to a final business model, synchronised with the IPR management of the project's results. To have a deeper analysis of the progress of the exploitation activities of the project, we present the result of iterations with the complementary self-assessment of the MTRL and BOSAT. Finally, we will further discuss the customer profiling building on the initial work published in D2.1 and D2.3, describing the customer journey reflecting the success cases and exploitation opportunities within the project use cases and how FISHY can be an advantage to their business scenarios.

4.4.1 IPR Analysis and Protection

In this section, we will elaborate on the achievements in regards to the registration, analysis and protection of the IP results, wrapping-up the IPR management activities, following the preceding work published in the deliverables D7.3 (public) and D7.6 (confidential). Following the substantial progress on the research and development of the project during this final reporting period, the IPR management concluded activities to let the exploitation effort define the KERs over the IPR achievements as a strong basis to the FISHY platform. The full log of IP results is available in the Annex 7.3 of this document.

According to our analysis, 25 IP results are released open source, most of which with an Apache 2.0 licence, with the exception of the Framework for InfSec evaluation within IoT holding a GPLv2 licence, and the Wazuh extensions as well as the detection and protection components (due to the Wazuh, Cowrie - copyright with permission to redistribute and modify, and Suricata holding that same licence, more restrictive than Apache 2.0). Their coverage is essentially homogeneous throughout the FISHY KERs.

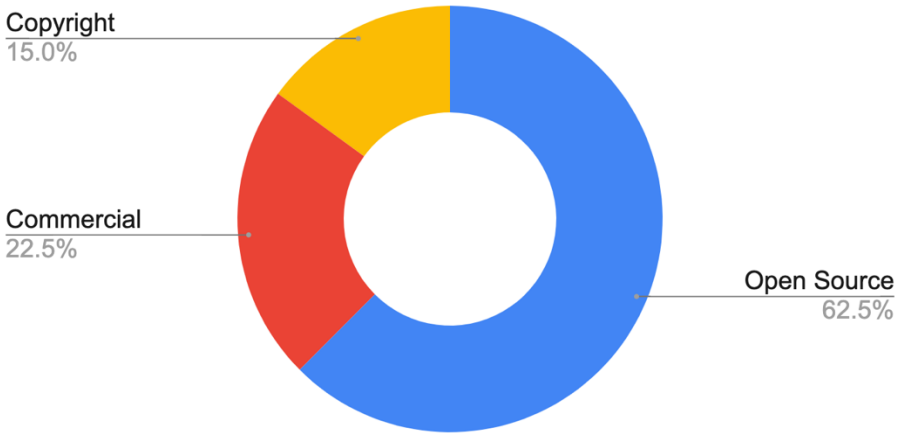


Figure 11 - IP results distribution across license types

We have used this analysis to enable the description of the capabilities and functionalities of Open FISHY, as well as of the potential paid features of FISHY, synchronised with the open source and commercial IP generated and logged (see Figure 11).

Moreover, we have analysed in collaboration with WP2 a selection of innovations from the whitespace perspective to identify potential risks and obstacles to the freedom to operate within FISHY. This study is published and detailed in the deliverable D2.4, and built on the preliminary Cooperative Patent Classification (CPC) analysis, expanding from the FISHY key innovations registered through their IP results.

The importance of the IPR management in FISHY is transversal across the project, serving as a basis to the definition of the exploitable results that, together with the research and development team, build the open source products and potential services that are outcomes of this project. This also reflects the R&D in the lifetime of the project and the opportunity, in particular for the SMEs in the consortium, that see their technology fed with new features based on industry requirements and promoting the success stories of the project's use cases.

This analysis fed the last update to the KER documentation to submit the seven FISHY KERs to the Horizon Result Portal. Moreover, the IPR manager has been responsible for the supervision of the content released in the communication activities, including blog posts and marketing campaigns, to avoid breeches.

4.4.2 Open FISHY

The consolidated business plans presented in this section builds from the discussions above, the knowledge gained with the Horizon Results Booster (particularly in the *Go-to-Market* coaching session) and what regards the individual and joint exploitation plans. It also takes into close consideration the exploitation of FISHY innovation assets by the early adopters in a lean perspective [38] and allows to comply with the requirements for Investors Corner of the Horizon Results Platform (the section 5 of the Horizon Results Platform profile) submission of the FISHY KERs, in line with the KER-focused lean business canvas prepared in the section 4.3.1. The following (see Figure 12) thus summarize the functionality provided through openFISHY complemented by the premium features available.

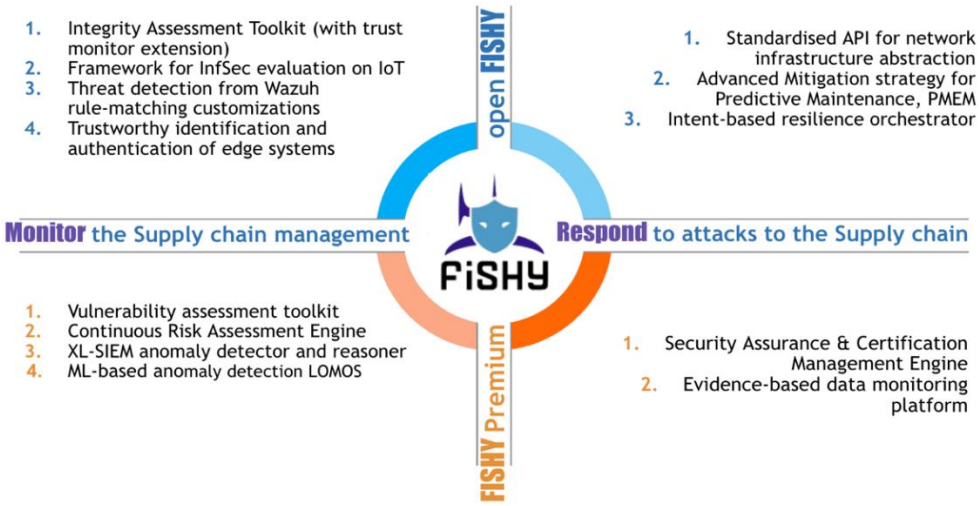


Figure 12 - OpenFISHY as complemented by the paid premium features

To sync our work with the IP available open source and the commercial IP in the project (see section 7.2.3 for the IP references) and guarantee basic functionality existing in an open source version, we prepared the OpenFISHY. This is a fully open source version of the end-to-end technology, available at the project's repository (as discussed in section 3.5). The functionality might be limited in some of the cases (e.g., the vulnerability assessment tool is available open source in a limited version based on the Wazuh extensions, but fully operational including the AI-based anomaly detection LOMOS through its commercial license) but allows us to consider the approach where premium paid features can be made available. Details per KER are confidential and were published in the confidential counterpart of this document, the deliverable D7.7.

Project results have been contributed to different standardization efforts to maximize their industrial impact, and more specifically their application to the scenarios identified in the use cases. Standards activities of all nature (SDOs, industry associations, open-source communities) have been tracked, analysing the most relevant opportunities, and bringing not only results as direct contributions to existing activities, but also supporting the emergence of new activities based on relevant FISHY outcomes. The project team has sought the collaboration with other related research projects.

4.4.2.1 KER1: FISHY Platform

OSS Functionality:

End-to-end (light) functionality prototype of FISHY platform ready with validation in a real context. The OSS repository locations are as follows:

- FISHY GUI: https://github.com/H2020-FISHY/Fishy-Dashboard
- FISHY-Sandbox-development https://github.com/H2020-FISHY/FISHY-Sandbox-development

Current stage:

There were 2 versions in IT-1, one in UPC (with F2F and WBP use cases integrated) and one in CAPGEMINI premises with SADE use case. There has never been a version in SYN. This was for IT-2. Then for IT-2 these 2 versions have been migrated to the FISHY Reference Framework. In the FRF again we have two versions, one for F2F and WBP, and another one a little tuned (with extra menus) for SADE use case.

Licensing: Apache 2.0

4.4.2.2 KER2: **FISHY Trust & Incident Manager**

OSS Functionality:

(i) Detection and protection components to verify the application of a predefined path in a given network, supporting routing verification and topology attestation AI-based anomaly detection; (ii) Integrity Assessment Toolkit (Trust Monitor) relying on a physical root-of-trust (the TPM chip) and creating problems in virtualized environments or devices with limited capabilities that lack this chip; (iii) Advanced Mitigation strategy (PMEM) AI-assisted tool that suggests maintenance actions to mitigate potential attacks effects based on data analytics and predictive models.

The OSS repository locations are as follows:

- **TIM-Deployment** https://github.com/H2020-FISHY/TIM-Deployment-Appliance-Agent-Deployment
- **Trust monitor**: https://github.com/H2020-FISHY/trust-monitor
- **Central Repository** https://github.com/H2020-FISHY/TIM/tree/master/tar
- **Appliance-Agent-Deployment** https://github.com/H2020-FISHY/Appliance-Agent-Deployment
- **Advanced Mitigation strategy - PMEM:** https://github.com/H2020-FISHY/pmem

Current stage:

The TIM components are in the finishing stages of deployment and validation with the use case partners. Concretely, VAT and WAZUH were already deployed and validated. XL-SIEM, RAE, PMEM and LOMOS deployment is almost done and then these components only need to be validated. The Central Repository has also already been successfully deployed and validated. Business Model Scalability: The technology is scalable by design, based on well-established technology.

Licensing: Apache 2.0

4.4.2.3 KER3 FISHY Intent-based Resilience Orchestration

OSS Functionality:

AI/ML-based intent-based resilience orchestrator IRO responsible for mapping high-level intents given by a user into configured policies that can run by a lower-level system controller. In FISHY, IRO will receive intents from users as plain text and uses ML techniques to translate user requirements into

structured policies compatible with the FISHY enforcer component. The OSS repository locations are as follows:

- IRO: https://github.com/H2020-FISHY/IRO

Current stage:

The IRO is currently containerized and deployed in UPC premises as well as in the FRF, including multi-tenancy and Keyclock authentication. An IRO Dashboard is developed and integrated with the FISHY Dashboard in the FRF. IRO is integrated with the Central Repository in order to get information about alerts through the API and through RabbitMQ for event based messaging enabling user notification. IRO is also integrated with EDC through the Central Repository to enforce policies. Moreover, IRO has integrated the EDC graphical interface to easily receive recommendations from EDC allowing the user to select best remediation decision. IRO integrated Smart Contracts verification to trustworthiness of the received events. Smart Contracts events are received using RabbitMQ consumers subscribed to the Central Repository.

Licensing: Apache 2.0

4.4.2.4 KER4 FISHY Security Assurance & Certification Manager

OSS Functionality:

Blockchain-based trustworthy identification and authentication of edge solution aimed at enabling a proper authentication of edge devices specifically designed for mobile scenarios and highly constrained devices. The OSS repository locations are as follows:

- Trustworthy identification and authentication of edge systems: https://github.com/H2020-FISHY/SEN

Current stage:

For the current state : SACM tool if fully deployed in the FRF (Kubernetes environment). Evidence Collection Engine (as part of the SACM tool) is communicating/collecting data from the pilots (use cases) directly in the FRF environment or via the Fishy Appliance (FA) framework.

Licensing: Apache 2.0

4.4.2.5 KER5: FISHY Security & Privacy Dataspace Infrastructure

OSS Functionality:

Framework for InfSec evaluation with a focus on IoT, including a metrics taxonomy addressing all types of information (security, performance, environmental, and operational) and a model for establishing relation with attacks, aiming at providing automatic (as best as possible) security assessment. The OSS repository locations are as follows:

- SPI implementation including Data Management module to provide format conversion (to CEF format) and privacy protection function: https://github.com/H2020-FISHY/SPI
- Zeek Log collection, which adapts Zeek architecture to the requirements of the FISHY project. The work includes Zeek scripts to accommodate external interface for log storage: https://github.com/H2020-FISHY/zeek-deployment
- Zeek Log analysis, a set of Python functions to facilitate the exploration of network metrics and design of Zeeq scripts according to metrics definitions: https://github.com/nonvegan/FISHY-NetAnalysis

Current stage:

Keycloak was implemented in a Docker-based architecture, and it was already used for user authentication for most FISHY components. Moreover, it was used for application authentication, too, for the components in the SPI itself and other web services-like FISHY modules. The metrics taxonomy and security event format are in a first-draft version. The correspondent software module to implement the data organisation are fully operational. A RabbitMQ data handler, implemented in a Docker-based architecture too, was also deployed and it is ready to use. SPI also implements privacy enforcing techniques - so far, cryptographic and anonymity techniques were already tested.

Licensing: Apache 2.0

4.4.2.6 FISHY: KER6 Enforcement & Dynamic Configuration (EDC)

OSS Functionality:

Enforcement & Dynamic Configuration (EDC) to refine high-level policies into low-level configurations. It leverages a modular security capability model to describe the available security controls and an inferential engine to perform a smart and adaptive generation of the controls' configurations. In addition, the EDC allows a timely reaction to a variety of threats by proposing how to reconfigure the security controls for mitigating the attack. The OSS repository locations are as follows:

- EDC (Enforcement & Dynamic Configuration): The EDC has four components:
  - Controller: https://github.com/H2020-FISHY/edc-controller
  - Register & Planner: https://github.com/H2020-FISHY/edc-register
  - Enforcer: https://github.com/H2020-FISHY/edc-enforcer
  - Remediation Module: https://github.com/H2020-FISHY/edc-rem

Current stage:

EDC initial PoC released, EDC based on 4 web services, each one exposing an API that allow the management of its features and workflow through a dashboard (web-based GUI accessible via browser). The EDC is currently a Docker container and leverages Python and Java to perform the policy refinement. It is currently deployed in the F2F and WBC where it automatically generates stateful firewall configuration for banning users and devices. Moreover, it is able to generate configuration rules for the proprietary security controls used in the pilots (e.g., to enforce Ethereum policies). The EDC components can be managed independently with their EDC-specific GUIs. Furthermore, the functionalities that are needed to implement the sophisticated FISHY workflows have been offloaded to the IRO and are hence available in the FISHY dashboard.

Licensing: GPL v.2 and Apache 2.0

4.4.2.7 KER7: FISHY Secure Infrastructure Abstraction

OSS Functionality:

Standardised API for network infrastructure abstraction supporting a consistent connectivity framework, based on a virtual distributed switch. The OSS repository locations are as follows:

- CCIPS: https://github.com/Telefonica/cne-cfgipsec2/tree/vRFC9061/src
- OSM NBI: The original version https://github.com/Networks-it-uc3m/Software-driven-Connectivity-Orchestrator, evolving towards being integrated as an OSM feature, here: https://osm.etsi.org/pad/p/feature10921
- L2S-M: https://github.com/Networks-it-uc3m/L2S-M or http://l2sm.io/

Current stage:

The SIA components (NED, Monitoring and orchestration elements) have been developed, integrated and validated in the project use cases. The current version is based on Kubernetes and Open Source MANO (OSM), and available within FISHY IT-2, constituting the core of the FISHY Reference Framework (FRF).

Licensing: Apache 2.0

4.4.3 Sustainability Strategy

In line with the contribution to the OSS Community discussed in section 3, the distribution of IP results presented in section 4.4.1 and the business model discussed in the previous section, the strategy for the sustainability of FISHY is based on the individual/joint exploitation plans of partners and guided by the seven KERs defined in this project. Particularly, discussions lead to a use model that fits well with the nature of each KER, mostly revealing the intention to mature the technology and rise the TRL through a new funding round (as, e.g., an Innovation Action) building on the achievements in the lifetime of the project.

To better understand the sustainability of our approach we have analysed, per KER, the interest, role and contribution of each consortium partner. This work extended what was discussed in the first Horizon Results Booster coaching session, *Portfolio of Dissemination and Exploitation - Module C.* In the following paragraphs we present the costs related to each KER, both on technology and staff, but also the user tasks and the optimisation of time and budget related to the improvement brought by each KER.

This information reveals a great advantage to European SMEs that require a flexible solution fit to their needs, but also to their often limited budget, promoting a more appropriate adoption of cybersecurity methodologies and tools based on state-of-the-art technologies and research results achieved in the project's lifetime.

In the confidential version of this report, the deliverable D7.7, we also present the responsibilities of each partner that is IP owner, and their engagement, plans and foreseen opportunities in the code that is vital to the sustainability of each KER.

Moreover, we have also discussed with the Horizon Results Booster the 4Ps model that can complement the business models published in the preceding deliverable D7.6. It shows in a clear fashion the relevant characteristics of the FISHY solution in parallel to pricing categories, and in relation to the geography of initial business opportunities, and the characteristics of the related campaign, following the OpenFISHY release campaign discussed in section 2.5.3.

4.4.4 MTRL & BOSAT Assessments

In the following paragraphs we will describe the innovation analysis of the outcome of the project from two different but complementary perspectives. These provide us with a guided analysis on the relation between the technical and exploitation progress (MTRL), but also measures the progress over six quadrants that are meaningful to appropriately address further investment and business opportunities.

MTRL Assessment

The results of the MTRL analysis previously guided by the University of Oxford and member of the Oxford e-Research Centre [39], were followed in the context of the SWForum.eu initiative in direct communication in May 17, 2023. The full self-assessment can be seen in the Annex 7.6 of this document. We recall that the MTRL approach aims for the enablement of innovation, helping to improve the exploitable results as outcomes of the project, and that the final results of the overall

evaluation are on an XY positioning crossing aspects relating to the TRL and others to the MRL of the project's exploitable results (see Figure 13 below**¡Error! No se encuentra el origen de la referencia.**). A second evaluation was done in Q3 of 2022 and a final one towards the end of the project at Q2 of 2023, showing a significant evolution taking into consideration the other two evaluations, and the questions and answers.

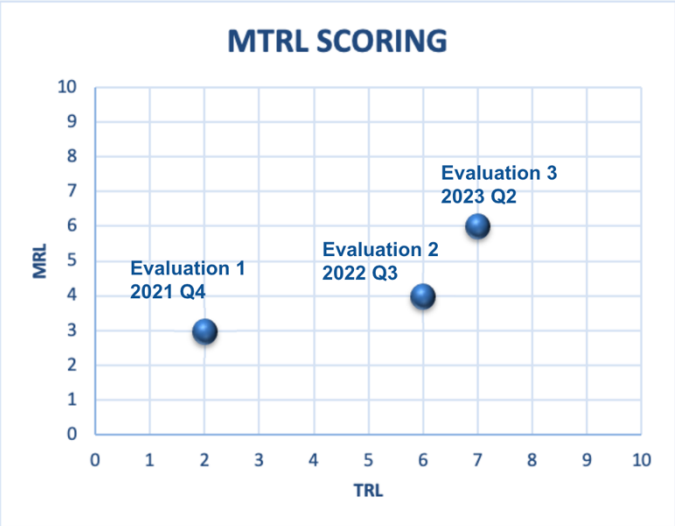


Figure 13 - MTRL positioning for the research and innovation at FISHY

BOSAT Assessment

During the HRB coaching programme for the Business Plan Development, we were requested to provide the BOSAT self-assessment. This tool is based on the business opportunity self-assessment, developed within BOSS and co-funded by the Erasmus+ Programme of the European Union (available at https://bossplatform.rect.bg.ac.rs). The full self-assessment can also be seen in the Annex 7.6 of this document.

The analysis of the two interactions, done at the timing of the two last coaching sessions with the Horizon Results Booster programs for *Business Plan Development* and *Go-to-Market*, in November 2021 and March 2023, respectively. The generated chart in the Figure 14 below shows that the stronger pillars of this project through the BOSAT perspective are "Market", "Team", "IP" and "Technology". There are again limitations due to the general purpose of this assessment where the maximum levels in the "IP" category consider patenting, what is not considered in this project neither is it identified as an exploitation opportunity. These limitations are also visible in the "Financials" category.

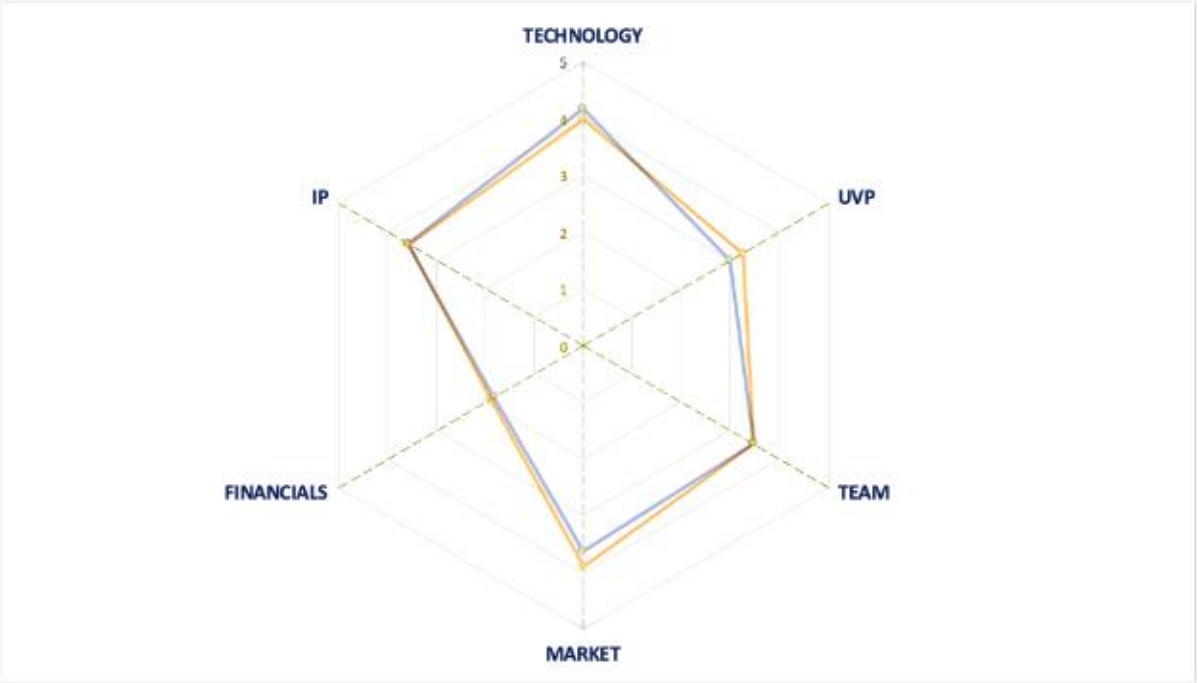


Figure 14 - Multidimensional BOSAT assessment output at FISHY

4.4.5 Exploitation of Use Cases

In this final phase of the FISHY project we have intensified the business development work in the light of the newly defined Open FISHY offer and the premium features that can be offered based on the commercial IP in the project. To that aim we have analysed the stakeholders in FISHY and how they help us shape the customer profiling within B2B business relationships.

To understand in better detail the diversity of potential customers and users of the FISHY solution, we have discussed with the use case owners in the consortium, representing the early adopters, the fundamental aspects of their business case and how FISHY can be beneficial to its empowerment.

In what regards the user profiles, and as earlier presented in the discussion of the FISHY Value Survey in section 4.3.2, we wrap-up this analysis with the Table 9 summarising the user profiles interacting with the FISHY Platform, their level of access, and the use cases that include these profiles.

Table 9 - FISHY User Profiles (UP)

ID	Name	Use Cases	Access
UP-1	Owner (of the complete supply-chain)	/	Chain
UP-2	Manager (root node of the supply chain)	UC3	Chain
UP-3	Participant (as part of the supply chain)	/	Node
UP-4	Technology integrator	UC1	Node
UP-5	Administrator of the IT platform integrating all supply chain island	UC2	Chain
UP-6	IT Cybersecurity leader	UC3	Node

In the following, we detail the exploitation content based on the exploitation of the use case scenarios (including expectations and plans, or user roles and stories).

4.4.5.1 UC1: Farm-to-fork (F2F)

Achievements:

In the F2F use case, the FISHY platform needs to support the administrators of the IT systems of the three types of actors of the F2F chain to monitor the security of the IoT solution they operate in a flexible and credible way, supporting also blockchain-relevant trust/security management.

This use case achieves the reduction in downtime (this cannot be calculated but given that 62% of supply chain attacks exploit the trust of client to their supplier and that 58% of attacks aim at accessing data, it is obvious that as FISHY protects against these two categories of attacks significantly reduces the downtime).

With FISHY, F2F can mitigate 5 different attacks of different types: brute force attack, network analysis attack, compromised device (wallet ID level and DID level), blockchain node attack, machine-learning based attack detection at endpoint.

User Roles:

- UC1-P1. Farmer node.
- UC1-P2. Logistics node.
- UC1-P3. Supermarket node.
- UC1-P4. Supply-chain manager.

Benefits

- Protect against multiple types of attacks and minimize down-time.
- Be able to confirm/certify the absence of attacks or the types of attacks that occurred (e.g. through blockchain based evidence).
- The flexibility of deployment and the flexibility in the way attacks are detected based on logs or traffic analysis or embracing machine learning techniques is very important to ensure the continuous update of the attacks that can be detected and mitigated.

Limitations

- The current version of the FISHY platform does not offer an intuitive interface for managing the reconfiguration of the IT systems (e.g. introduction of new devices).

Useful Innovation:

- Protect against multiple types of attacks and minimize down-time.
- Be able to confirm/certify the absence of attacks or the types of attacks that occurred (e.g. through blockchain based evidence).

4.4.5.2 UC2: Smart manufacturing (WBP)

Achievements:

The FISHY Platform supports system's administrators in their responsibility of monitoring the security of the IoT devices and systems they operate. The main achievements of this use case were the following:

- Automated identification of rogue IoT devices reducing cybersecurity effort by detecting unauthorized and potentially malicious devices within the network.

- IoT network traffic monitoring improves the threat identification.
- Recommendations for action in EDI communication attacks reduce impact.

User Roles:

- UC2-P0. Individual Node Monitoring.
- UC2-P1. SAP Applicational Administrator.
- UC2-P1b. Supply Chain Sec Expert.
- UC2-P2. FISHY IT administrator.

Benefits:

- Automated identification of rogue IoTs reducing cybersecurity effort by detecting unauthorized and potentially malicious devices within the network.
- IoT network traffic monitoring improves the threat identification.
- Recommendations for action in electronic data interchange communication attacks reduces impact potential.

Limitations:

- The addition and configuration of new devices to the current version of the FISHY platform is not centralized in the dashboard.

Useful Innovation:

- Automated identification of rogue IoTs reducing cybersecurity effort by detecting unauthorized and potentially malicious devices within the network.
- IoT network traffic monitoring improves the threat identification.
- Recommendations for action in electronic data interchange communication attacks reduces impact potential.

4.4.5.3 UC3: Connected cars (SADE)

Achievements:

The connected cars use case SADE was able to leverage FISHY innovation to ensure the identification of SW Certifications of Components Vehicle. This allowed getting a connection model between manufacturers and vehicles connected, while getting integration with XL-SIEM, a FISHY tool for live monitoring of service' logs. This tool allowed also to prevent security issues related with car access and traffic tampering attacks.

- Significant improvement concerning the security of the car thanks to logs and certifications monitoring (however, it is difficult to estimate the % of improvement with respect to the current status);
- 100% improvement given the possibility to know the SW version installed in the car and compare it to versions that are certified by manufacturers;
- Significant reduction of the risk for a car to be attacked due to non-validated running software or unknown errors.

User Roles:

- UC3-P0. Manufacturer.
- UC3-P1. Dealer.
- UC3-P2. Local operator.

- UC3-P3. Owner.

Benefits:

- Automatic generation of events and alarms by reading logs that improve the knowledge of the different actors in the supply chain in case of issue/attack. With this information they will be able to apply mitigation measures (software updates, car deactivation, car blocked).
- On-live add/revoke software certificates by manufacturers.
- Continuous monitoring of the software certificates deployed in each vehicle, allowing rapid detection of vehicles with revoked certificates and/or camouflaged malware.
- Role-based access control using centralized FISHY dashboard and the SPI for all the suppliers (multi-user for one on-premise cloud, not multi-tenancy for multiple clouds).

Limitations:

- The integration of on-premise environment requires some adaptions that requires high effort;
- The automatic reaction to alarms for SADE requires a customized interaction with the central repository;
- Multi-owner cloud is not included in this version, which implies the limitation to only one cloud owner (a car manufacturer cloud). Multi-user for this cloud if it was considered.

Useful Innovation:

- Protection against driver-based attacks.
- Management and security check for authorised drivers.
- On-live car compromised secure detection.

5 Conclusions & Future Work

In this deliverable D7.4, the FISHY consortium has presented all activities related to dissemination and communication, standardisation, and exploitation for the third and final year of FISHY, in the light of the accumulative work done along the whole project duration. The plans beyond the lifetime of the project are also presented and discussed, having in mind that in this period FISHY must maximize the impact and achieve all the KPIs related to dissemination, communication, standardisation, and exploitation.

During this final reporting period, we intensified the communication and exploitation activities based on the advanced level of R&D and the maturity of the FISHY technology in pair with the final state of its validation by the project's use cases. This allowed us to produce robust marketing materials with different industrial focus, capturing the benefits and challenges of the different domains tangential to the project, but consistent to the core aims that determine the vision of the FISHY team. This was very well accepted by a wide range of audiences we have targeted across several events in the lifetime of the project, from workshop participants to booth demo presentations.

The contribution to the scientific community was very substantial in this project, through: (i) the publication of research results in mostly open journals and conferences, sharing the knowledge over open research whenever possible and exposing it also through our Zenodo Community; (ii) the lively contribution to standards, positioning FISHY as a successful example of innovation to further adopt; and (iii) the contribution to Open Source Communities over the availability of the code, and the upstream of the different FISHY technologies by already OSS engaged partners.

This document reports on the achievements of all of these activities but also drafts the guidelines for the sustainability of the project's KERs in their different exploitation pathways as defined by IP owners and the consortium team, with the support of the Horizon Results Booster across three levels of coaching support to explore the best fit strategies. These HRB programmes have equipped us with valuable knowledge and skills, instilling confidence in our ability to elevate our innovation management to new heights. We express gratitude for the support we have received and eagerly anticipate harnessing our newfound expertise to drive continuous innovation and expansion.

6 References

[1] **J. Manzanas**, "FISHY HRB PDES-C Final Report," Horizon Results Booster, 2022.

[2] **J. Manzanas**, "FISHY HRB BPD Final Report," Horizon Results Booster, 2023.

[3] **M. A. Mancini**, "FISHY HRB G2M Final Report," Horizon Results Booster, 2023.

[4] FISHY Consortium (2021) **D7.2 (public) and D7.5 (confidential) Report on dissemination, standards and exploitation (Y1)**. Public version available at: https://fishy-project.eu/library/deliverables.

[5] FISHY Consortium (2021) **D7.3 (public) and D7.6 (confidential) Report on dissemination, standards and exploitation (Y2)**. Public version available at: https://fishy-project.eu/library/deliverables.

[6] Datatracker (2023) **Service Assurance for Intent-Based Networking Architecture** [RFC 9417], available at: https://datatracker.ietf.org/doc/draft-ietf-opsawg-service-assurance-architecture/

[7] Datatracker (2023) **Data Model for Lifecycle Management and Operations** [draft-palmero-opsawg-dmlmo-10], available at: https://datatracker.ietf.org/doc/draft-palmero-opsawg-dmlmo/

[8] Datatracker (2022) **Intent Classification** [RFC 9316], available at: https://datatracker.ietf.org/doc/rfc9316/

[9] Datatracker (2023) **An Evolution of Cooperating Layered Architecture for SDN (CLAS) for Compute and Data Awareness** [draft-contreras-coinrg-clas-evolution-01], available at: https://datatracker.ietf.org/doc/draft-contreras-coinrg-clas-evolution/

[10] Datatracker (2023) **Supply Chain Integrity, Transparency, and Trust** (scitt), available at: https://datatracker.ietf.org/wg/scitt/about/

[11] Datatracker (2023) **Network Inventory YANG** (ivy), available at: https://datatracker.ietf.org/wg/ivy/about/

[12] ISG (2023) **Add_Trust_management_service**, available at: https://docbox.etsi.org/ISG/ZSM/05-CONTRIBUTIONS/2022/ZSM(22)000343r3_ZSM014_Add_Trust_management_service.docx

[13] ISG (2023) **Report_NOC_Meeting__195**, available at: https://docbox.etsi.org/ISG/NFV/NOC/05-CONTRIBUTIONS/2023//NFVNOC(23)000017_Report_NOC_Meeting__195.docx

[14] CYBER (2023) **ONDS_-_Test_suite_TSS_TP**, available at: https://docbox.etsi.org/CYBER/CYBER/05-CONTRIBUTIONS/2023/CYBER(23)034004r1_ONDS_-_Test_suite_TSS_TP_.zip

[15] CYBER (2023) **ONDS_-_Test_suite_ Protection_Profile_-_Test_cases**, available at: https://docbox.etsi.org/CYBER/CYBER/05-CONTRIBUTIONS/2023/CYBER(23)034005r1_ONDS_-_Test_Suite_-_Protection_Profile_-_Test_cases.zip

[16] CYBER (2023) **ONDS_test_and_evaluation_-_new_work_item_discussion**, available at: https://docbox.etsi.org/CYBER/CYBER/05-CONTRIBUTIONS/2023/CYBER(23)034003_ONDS_test_and_evaluation_-_new_work_item_discussion.pptx

[17] https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_110_Athens/Docs/S3-231613.zip

[18] 3GPP (2023) **3GPP TSG-SA3 Meeting #110 S3-231489**, available at: https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_110_Athens/Docs/S3-231489.zip

[19] 3GPP (2023) **3GPP TSG-SA3 Meeting #110 S3-231358**, available at: https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_110_Athens/Docs/S3-231358.zip

[20] 3GPP (2023) **3GPP TSG-SA3 Meeting #111 S3-233090**, available at: https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_111_Berlin/Docs/S3-233090.zip

[21] 3GPP (2023) **3GPP TSG-SA3 Meeting #111 S3-233091**, available at: https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_111_Berlin/Docs/S3-233091.zip

[22] 3GPP (2023) **3GPP TSG-SA3 Meeting #111 S3-233092**, available at: https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_111_Berlin/Docs/S3-233092.zip

[23] 3GPP (2023) **3GPP TSG-SA3 Meeting #111 S3-233086**, available at: https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_111_Berlin/Docs/S3-233086.zip

[24] 3GPP (2023) **3GPP TSG-SA3 Meeting #111 S3-233085**, available at: https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_111_Berlin/Docs/S3-233085.zip

[25] 3GPP (2023) **3GPP TSG-SA3 Meeting #111 S3-233088**, available at: https https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_111_Berlin/Docs/S3-233088.zip

[26] 3GPP (2023) **3GPP TSG-SA3 Meeting #111 S3-233089**, available at: https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_111_Berlin/Docs/S3-233089.zip

[27] OSM (2023) **OSM-MR14 Ecosystem Day**, available at: https://osm.etsi.org/wikipub/index.php?title=OSM-MR14_Ecosystem_Day

[28] **UC3M** (2023) , available at: L2S-M https://github.com/Networks-it-uc3m/L2S-M

[29] **FISHY GitHub (2023)**, available at: https://github.com/H2020-FISHY

[30] ETSI (2023) **ETSI Software Development Groups flyer**, available at: https://www.etsi.org/images/News/2023/pdf/SDG_flyer_2023_v03.pdf

[31] European Commission (2023), **The EU cybersecurity certification framework**, available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework

[32] European Commission (2023), **The EU cybersecurity certification group**, available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-group

[33] European Commission (2023), **Cyber Act Certification**, available at: https://www.cyberactcertification.eu/

[34] European Commission (2020) **Open Source Software Strategy 2020-2023**, , available at: https://commission.europa.eu/system/files/2023-02/en_ec_open_source_strategy_2020-2023.pdf

[35] European Commission (2020) **EIC Transition**, available at: https://eic.ec.europa.eu/eic-funding-opportunities/eic-transition_en

[36] Strategyzer (2020) **Value proposition canvas**, available at: https://www.strategyzer.com/canvas/value-proposition-canvas

[37] Best3minutes (2018) **The Pitch Canvas**, available at: https://best3minutes.com/the-pitch-canvas/

[38] **A. Osterwalder, Business Model Generation: A Handbook For Visionaries, Game Changers, and Challengers.**, vol. John Wiley & Sons, John Wiley & Sons, 2010.

[39] SWForum.EU (2021) **Improving exploitation of Project outcomes using MTRL [online]**, available at: https://swforum.eu/news/swforumeu-improving-exploitation-project-outcomes-using-mtrl

[40] **Moore, Geoffrey A., and Regis McKenna** (1999) Crossing the chasm. Collins Business Essentials.

[41] **Barcelona Cybersecurity Congress 2023**: https://www.barcelonacybersecuritycongress.com/

[42] **Open Config project**: https://www.openconfig.net/

[43]FISHY Consortium (2022) D2.3 (public) and D2.6 (confidential) versions of **Tracking External Efforts, Technology Evolution and Business Trends**. Public version available at https://fishy-project.eu/library/deliverables

[44] FISHY Consortium (2022) D6.2 **IT-1 FISHY Release Validated**. Available at https://fishy-project.eu/library/deliverables

[45]FISHY Consortium (2023) D6.4 **IT-2 FISHY Final Release**

7 Annexes

7.1 Publications

In this annex it is listed the total number of publications with ACK to FISHY during the whole duration of the project.

7.1.1 Conference Papers

1. Scalability analysis of a blockchain-based security strategy for complex IoT systems

DOI 10.1109/HPSR52026.2021.9481865

Type of publication Conference Proceedings

Repository link https://ieeexplore.ieee.org/xpl/conhome/9481789/proceeding

Link to publication https://ieeexplore.ieee.org/document/9481865

Authors Martí Miquel Martínez, Eva Marin-Tordera;,Xavi Masip-Bruin

Title of journal/proceedings/book series/bok Proceedings of 2021 IEEE 22nd International Conference on High Performance Switching and Routing (HPSR)

Number, date or frequency of the Journal/proceedings/book

Relevant pages

ISBN

Publisher IEEE

Place of publication Paris, France

Year of publication 2021

Is this publication available in Open Access, or it will be made available? No

Is this a peer-reviewed publication? Yes

Is this a joint public/private publication? Public

2. Farm to fork: securing a supply chain with direct impact on food security

DOI 10.1109/HPSR52026.2021.9481866

Type of publication Conference Proceedings

Repository link https://ieeexplore.ieee.org/xpl/conhome/9481789/proceeding

Link to publication https://ieeexplore.ieee.org/document/9481866

Authors Panagiotis Trakadas; Helen C. Leligou; Panagiotis Karkazis; Antonis Gonos; Theodore Zahariadis

Title of journal/proceedings/book series/bok Proceedings of 2021 IEEE 22nd International Conference on High Performance Switching and Routing (HPSR)

Number, date or frequency of the Journal/proceedings/book

Relevant pages

ISBN

Publisher IEEE

Place of publication Paris, France

Year of publication 2021

Is this publication available in Open Access, or it will be made available? No

Is this a peer-reviewed publication? Yes

Is this a joint public/private publication? Public

3. Challenges in the Automotive Software Supply Chain, Connected CAR : Benefits from an Intent Policy framework

DOI 10.1109/HPSR52026.2021.9481853

Type of publication Conference Proceedings

Repository link https://ieeexplore.ieee.org/xpl/conhome/9481789/proceeding

Link to publication https://ieeexplore.ieee.org/document/9481853

Authors Jose Soriano; Guillermo Jiménez; Ernesto Correa; Noel Ruiz

Title of journal/proceedings/book series/bok Proceedings of 2021 IEEE 22nd International Conference on High Performance Switching and Routing (HPSR)

Number, date or frequency of the Journal/proceedings/book

Relevant pages

ISBN

Publisher IEEE

Place of publication Paris, France

Year of publication 2021

Is this publication available in Open Access, or it will be made available? No

Is this a peer-reviewed publication? Yes

Is this a joint public/private publication? Public

4. The Role of Intent-Based Networking in ICT Supply Chains

DOI 10.1109/HPSR52026.2021.9481801

Type of publication Conference Proceedings

Repository link https://ieeexplore.ieee.org/xpl/conhome/9481789/proceeding

Link to publication https://ieeexplore.ieee.org/document/9481801

Authors Mounir Bensalem; Jasenka Dizdarević; Francisco Carpio; Admela Jukan

Title of journal/proceedings/book series/bok Proceedings of 2021 IEEE 22nd International Conference on High Performance Switching and Routing (HPSR)

Number, date or frequency of the Journal/proceedings/book

Relevant pages

ISBN

Publisher IEEE

Place of publication Paris, France

Year of publication 2021

Is this publication available in Open Access, or it will be made available? No

Is this a peer-reviewed publication? Yes

Is this a joint public/private publication? Public

5. Information Security Assessment and Certification within Supply Chains

DOI 10.1145/3465481.3470078

Type of publication Conference Proceedings

Repository link https://dl.acm.org/doi/proceedings/10.1145/3465481

Link to publication https://dl.acm.org/doi/10.1145/3465481.3470078

Authors Henrique Santos, André Oliveira, Lúcia Soares, Alan Satis, Alexandre Santos

Title of journal/proceedings/book series/bok Proceedings of ARES 2021: The 16th International Conference on Availability, Reliability and Security

Number, date or frequency of the Journal/proceedings/book

Relevant pages

ISBN

Publisher ACM Digital Library

Place of publication Vienna, Austria

Year of publication 2021

Is this publication available in Open Access, or it will be made available? No

Is this a peer-reviewed publication? Yes

Is this a joint public/private publication? Public

6. Engineering and Experimentally Benchmarking a Serverless Edge Computing System

DOI 10.1109/GLOBECOM46510.2021.9685235

Type of publication Conference Proceedings

Repository link https://ieeexplore.ieee.org/xpl/conhome/9685019/proceeding

Link to publication https://ieeexplore.ieee.org/document/9685235

Authors Francisco Carpio, Marc Michalke, Admela Jukan

Title of journal/proceedings/book series/bok Proceedings of the 2021 IEEE Global Communications Conference

Number, date or frequency of the Journal/proceedings/book

Relevant pages

ISBN

Publisher IEEE

Place of publication Madrid, Spain

Year of publication 2021

Is this publication available in Open Access, or it will be made available? No

Is this a peer-reviewed publication? Yes

7. A Machine Learning IDS for Known and Unknown Anomalies

DOI 10.1109/DRCN53993.2022.9758010

Type of publication Conference Proceedings

Repository link https://ieeexplore.ieee.org/xpl/conhome/9758003/proceeding

Link to publication https://ieeexplore.ieee.org/document/9758010

Authors F. Aguiló–Gost; E. Simó–Mezquita; E. Marín–Tordera; A. Hussain

Title of journal/proceedings/book series/bok Proceedings of the 2022 International Workshop on Design of Reliable Communication Networks (DRCN)

Number, date or frequency of the Journal/proceedings/book

Relevant pages

ISBN

Publisher IEEE

Place of publication Vilanova i la Geltrú, Spain

Year of publication 2022

Is this publication available in Open Access, or it will be made available? No

Is this a peer-reviewed publication? Yes

8. Continuous Industrial Sector Cybersecurity Assessment Paradigm* : Proposed Model of Cybersecurity Certification

DOI 10.1109/DRCN53993.2022.9758022

Type of publication Conference Proceedings

Repository link https://ieeexplore.ieee.org/xpl/conhome/9758003/proceeding

Link to publication https://ieeexplore.ieee.org/document/9758022

Authors André da Silva Oliveira; Henrique Santos

Title of journal/proceedings/book series/bok Proceedings of the 2022 International Workshop on Design of Reliable Communication Networks (DRCN)

Number, date or frequency of the Journal/proceedings/book

Relevant pages

ISBN

Publisher IEEE

Place of publication Vilanova i la Geltrú, Spain

Year of publication 2022

Is this publication available in Open Access, or it will be made available? No

Is this a peer-reviewed publication? Yes

9. Benchmarking Various ML Solutions in Complex Intent-Based Network Management Systems

DOI 10.23919/MIPRO55190.2022.9803584

Type of publication Conference Proceedings

Repository link

Link to publication https://ieeexplore.ieee.org/document/9803584

Authors Mounir Bensalem; Jasenka Dizdarević; Admela Jukan

Title of journal/proceedings/book series/bok Proceedings of 2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO)

Number, date or frequency of the Journal/proceedings/book

Relevant pages

ISBN

Publisher IEEE

Place of publication Opatija, Croatia

Year of publication 2022

Is this publication available in Open Access, or it will be made available? No

Is this a peer-reviewed publication? Yes

Is this a joint public/private publication? Public

10. A model of capabilities of Network Security Functions

DOI 10.1109/NetSoft54395.2022.9844057

Type of publication Conference

Repository link https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=65

Link to publication https://ieeexplore.ieee.org/document/9844057

Authors Cataldo Basile; Daniele Canavese; Leonardo Regano; Ignazio Pedone; Antonio Lioy

Title of journal/proceedings/book series/bok Proceedings of 2022 IEEE 8th International Conference on Network Softwarization (NetSoft)

Number, date or frequency of the Journal/proceedings/book

Relevant pages

ISBN

Publisher IEEE

Place of publication Milan, Italy

Year of publication 2022

Is this publication available in Open Access, or it will be made available? No

Is this a peer-reviewed publication? Yes

Is this a joint public/private publication? Public

11. Incident Handling for Healthcare Organizations and Supply-Chains

DOI 10.1109/ISCC55528.2022.9912965

Type of publication Conference

Repository link https://ieeexplore.ieee.org/xpl/conhome/9912737/proceeding

Link to publication https://ieeexplore.ieee.org/document/9912965

Authors Eftychia Lakka; George Hatzivasilis; Stylianos Karagiannis; Andreas Alexopoulos; Manos Athanatos; Sotiris Ioannidis; Manolis Chatzimpyrros; Grigoris Kalogiannis; George Spanoudakis

Title of journal/proceedings/book series/bok Proceedings of 2022 IEEE Symposium on Computers and Communications (ISCC)

Number, date or frequency of the Journal/proceedings/book

Relevant pages

ISBN

Publisher IEEE

Place of publication Rhodes, Greece

Year of publication 2022

Is this publication available in Open Access, or it will be made available? No

Is this a peer-reviewed publication? Yes

Is this a joint public/private publication? Public

12. A data infrastructure for heterogeneous telemetry adaptation. Application to Netflow-based cryptojacking detection

DOI 10.1109/ICIN56760.2023.10073490

Type of publication Conference

Repository link https://ieeexplore.ieee.org/xpl/conhome/10072394/proceeding

Link to publication https://ieeexplore.ieee.org/document/10073490

Authors Alejandro Moreno (ATOS) Antonio Pastor (TID), Ignacio D. Martínez-Casanueva (TID), Daniel González-Sánchez (UPM) y Luis Bellido Triana (UPM)

Title of journal/proceedings/book series/bok Proceedings of the 26th Conference on Innovation in Clouds, Internet and Networks, ICIN 2023

Number, date or frequency of the Journal/proceedings/book

Relevant pages

ISBN

Publisher

Place of publication Paris, France

Year of publication 2023

Is this publication available in Open Access, or it will be made available?

Is this a peer-reviewed publication? Yes

Is this a joint public/private publication? Public

13. Security in DevSecOps: Applying Tools and Machine Learning to Verification and Monitoring Steps

DOI https://doi.org/10.1145/3578245.3584943

Type of publication Conference

Repository link https://dl.acm.org/doi/proceedings/10.1145/3578245

Link to publication https://dl.acm.org/doi/10.1145/3578245.3584943

Authors Matija Cankar, Nenad Petrovic, Joao Pita Costa, Ales Cernivec), Jan Antic, Tomaz Martincic, Dejan Stepec

Title of journal/proceedings/book series/bok Proceedings of the ICPE '23 conference

Number, date or frequency of the Journal/proceedings/book

Relevant pages Pages 201–205

ISBN

Publisher

Place of publication Coimbra, Portugal

Year of publication 2023

Is this publication available in Open Access, or it will be made available?

Is this a peer-reviewed publication? Yes

Is this a joint public/private publication? Public

14. Runtime Security Monitoring by an Interplay Between Rule Matching and Deep Learning-Based Anomaly Detection on Logs

DOI 10.1109/DRCN57075.2023.10108105

Type of publication Conference

Repository link https://ieeexplore.ieee.org/xpl/conhome/10108077/proceeding

Link to publication https://ieeexplore.ieee.org/document/10108105

Authors Jan Antić, Joao Pita Costa, Aleš Černivec, Matija Cankar, Tomaž Martinčič, Aljaz Potocnik,

Hrvoje Ratkajec, Gorka Benguria Elguezabal, Nelly Leligou, Alexandra Lakka, Ismael Torres Boigues

Title of journal/proceedings/book series/bok Proceedings of the Conference DRCN 2023

Number, date or frequency of the Journal/proceedings/book

Relevant pages

ISBN

Publisher IEEE

Place of publication Vilanova i la Geltrú, Spain

Year of publication 2023

Is this publication available in Open Access, or it will be made available?

Is this a peer-reviewed publication? Yes

Is this a joint public/private publication? Public

15. An NIDS for Known and Zero-Day Anomalies

DOI 10.1109/DRCN57075.2023.10108319

Type of publication Conference

Repository link https://ieeexplore.ieee.org/xpl/conhome/10108077/proceeding

Link to publication https://ieeexplore.ieee.org/document/10108105

Authors Ayaz Hussain; Francesc Aguiló-Gost; Ester Simó-Mezquita; Eva Marín-Tordera; Xavier Massip

Title of journal/proceedings/book series/bok Proceedings of the Conference DRCN 2023

Number, date or frequency of the Journal/proceedings/book

Relevant pages

ISBN

Publisher IEEE

Place of publication Vilanova i la Geltrú, Spain

Year of publication 2023

Is this publication available in Open Access, or it will be made available?

Is this a peer-reviewed publication? Yes

Is this a joint public/private publication? Public

16. MONCHi MONitoring for Cloud-native Hyperconnected Islands

DOI

Type of publication Conference (Workshop)

Repository link https://asmta2023.sciencesconf.org/

Link to publication

Authors Dulce N. de M. Artalejo, Ivan Vidal, Francisco Valera, and Borja Nogales

Title of journal/proceedings/book series/bok LNCS book from Springer, proceedings of ECMS International Conference on Modelling and Simulation

Number, date or frequency of the Journal/proceedings/book

Relevant pages

ISBN

Publisher Springer

Place of publication Florence, Italy

Year of publication 2023

Is this publication available in Open Access, or it will be made available? No

Is this a peer-reviewed publication? Yes

Is this a joint public/private publication? Public

17. A Model for Automated Cybersecurity Threat Remediation and Sharing

DOI

Type of publication Conference

Repository link

Link to publication

Authors Francesco Settanni, Leonardo Regano, Cataldo Basile and Antonio Lioy

Title of journal/proceedings/book series/bok Proceedings of the SecSoft - 5th International Workshop on Cyber-Security in Software-defined and Virtualized Infrastructures(co-located NetSoft2023)

Number, date or frequency of the Journal/proceedings/book

Relevant pages

ISBN

Publisher

Place of publication Madrid

Year of publication June 2023

Is this publication available in Open Access, or it will be made available? No

Is this a peer-reviewed publication? Yes

Is this a joint public/private publication? Public

7.1.2 Posters

1. Providing Secure NFV Multi Site Connectivity Services

DOI To be added

Type of publication Poster

Repository Link

Link to publication

Authors José Manuel Manjón Cáliz; Borja Nogales; Diego R. López; Antonio Pastor, Antonio; Iván Vidal; Francisco Valer

Title of journal/proceedings/book series/bok Proceedings of the 2023 EuCNC & 6G Summit

Number, date or frecuency of the Journal/proceedings/book

Relevant pages

ISBN

Publisher

Place of publication Gothenburg, Sweden

Year of publication 2023

Is this publication available in Open Access, or it will be made available? Yes (the poster)

Is this a peer-reviewed publication? Yes

Is this a joint public/private publication? Public

2. A Multi-domain Testbed for Collaborative Research on the IoT-Edge-Cloud Continuum

DOI To be added

Type of publication Poster

Repository link To be added

Link to publication To be added

Authors Ivan Vidal, Luis F. Gonzalez, Francisco Valera, Borja Nogales Raul Martin, Dulce Artalejo, Diego R. Lopez, Jose M. Majon and Antonio Pastor

Title of journal/proceedings/book series/bok Proceedings of the 2023 20th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)

Number, date or frecuency of the Journal/proceedings/book

Relevant pages

ISBN

Publisher IEEE

Place of publication Madrid

Year of publication September 2023

Is this publication available in Open Access, or it will be made available? No

Is this a peer-reviewed publication? Yes

Is this a joint public/private publication? Public

7.1.3 Journal Papers

1. Cybersecurity in ICT Supply Chains: Key Challenges and a Relevant Architecture

DOI https://doi.org/10.3390/s21186057

Type of publication Journal

Repository link https://www.mdpi.com/journal/sensors

Link to publication https://www.mdpi.com/1424-8220/21/18/6057

Authors Xavi Masip-Bruin, Eva Marín-Tordera, José Ruiz, Admela Jukan, Panagiotis Trakadas, Ales Cernivec, Antonio Lioy, Diego López, Henrique Santos, Antonis Gonos, Ana Silva, José Soriano, Grigorios Kalogiannis

Title of journal/proceedings/book series/bok Sensors

Number, date or frecuency of the Journal/proceedings/book 21(18), 6057;

Relevant pages

ISBN

Publisher MDPI

Place of publication

Year of publication 2021

Is this publication available in Open Access, or it will be made available? Yes

Is this a peer-reviewed publication? Yes

Is this a joint public/private publication? Public

2. The Green Blockchains of Circular Economy

DOI https://doi.org/10.3390/electronics10162008

Type of publication journal

Repository link https://www.mdpi.com/journal/electronics

Link to publication https://www.mdpi.com/2079-9292/10/16/2008

Authors George Hatzivasilis, Sotiris Ioannidis, Konstantinos Fysarakis, George Spanoudakis, Nikos Papadakis

Title of journal/proceedings/book series/bok Electronics 2021

Number, date or frecuency of the Journal/proceedings/book 10(16), 2008

Relevant pages

ISBN

Publisher MDPI

Place of publication

Year of publication 2021

Is this publication available in Open Access, or it will be made available? Yes

Is this a peer-reviewed publication? Yes

Is this a joint public/private publication? Public

3. Scaling migrations and replications of Virtual Network Functions based on network traffic forecasting

DOI https://doi.org/10.1016/j.comnet.2021.108582

Type of publication Journal

Repository link https://www.sciencedirect.com/journal/computer-networks/vol/203/suppl/C

Link to publication: https://www.sciencedirect.com/science/article/pii/S1389128621004898?via%3Dihub

Authors Francisco Carpio, Wolfgang Bziuk, , Admela Jukan

Title of journal/proceedings/book series/bok Computer Networks

Number, date or frecuency of the Journal/proceedings/book Volume 203, 11 February 2022, 108582

Relevant pages

ISBN

Publisher Elsevier

Place of publication

Year of publication 2022

Is this publication available in Open Access, or it will be made available? Yes

Is this a peer-reviewed publication? Yes

Is this a joint public/private publication? Public

4. A Combinatorial Reliability Analysis of Generic Service Function Chains in Data Center Networks

DOI https://doi.org/10.1145/3477046

Type of publication Journal

Repository link

Link to publication https://dl.acm.org/doi/10.1145/3477046

Authors Anna Engelmann, Admela Jukan

Title of journal/proceedings/book series/bok ACM Transactions on Modeling and Performance Evaluation of Computing Systems

Number, date or frecuency of the Journal/proceedings/book Volume 6,Issue 3, September 2021

Relevant pages

ISBN

Publisher ACM Digital Library

Place of publication

Year of publication 2021

Is this publication available in Open Access, or it will be made available? Yes

Is this a peer-reviewed publication? Yes

Is this a joint public/private publication? Public

5. A Secure Link-Layer Connectivity Platform for Multi-Site NFV Services

DOI https://doi.org/10.3390/electronics10151868

Type of publication Journal

Repository link https://www.mdpi.com/journal/electronics

Link to publication https://mdpi-res.com/d_attachment/electronics/electronics-10-01868/article_deploy/electronics-10-01868-v3.pdf?version=1628143516

Authors Ivan Vidal, Borja Nogales , Diego Lopez, Juan Rodríguez, Francisco Valera and Arturo Azcorra

Title of journal/proceedings/book series/bok Electronics 2021

Number, date or frecuency of the Journal/proceedings/book 10, 1868

Relevant pages

ISBN

Publisher MDPI

Place of publication

Year of publication 2021

Is this publication available in Open Access, or it will be made available? Yes

Is this a peer-reviewed publication? Yes

6. Link Layer Connectivity as a Service for Ad-Hoc Microservice Platforms

DOI 10.1109/MNET.001.2100363
Type of publication Journal
Repository link https://ieeexplore.ieee.org/xpl/tocresult.jsp?isnumber=9740617
Link to publication https://ieeexplore.ieee.org/document/9740640
Authors Luis F. Gonzalez; Ivan Vidal; Francisco Valera; Diego R. Lopez
Title of journal/proceedings/book series/bok IEEE Network
Number, date or frecuency of the Journal/proceedings/book Volume: 36, Issue: 1
Relevant pages
ISBN
Publisher IEEE
Place of publication
Year of publication January/February 2022
Is this publication available in Open Access, or it will be made available? No
Is this a peer-reviewed publication? Yes

7. BenchFaaS: Benchmarking Serverless Functions in an Edge Computing Network Testbed

DOI 10.1109/MNET.125.2200294
Type of publication Journal
Repository link https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=65
Link to publication https://ieeexplore.ieee.org/document/9877930

Title
Authors Francisco Carpio; Marc Michalke; Admela Jukan
Title of journal/proceedings/book series/bok IEEE Networks
Number, date or frecuency of the Journal/proceedings/book
Relevant pages 1 - 8
ISBN
Publisher IEEE
Place of publication
Year of publication 2022
Is this publication available in Open Access, or it will be made available? No
Is this a peer-reviewed publication? Yes
Is this a joint public/private publication? Public

7.1.4 Blog Posts

Table 10 - Blog posts

Partner	***Date***	***Titles***
ATOS	*February 28, 2021*	*FISHY: Trustful and smart cybersecurity for supply chains*

UPC	*May 14, 2021*	*Securing IoT nodes in supply of chains*
SYN	*June 30, 2021,*	*Vulnerability Assessment*
SONAE	*August 31, 2021*	*The importance of security in the Industry 4.0 paradigm*
CAPGEMINI	*October 27, 2021*	*FISHY, IoT Security for the automotive Supply Chain*
XLAB	*December 21, 2021*	*The importance of early detection of vulnerabilities and attacks for a healthy supply chain*
POLITO	*March 7, 2022*	*Easing the burden of network configuration: a capability-driven approach*
TID	*May 7, 2022*	*A reference framework for FISHY*
TUBS	*June 30, 2022*	*Intent-based Resilience Orchestration in Supply Chains*
ENTERSOFT/SYN	*September 29, 2022*	*Experiences from validation of FISHY in the Farm to Fork use case*
STS	*October 31, 2022*	*The role of Security Assurance Certification Module on a Supply Chain*
UMINHO	*December 22, 2022*	*Security and Privacy Data Space Infrastructure*
XLAB, UPC, ATOS, UC3M	*January 31, 2023*	*FISHY's Demo & Booth at the Barcelona Cybersecurity Congress 2023*
XLAB	*April 12, 2023*	*Wrapping-up the Horizon Results Booster experience with innovation management training and a hands-on workshop*
CAPGEMINI	*May 15, 2023*	*Video-blog: FISHY SADE use case*
SONAE	*May 15, 2023*	*Video-blog: FISHY SADE use case*
SYN	*May 16, 2023*	*Video-blog: F2F use case demo*
SYN	*May 26, 2023*	*Using blockchain technology to secure security information*
UPC	*July 25, 2023*	*FISHY liaisons and collaborations*
XLAB	*August 16, 2023*	*Key Innovations in Supply Chain Cybersecurity and Resillience that Make Sense in Today's Industry*
XLAB	August 30, 2023	*Video-blog: TIM*
UC3M	*To be added*	*Video-blog: SIA-FRF*
ATOS/UPC	*August 31, 2023*	*[to be announced]*

In summary we have the following:

Table 11 - List of communication activities

ACTIVITY	**Number of Activities (Activities in M19-M36)**

Organisation of a Conference	0(0)
Organisation of a Workshop	4(2)
Press release	3(2)
Non-scientific and non-peer-reviewed publication	23 (13)
Exhibition	3(0)
Flyer	1(1)
Training	6(1)
Social Media	405 (263)[46]
Website	19785 (12564)[47]
Communication Campaign (e.g. Radio, TV)	0
Participation to a Conference	17(6)
Participation to a Workshop	4(2)
Participation to an Event other than a Conference or a Workshop	24(5)
Video/Film	6(2)
Brokerage Event	0
Pitch event	8
Trade Fair	2
Participation in activities organized jointly with other EU project(s)	8(3)
Other	0

Table 12 - People reached by FISHY

CATEGORY	Estimated number of persons
Scientific Community (Higher Education, Research)	2000-2500
Industry	600-1000
Civil Society	80-100
General Public	700
Policy Makers	100
Media	500
Investors	10
Customers	50
Other	0

[46] Number of followers of Twitter and LinkedIn at the end of the project and in Y2
[47] Number of page views

7.2 Web and social media data

In this annex FISHY presents some extra data about activity in the FISHY website and in social media.

7.2.1 Website analytics

Until June 2023 the data analytics about FISHY website has been collected from Google Analytics. Figure 15, Figure 16, Figure 17 and Figure 18 show the evolution of users during the whole project, the origin of the users, the top channels of accessing the FISHY website and the most visited pages respectively. As it has been reported in previous deliverables, peaks in users are usually related to main publications in the website as blog entries or deliverables. Also it is noticeable in the origin of the users, that we can find countries from partners but also other such as United State, France, India, Netherlands, etc. Finally, regarding the most visited pages during the 3 years of project (until June 2023), it is remarkable that apart of the consortium page, the use case, the blog and news are the most visited pages.

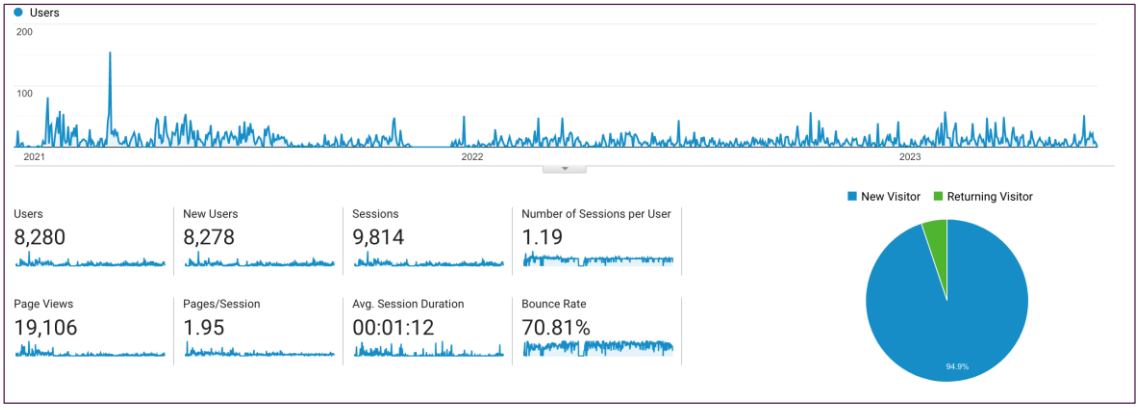


Figure 15 - Website summary analysis until June 2023

	Country	Users	% Users
1.	Spain	3,011	36.33%
2.	United States	622	7.50%
3.	Portugal	541	6.53%
4.	Greece	504	6.08%
5.	Italy	382	4.61%
6.	Slovenia	333	4.02%
7.	Germany	273	3.29%
8.	Netherlands	220	2.65%
9.	India	215	2.59%
10.	France	202	2.44%

Figure 16 - Users' country until June 2023

Figure 17 - FISHY website access and users' gender until June 2023

	Page	Page Views	% Page Views
1.	/	5,371	28.11%
2.	/consortium	932	4.88%
3.	/news-events	911	4.77%
4.	/casos-de-uso	762	3.99%
5.	/blog	605	3.17%
6.	/que-es-el-5g	476	2.49%
7.	/form/contact	450	2.36%
8.	/farm-fork-f2f	407	2.13%
9.	/library/deliverables	381	1.99%
10.	/coordinated-framework-cyber-resilient-supply-chain-systems-over-complex-ict-infrastructures	374	1.96%

Figure 18 - Most visited pages until June 2023.

From June 2023 the way of analysing the FISHY website was changed, and the analysis of the last period of the project is shown in Figure 19 and Figure 20. The effect of the last communication campaign started in May, can be observed with the growing interest on blog posts and promotional material.

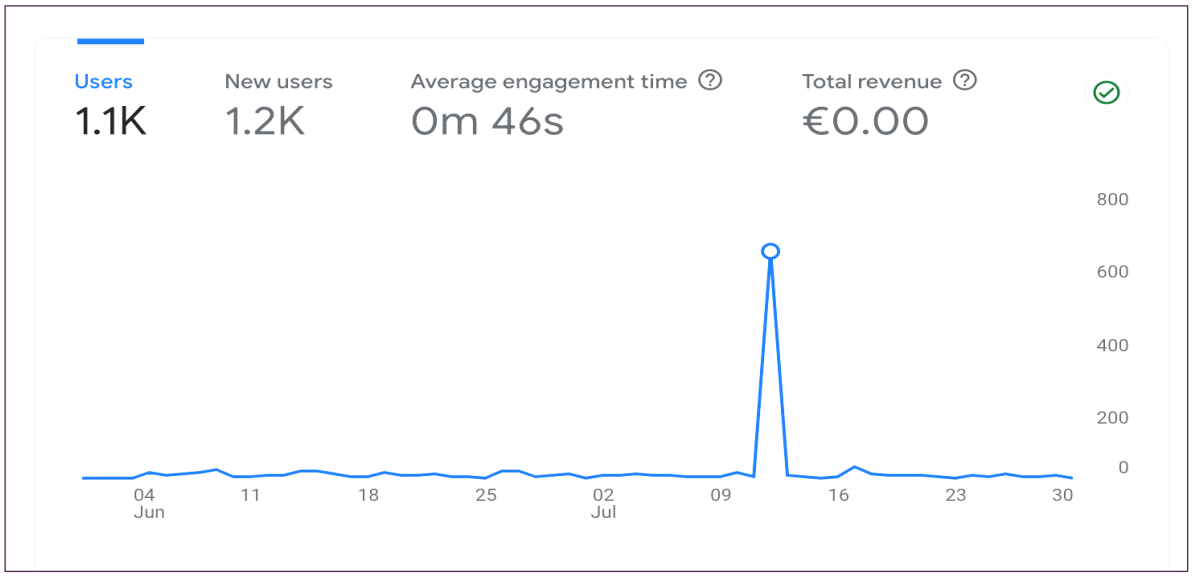


Figure 19 - Website analysis from June 2023

		2,917 100% of total	1,051 100% of total	2.78 Avg 0%	0m 46s Avg 0%	6,135 100% of total
1	/	2,386	777	3.07	0m 52s	4,362
2	/blog	48	26	1.85	0m 31s	153
3	/news-events	44	21	2.10	0m 17s	115
4	/library/deliverables	43	24	1.79	0m 38s	172
5	/farm-fork-f2f	25	25	1.00	0m 15s	91
6	/project/promotional_material	23	16	1.44	0m 25s	72
7	/promotional-material/fishy-pitch-deck	21	12	1.75	0m 13s	63
8	/consortium	20	20	1.00	0m 10s	76
9	/blog/fishy-sade-use-case	18	14	1.29	0m 08s	61
10	/publications	17	12	1.42	0m 25s	55

Figure 20 - Most visited pages from June 2023

7.2.2 Social media

Some of the most appreciated posts, 3 of them relate to important events in the project: GAs, FISHY summer camp and the Cybersecurity Congress, as well as a post related to one of the FISHY video blogs (see Figure 21).

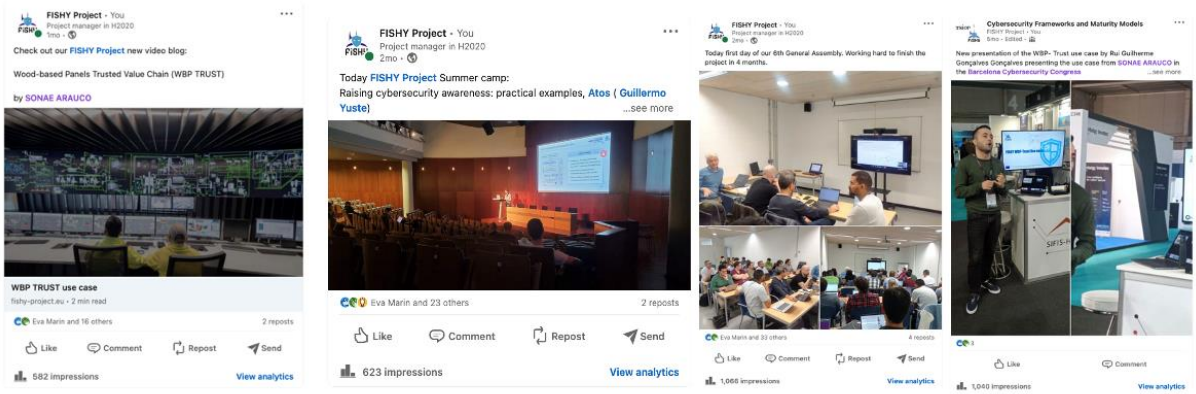


Figure 21 - Some of the most appreciated posts

Regarding Twitter, during this last year the FISHY account had 6K impressions, and some of the most appreciated tweets in Figure 22, also most of them related to the event in the Cybersecurity Congress.

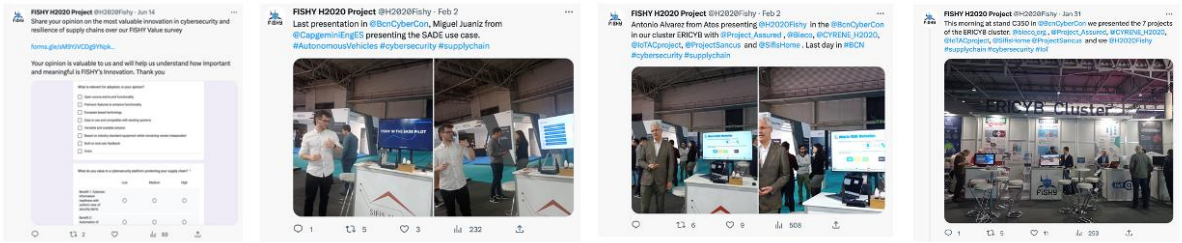


Figure 22 - Some of the most appreciated tweets

7.2.3 IP background and IP results

For the sake of completeness, we present in this section the registry log of the KERs, ERs, IP results and IP background corresponding to the research and development in FISHY, including the IDs used across this deliverable. Some of the results are crossed out due to the reorganization described in the section 4.3.1.

Table 13 - FISHY IP background log

ID	Name	Owner(s)	License
IPB-1	Extended Continuous Risk Assessment Engine	ATOS	Proprietary Copyright
IPB-2	XL-SIEM	ATOS	Proprietary Copyright
IPB-3	SynField devices and platform	SYN	Proprietary Copyright
IPB-4	Wazuh extensions for vulnerability assessment	XLAB	GPL v2, partial copyright, OpenSSL licence

IPB-5	Vulnerability Assessment Tool (VAT)	XLAB	Proprietary Copyright
~~IPB-6~~	~~xOpera~~	~~XLAB~~	~~Open Source Apache 2.0~~
IPB-7	Integrity assessment toolkit	POLITO	Open Source APL 2.0
IPB-8	OSM Network Orchestration	TID	Open Source Apache 2.0
IPB-9	Netphony routning control Framework	TID	Open Source Apache 2.0
IPB-10	MAMI ACME-STAR	TID	Open Source Apache 2.0
IPB-11	TID virtualized implementation for synthetic traffic generation	TID	Standards FRAND
IPB-12	TID monitoring platform	TID	Standards FRAND
~~IPB-13~~	~~TID OPoT implementation~~	~~TID~~	~~Standards FRAND~~
IPB-14	TIB Blockchain-based network assurance tool	TID	Standards FRAND
IPB-15	TID mcTLS-based security services	TID	Standards FRAND
IPB-16	Secure Edge Node (SEN)	UPC	Open Source Apache 2.0
IPB-17	Predictive Maintenance Tool (PMEM)	UPC	Open Source Apache 2.0
IPB-18	Intent-based resilience orchestrator (IRO)	TUBS	Open Source Apache 2.0
IPB-19	Aberon Warehouse Management System	OPT	Proprietary Copyright
IPB-20	Know-how, experience and data owned by SONAE on smart industry	SONAE	Proprietary Copyright
IPB-21	ENSCONCE components	CAPGEMINI	Confidential Open Source
IPB-22	EDGE components	CAPGEMINI	Confidential Open Source
IPB-23	REMOTIS car components	CAPGEMINI	Confidential Open Source
IPB-24	REMOTIS SW components	CAPGEMINI	Confidential Open Source
IPB-25	Recognition and GDPR SW	CAPGEMINI	Confidential Open Source
IPB-26	Semantic Data Collector (SDA)	TID	Open Source Apache 2.0
IPB-27	CCIPS TID	TID	Open Source Apache 2.0

IPB-28	Continuous assessment of security and privacy	STS	Proprietary Copyright
IPB-29	Attack Remediation Engine (ARE)	POLITO	Open Source APL 2.0
IPB-30	vNSF in the SIA block	POLITO	Open Source APL 2.0
IPB-31	Model-driven customisations to Keycloak enabling the realisation of different security standards and risk management requirements	UMinho	Open Source APL 2.0
IPB-33	Know-how, experience and data owned by SYN on F2F	SYN	Proprietary Copyright
IPB-34	Know-how, experience and data owned by ALTRAN on autonomous driving funtion at the edge	CAPGEMINI	Proprietary Copyright
IPB-35	Prototype developed by the company in previous projects , including the SPAP platform (GUI), auditing mechanism and evidence collection engine with several metrics	STS	Proprietary Copyright
IPB-36	Know-how, related to best-practices and performance comparison among technologies used in IoT architectures	UMinho	Proprietary Copyright
IPB-37	Monitoring systems	UMinho	Proprietary Copyright
IPB-38	Security evaluation and metrics	UMinho	GPL v2, partial copyright, OpenSSL license

Table 14 - FISHY IP results log

IP Result	Name	Owner(s)	License
IPR-1	Wazuh extensions	XLAB	Open Source GPL v.2
IPR-2	VAT extensions	XLAB	Proprietary Copyright
IPR-3	Enhanced capabilities for ATOS XL-SIEM	ATOS	Proprietary Copyright
IPR-4	Extended Continuous Risk Assessment Engine	ATOS	Proprietary Copyright
~~IPR-5~~	~~Standardised API for network infrastructure abstraction~~	~~TID~~	~~Open Source Apache 2.0~~
IPR-6	Centrally Controlled IPsec (CCIPS)	TID	Open Source Apache 2.0

IPR-7	Security Assurance & Certification Management Platform	STS	Proprietary Copyright
IPR-8	Detection and protection components	XLAB	Open Source GPLv2
~~IPR-9~~	~~Extensions to xOpera~~	~~XLAB~~	~~Apache 2.0~~
~~IPR-10~~	~~ILT-based warehouse management system~~	~~OPT~~	~~Proprietary Copyright~~
IPR-11	Evidence-based data monitoring platform	SYN	Proprietary Copyright
IPR-12	Trustworthy identification and authentication of edge systems	UPC	Open Source Apache 2.0
IPR-13	Advanced Mitigation strategy - PMEM	UPC	Open Source Apache 2.0
IPR-14	Intent-based resilience orchestrator (IRO)	TUBS	Open Source Apache 2.0
IPR-15	Integrity Assessment Toolkit (Trust monitor extension)	POLITO	Open Source Apache 2.0
IPR-16	Framework for InfSec evaluation within IoT	UMinho	Open Source GPL v.2
IPR-17	Link-Layer Secure connectivity for Microservice platforms (L2S-M)	UC3M	Open Source Apache 2.0
IPR-18	ETSI Open Source MANO (OSM) extension	UC3M	Open Source Apache 2.0
IPR-19	LOMOS extension to FISHY	XLAB	Proprietary Copyright
IPR-20	EDC (Enforcement & Dynamic Configuration)	POLITO	Open Source MIT
IPR-21	Recommendation module	POLITO	Open Source MIT
IPR-22	Central Repository	XLAB	Open Source Apache 2.0
IPR-23	FISHY Platform GUI	UPC	Open Source Apache 2.0
IPR-24	FISHY SandBox	UC3M	Open Source Apache 2.0
IPR-25	FISHY Brand	ATOS	Proprietary Copyright
IPR-26	Smart Contracts	SYN	Open Source Apache 2.0
IPR-27	GUI for UC pilot	SYN	Confidential Open Source
IPR-28	F2F GUI extension for UC pilot	CAPGEMINI	Confidential Open Source

7.3 Key Results and Innovations

The exploitable results and their leaders guiding the R&D in the project are as follows:

Table 15 - FISHY ERs log

ID	Name	Lead	Task
ER-1	Enhanced capabilities for ATOS XL-SIEM	ATOS	3.2
ER-2	Extended Continuous Risk Assessment Engine	ATOS	3.2
ER-3	Standardised API for network infrastructure abstraction	TID	5.2
ER-4	Centrally Controlled IPsec (CCIPS)	TID	5.2
ER-5	Security Assurance & Certification Management Platform	STS	4.2
ER-6	Detection and protection components	XLAB	3.2
ER-7	Vulnerability Assessment	XLAB	3.2
ER-8	~~Extensions to xOpera~~	~~XLAB~~	~~4.1~~
ER-9	ILT-part of smart contract components	OPT	3.3
ER-10	Smart contract components (blockchain functionality of FISHY platform)	SYN	3.3
ER-11	Trustworthy identification and authentication of edge systems	UPC	3.3
ER-12	Advanced Mitigation strategy - PMEM	UPC	3.2
ER-13	Intent-based resilience orchestrator (IRO)	TUBS	5.1
ER-14	Integrity Assessment Toolkit (Trust Monitor)	POLITO	3.2
ER-15	Framework for InfSec evaluation within IoT	UMinho	5.2
ER-16	Connected & Autonomous Car Use Case	Altran	6.2
ER-17	Prototype of FISHY platform ready for validation in a real context	UPC	6.2

7.4 Key Exploitable Results

The Key Exploitable Results, extensively described in the section 4.3 are as follows:

Table 16 - FISHY KERs log

ID	Name	Acronym	Lead
KER-1	Dashboard & Platform	FISHY Platform	UPC
KER-2	Vulnerability Forecast & Risk Estimation	TIM	XLAB
KER-3	Intent-based Resilience Orchestration	IRO	TUBS
KER-4	Security Assurance and Certification Manager	SACM	STS
KER-5	Security & Privacy Dataspace Infrastructure	SPI	UMinho
KER-6	Enforcement & Dynamic Configuration	EDC	POLITO
KER-7	Secure Infrastructure Abstraction	SIA	TID