Deliverable D6.2

Communication and Dissemination Report - Initial

Editor	D. Bringhenti (POLITO)
Contributors	AIT, CNR, NASK, ONE
Version	1.0
Date	23rd February 2026
Distribution	PUBLIC (PU)
Classification	UNCLASSIFIED (U)

This project has received funding from the European Union's Horizon Europe Research and Innovation programme under grant agreement No. 101168144. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

Authors

POLITO	Politecnico di Torino
Daniele Bringhenti	
AIT	Austrian Institute of Technology
Max Landauer	
CNR	Consiglio Nazionale delle Ricerche
Matteo Repetto	
NASK	NAUKOWA I AKADEMICKA SIEC KOMPUTEROWA - PAŃSTWOWY INSTYTUT BADAWCZY
Joanna Kolodziej	
ONE	OneSource
Luis Cordeiro, Jorge Proença, Artur Dias, Luis Rosa, Miguel Domingues, Ricardo Martins, Wilson Ferreira	

Reviewers

DAEM	DIMOS ATHINAION EPICHEIRISI MICHANOGRAFISIS
Dimitra Tsakanika	
NASK	NAUKOWA I AKADEMICKA SIEC KOMPUTEROWA - PAŃSTWOWY INSTYTUT BADAWCZY
Joanna Kolodziej	

Copyright and Disclaimer

Funded by
The European Union

This document has been produced under the ECCC Grant Agreement 101168144. It is confidential and its content is the property of the companies listed on the cover page. Its content shall not be copied, disclosed, or used in whole or in part without the formal approval of the owning companies.

The MIRANDA project is funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The reader uses the information at his/her sole risk and liability.

Version History

Rev. N	Description	Author	Date
0.1	Initial template of the D6.2 document	Daniele Bringhenti (POLITO)	18.11.2025
0.2	First complete draft of the D6.2 document	Daniele Bringhenti (POLITO)	06.02.2026
0.3	First review of the D6.2 document	Joanna Kolodziej (NASK)	09.02.2026
0.4	Second review of the D6.2 document	Dimitra Tsakanika (DAEM)	12.02.2026
0.5	D6.2 update, based on the two reviews	Daniele Bringhenti (POLITO)	20.02.2026
1.0	Quality check	Matteo Repetto (CNR)	23.02.2026

List of Acronyms

Acronym	Meaning
CDT	Cybersecurity Digital Twin
DSC	Digital Service Chain
EU	European Union
HPC	High Performance Computing
ICT	Information and Communication Technology
I2DT	Industrial Internet Digital Twin
KPI	Key Performance Indicator
LLM	Large Language Model
OSINT	Open-Source Intelligence
R&I	Research & Innovation
SME	Small and Medium-sized Enterprise

Executive Summary

MIRANDA is a Horizon Europe project aiming to design, develop, and validate a framework for collaborative cybersecurity operations in digital service chains, based on the Cybersecurity Digital Twin (CDT) paradigm. Effective communication and dissemination are essential to ensure the visibility, impact, and long-term sustainability of the project's results across technical, industrial, policy, and societal stakeholders.

This deliverable D6.2 (Communication and Dissemination Report - Initial) reports on the communication and dissemination activities carried out during the first phase of the project (September 2024 - February 2026). It documents how the strategy, objectives, and actions defined in the Communication and Dissemination Plan (D6.1) have been implemented in practice during the initial project period.

In this early stage, communication activities focused on establishing the MIRANDA project identity and raising awareness of its vision, objectives, and relevance. The consortium engaged with a wide range of audiences through participation in public events, meetings, interviews, institutional websites, social media channels, and dedicated communication material. These efforts targeted citizens, service providers, municipalities, research communities, and industry stakeholders, fostering early interest and visibility. Dissemination activities were aligned with the project's results maturity and focused on scientific and professional outreach. The consortium contributed to international conferences, journals, and workshops, supported education and training activities, and initiated clustering and collaboration with other EU-funded projects. In addition, several software tools developed within MIRANDA were released as open source, reinforcing the project's commitment to open science and early community engagement.

The deliverable also provides an assessment of progress towards the Key Performance Indicators defined in D6.1. While several indicators already show tangible progress (particularly in terms of events attended, scientific dissemination, and open-source releases), other activities planned for later stages of the project, such as large-scale demonstrations, external training sessions, and platform-level dissemination, are scheduled for the next reporting periods.

Overall, the activities carried out in the first phase have successfully laid the foundations for effective communication and dissemination, established MIRANDA's presence within relevant stakeholder communities, and prepared the ground for more intensive, result-driven outreach in the second half of the project.

Table of Contents

List of Figures

List of Tables

1. INTRODUCTION

Communication and dissemination play a central role in maximising the impact of the MIRANDA project by ensuring that its vision, methods, and results reach relevant stakeholders in a timely, targeted, and effective manner. In line with this objective, the MIRANDA consortium defined a comprehensive strategy and plan in Deliverable D6.1 (Communication and Dissemination Plan), covering the entire project duration.

This deliverable D6.2 (Communication and Dissemination Report - Initial) provides an overview of the communication and dissemination activities carried out during the first reporting period of the project, from September 2024 to February 2026. It is produced within the scope of Task 6.1 “Communication and Stakeholders’ Engagement” and Task 6.2 “Dissemination, Clustering & EU-Wide Activities”, as defined in the Grant Agreement.

While D6.1 focused on defining objectives, target audiences, key messages, tools, timelines, and KPIs, this report documents the status of their implementation. It describes the activities undertaken, the audiences addressed, the channels and materials used, and the extent to which planned targets have been achieved. Where relevant, deviations from the original plan are highlighted and justified based on project progress and result maturity. The communication activities covered in this report aim to increase awareness and visibility of MIRANDA among a broad audience, including citizens, service providers, security operators, technology providers, researchers, and public authorities. Dissemination activities focus on the structured diffusion of scientific, technical, and methodological results through publications, conferences, workshops, open-source software, education, and clustering actions, consistent with the project’s open science principles.

This document is structured as follows.

Section 2 reports on communication activities, including their timing, participation in events and meetings, and use of communication channels and materials.

Section 3 presents dissemination activities carried out during the reporting period, covering publications, conference participation, workshops, open-source software and data, education and training, and clustering initiatives.

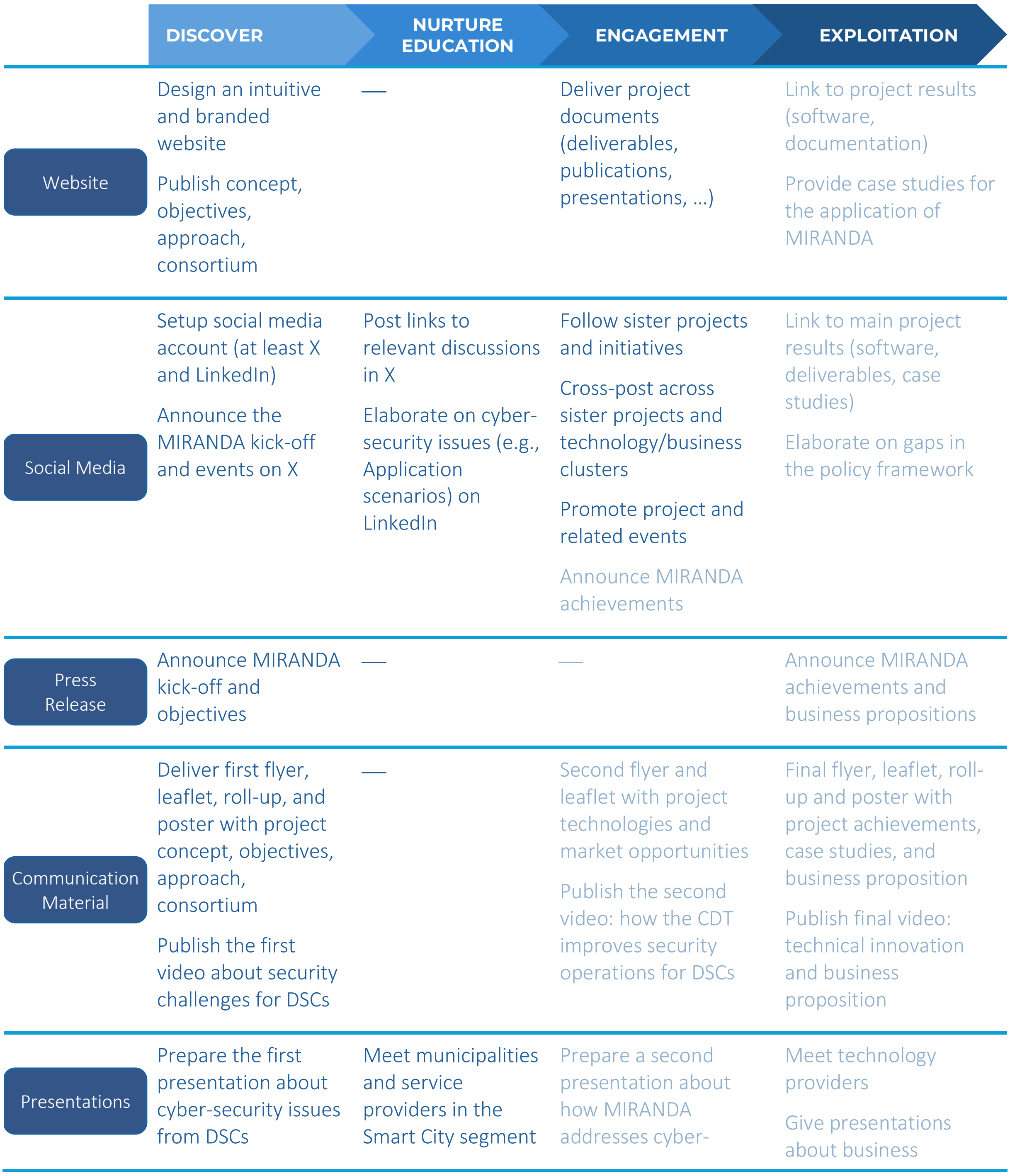
Section 4 discusses the current progress towards project impact and KPIs assessment.

Finally, Section 5 outlines updates and refinements to the Communication and Dissemination Plans based on the experience gained during this initial phase of the project.

2. Communication

2.1 Timing of activities

The Communication plan elaborated in D6.1 identifies 4 main stages roughly corresponding to the project's incremental maturity, with specific activities for 7 target groups, as shown in Figure 1. The project is currently in the middle of the "engagement" phase.



	DISCOVER	NURTURE EDUCATION	ENGAGEMENT	EXPLOITATION
Website	Design an intuitive and branded website Publish concept, objectives, approach, consortium	—	Deliver project documents (deliverables, publications, presentations, ...)	Link to project results (software, documentation) Provide case studies for the application of MIRANDA
Social Media	Setup social media account (at least X and LinkedIn) Announce the MIRANDA kick-off and events on X	Post links to relevant discussions in X Elaborate on cyber-security issues (e.g., Application scenarios) on LinkedIn	Follow sister projects and initiatives Cross-post across sister projects and technology/business clusters Promote project and related events Announce MIRANDA achievements	Link to main project results (software, deliverables, case studies) Elaborate on gaps in the policy framework
Press Release	Announce MIRANDA kick-off and objectives	—	—	Announce MIRANDA achievements and business propositions
Communication Material	Deliver first flyer, leaflet, roll-up, and poster with project concept, objectives, approach, consortium Publish the first video about security challenges for DSCs	—	Second flyer and leaflet with project technologies and market opportunities Publish the second video: how the CDT improves security operations for DSCs	Final flyer, leaflet, roll-up and poster with project achievements, case studies, and business proposition Publish final video: technical innovation and business proposition
Presentations	Prepare the first presentation about cyber-security issues from DSCs	Meet municipalities and service providers in the Smart City segment	Prepare a second presentation about how MIRANDA addresses cyber-	Meet technology providers Give presentations about business

			security issues for DSCs with the CDT	propositions and market opportunities
Meetings	Distribute flyers and leaflets Present the project concept and scope Meet service providers and municipalities	—	Distribute flyers and leaflets Present business proposition and innovation over competitors Meet technology providers	Distribute flyers and leaflets Present Use Cases and case studies Present business proposition and innovation over competitors
Education & Training		Organize cyber-security laboratories for young students		

Figure 1. Communication channels and key activities. Activities already implemented are highlighted.

These activities are scheduled according to a loose sequential logic, and therefore they largely overlap during the whole programme. They will have a **higher intensity in the first year and in the last six months**, when the main concept and approach, and the technical innovation and business proposition will be communicated, respectively.

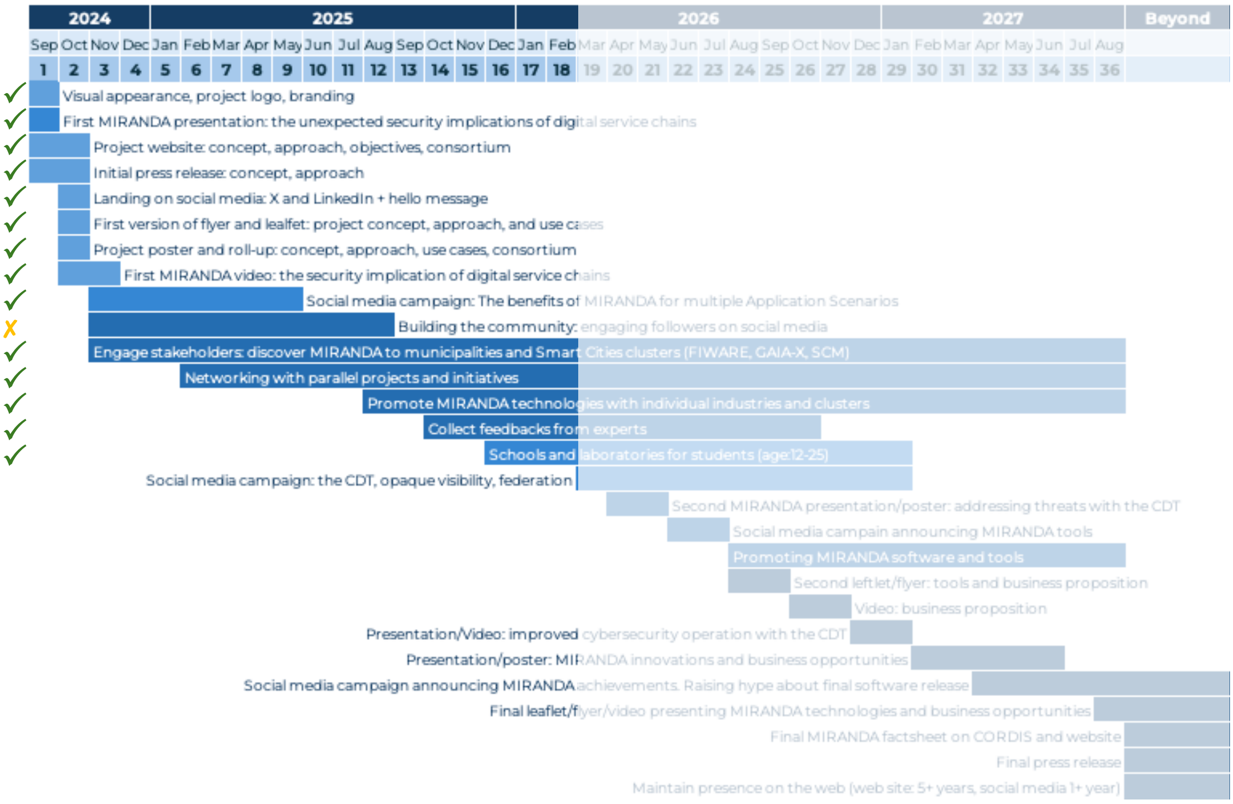


Figure 2. Timing of the Communication actions, first period highlighted.

During the **intermediary period**, the effort will shift towards stakeholder engagement, community building, and education aligned with the project vision. Social media content will be distributed throughout the period, paying attention to not leaving gaps and **continuously stimulating the community with news about the project's progress and related initiatives**. The Gantt chart of the planned activities is again reported in Figure 2, where the first period under consideration is highlighted.

In the following a brief overview of the Communication activities implemented in the first 18 months is given, organized according to the different channels.

2.2 Website

The project website has been published online in the very early stage of the project (by the end of the first month), and represents the landing page to easily reach all project resources and media:

- project concept, description, Consortium, and main contacts;
- social media: LinkedIn, X, YouTube;
- public deliverables;
- project presentations;
- communication materials: flyers, leaflet, posters, videos;
- sister projects.

The website was designed to be easily readable both on mobile devices and desktops; its layout allows to easily reach all sections without getting lost. A more detailed description of its look and appearance is already given in Sec. 2.7.5 of D6.1.

Table 1 Activities related to the website

Phase	Activity	Status	Notes
Discover	Design an intuitive and branded website Publish concept, objectives, approach, consortium	Delivered (M1)	Website structure and layout described in Sec. 2.7.5 of D6.1. Project website available at: https://www.mirandaproject.eu/.
Nurture Education	–	–	–
Engagement	Deliver project documents (deliverables, publications, presentations, …)	Ongoing (M1-M18)	Public deliverables available under "Resources -> Deliverables": https://www.mirandaproject.eu/deliverables/. Presentations at conferences and events available under "Media -> Presentations": https://www.mirandaproject.eu/presentations/.

Exploitation	Link to project results (software, documentation) Provide case studies for the application of MIRANDA	Planned	M32-M36

2.3 Social media

LinkedIn, X, and YouTube accounts have been created, as described in Sec. 2.7.6 of D6.1. During the past months, LinkedIn has turned out to be the most effective way to keep in touch with followers, so this will be the preferred media in the next period.

Table 2 Activities related to social media

Phase	Activity	Status	Notes
Discover	Setup social media account (at least X and LinkedIn) Announce the MIRANDA kick-off and events on X	Delivered (M1)	Social accounts described in Sec. 2.7.6 of D6.1. Kick-off announcement: https://x.com/mirandaprj/status/1836403064086909338.
Nurture Education	Post links to relevant discussions in X Elaborate on cyber-security issues (e.g., Application scenarios) on LinkedIn	M1-M18	45 posts on LinkedIn/Twitter; 3 articles delivered on LinkedIn: - Security implications behind interconnectedness - To twin or not to twin in cybersecurity? - Improving cyber-security operations with a Cyber-security Digital Twin
Engagement	Follow sister projects and initiatives Cross-post across sister projects and technology/business clusters Promote project and related events Announce MIRANDA achievements	Ongoing (M1-M18)	Following and cross-posting ECSSI cluster, INTACT, CASTOR, ENCRYPT, TRUSTEE. Posts on social media about project events and initiatives (SecSoft).

Exploitation	Link to main project results (software, deliverables, case studies) Elaborate on gaps in the policy framework	Planned	M32-M36

2.4 Press releases

An initial press release was delivered by the coordinator and some partners to announce the project kick-off. As additional outreach to the general audience, the Project Coordinator in Italy released an interview to a local broadcaster and published it on the YouTube channel with English subtitles (see Sec. 2.5).

Table 3 Activities related to press releases

Phase	Activity	Status	Notes
Discover	Announce MIRANDA kick-off and objectives	Delivered (M1-M2)	Press release from: - CNR - MIND - AIT - LOG
Nurture Education	–	–	–
Engagement	–	–	–
Exploitation	Announce MIRANDA achievements and business propositions	TBD	After M36

2.5 Communication material

The first release of the communication material (flyer, leaflet, poster, roll-up) was prepared and shared in the first months of the project, as described in Sec. 2.7.2-2.7.4 of D6.1. Additionally, a series of videos has been published on YouTube from other communication activities (presentations, interviews).

Table 4 Activities related to communication material

Phase	Activity	Status	Notes
Discover	Deliver first flyer, leaflet, roll-up, and poster with	Delivered (M1-M3)	Promo material: - Leaflet v1 - Flyer v1

	project concept, objectives, approach, consortium Publish the first video about security challenges for DSCs		- Poster v1 - Roll-up v1 Videos: - MIRANDA Promo video -
Nurture Education	–	Delivered (M5-M6)	Videos: - Interview to Primocanale - Presentation at AI Conference
Engagement	Second flyer and leaflet with project technologies and market opportunities Publish the second video: how the CDT improves security operations for DSCs	Planned	M24-M25 M28-M29
Exploitation	Announce MIRANDA achievements and business propositions	Planned	M30-M35

2.6 Presentations

The MIRANDA concept and objectives were presented by partners at several dissemination and communication opportunities. Below a short summary of the events attended:

2.6.1. 10th FIWARE Global Summit

Location: Naples, Italy

Date: 18th-19th September 2024

Partner: CNR:

Attendees: ~30

Presentation: Have you ever cared about the implications of digital interconnectedness?

The Project Coordinator was also invited as panellist at the round table: "Bringing new vision into the FIWARE world" where the impact of MIRANDA technologies was discussed.

2.6.2. 12th FOKUS FUSECO Forum

Location: Berlin, Germany

Date: 7th-8th November 2024

Partner: ONE:

Attendees: 30

Presentation: [6G Computing Continuum New Security and Trustworthy Challenges]

2.6.3. BSides Vienna

Location: Vienna, Austria

Date: 23rd November 2024

Partner: AIT:

Attendees: 150

Presentation: Rollup and leaflet.

2.6.4. AI Conference 2025

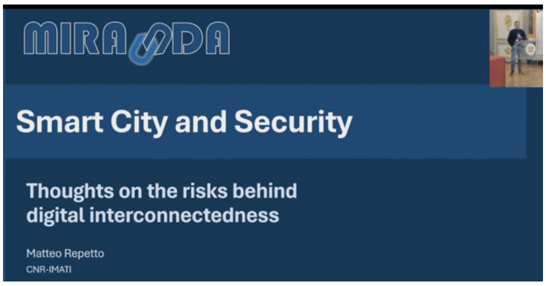
Location: Genoa, Italy

Date: 17th March 2025

Partner: CNR:

Attendees: ~50

Presentation: Smart City and Security – Thoughts on the risks behind digital interconnectedness



MIRANDA

Smart City and Security

Thoughts on the risks behind digital interconnectedness

Matteo Repetto
CNR-IMATI

2.6.5. CCGRID 2025

Location: Tromso, Norway

Date: 20th May 2025

Partner: NASK

Attendees: 40

Presentation: Flyers

2.6.6. 11th FIWARE Global Summit

Location: Rabat, Morocco

Date: 23rd May 2025

Partner: CNR

Attendees: 50

Presentation: [Secure Smart City – Cyber-security Digital Twins for Security Smart Cities]

2.6.7. 2025 CyberHOT Week

Location: Chania, Greece

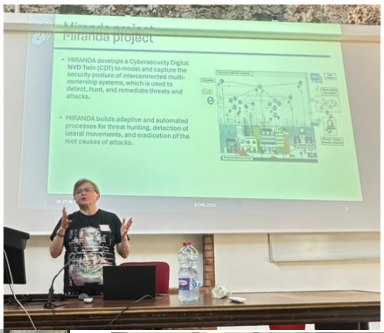
Date: 27th May 2025

Partner: ONE

Attendees: 20

Presentation: MIRANDA – Project Overview: Securing Interconnected Digital Services

2.6.8. ECMS2025-39th European Conference on Modelling and Simulation



Location: Catania, Italy

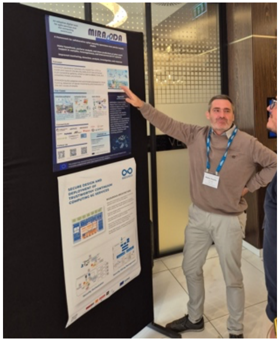
Date: 24th-28th June, 2025

Partner: NASK

Attendees: 40

Joanna Kolodziej chaired the SecMoS session and invited potential stakeholders attending the conference.

2.6.9. SecSoft 2025 (@NetSoft 2025)



Location: Budapest, Hungary

Date: 27th June 2025

Partner: CNR, POLITO

Attendees: 30

Presentation: MIRANDA poster

2.6.10. NeSecOr 2025 (@CNSM 2025)

Location: Bologna, Italy

Date: 31st October 2025

Partner: POLITO

Attendees: 25

Presentation: Project Overview

Table 5 Activities related to presentations

Phase	Activity	Status	Notes
Discover	Prepare the first presentation about cyber-security issues from DSCs	Delivered (M3)	Presentation used in different forms at the events listed above.
Nurture Education	Meet municipalities and service providers in the Smart City segment	Delivered (M1-M9)	Municipalities and potential end users present at the following events: - 10th FIWARE Summit - AI Conference - 11th FIWARE Summit
Engagement	Prepare a second presentation about how MIRANDA addresses cyber-security issues for DSCs with the CDT	Planned	M20-M21
Exploitation	Meet technology providers Give presentations about business propositions and market opportunities	Planned	M19-36

2.7 Meetings

MIRANDA attended large events and organized meetings with potential collaborators in the domain of Digital Twins and Cybersecurity operations, as listed below:

2.7.1. I2DT project

Location: Lisbon, Portugal + Remote attendees

Date: 5th May 2025

Partner: CNR, NASK

Attendees: 2

The meeting was organized to exchange vision, concept, and objectives in view of future collaboration and clustering between the projects.

2.7.2. University of Luxembourg

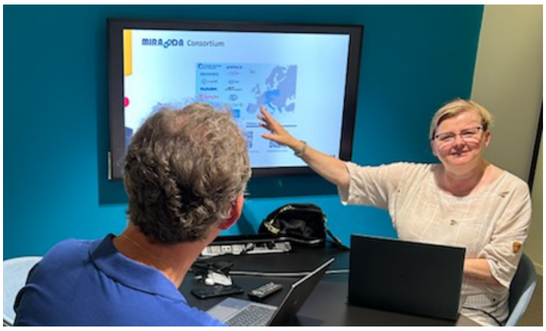
Location: Luxembourg, Luxembourg

Date: 2nd July 2025

Partner: NASK

Attendees: 40

Joanna Kołodziej was invited for a research visit to the University of Luxembourg on 1st-3rd July 2025. MIRANDA was presented during several bilateral meetings for the staff and leaders of the Cybersecurity and HPC groups.



2.7.3. Smart City Expo World Congress

Location: Barcelona, Spain

Date: 4th-6th November 2025

Partner: CNR

Attendees: ~27,000[1]

Presentation: [MIRANDA Promo video]

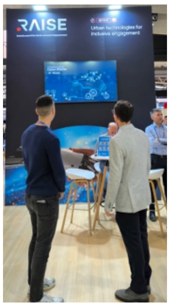


Table 6 Activities related to meetings

Phase	Activity	Status	Notes
Discover	Distribute flyers and leaflets Present the project concept and scope	Delivered (M1)	Met Smart Cities at: - 10th FIWARE Summit (see Section 2.6.1)

[1] https://www.firabarcelona.com/en/press-release/smartcityexpo_s078-en/smart-city-expo-closes-a-record-edition-calling-for-cities-to-lead-global-transformation/

	Meet service providers and municipalities		
Nurture Education	–	–	
Engagement	Distribute flyers and leaflets Present business proposition and innovation over competitors Meet technology providers	Ongoing (M9-M18)	Attendance of big exhibitions for Smart Cities: - 11th FIWARE Summit (see Section 2.6.6) - Smart City Expo World Congress
Exploitation	Distribute flyers and leaflets Present Use Cases and case studies Present business proposition and innovation over competitors	Planned	M19-36

2.8 Education and training

MIRANDA contributed to some educational events about cybersecurity topics for both young and PhD students. The project topics were briefly discussed at each event.

2.8.1. Le STEM @Area CNR – School meets research

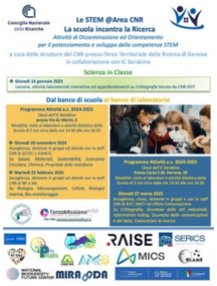
Location: Genoa, Italy

Date: 16th, 27th March 2025

Partner: CNR

Attendees: 30

Description: Presentation of research activities on cybersecurity to school students, with a focus on cryptographic principles and the need for securing data and communication.



Consiglio Nazionale delle Ricerche

Le STEM @Area CNR
La scuola incontra la Ricerca
Attività di Disseminazione ed Orientamento
per il potenziamento e sviluppo delle competenze STEM
a cura delle strutture del CNR presso l'Area Territoriale della Ricerca di Genova
in collaborazione con IC Barabino

Scienza in Classe

Giovedì 16 gennaio 2025
Lezione, attività laboratoriali interattive ed approfondimenti su *Crittografia* tenuta da CNR IEIIT

Dal banco di scuola al banco di laboratorio

Programma Attività a.s. 2024-2025
Classi dell'IC Barabino
presso Via de Marini, 6
Modalità: visita ai laboratori e attività didattica della durata di 2 ore circa dalle ore 14:30 alle ore 16:30

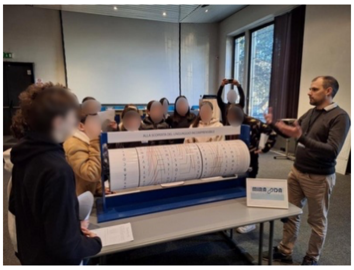
Giovedì 28 novembre 2024
Accoglienza, divisione in gruppi ed attività con lo staff CNR di SCITEC e ICMATE.
Su Salute, Materiali, Sostenibilità, Economia Circolare, Chimica, Proprietà delle interfacce

Martedì 25 febbraio 2025
Accoglienza, divisione in gruppi ed attività con lo staff CNR di IBF e IAS.
Su Biologia, Microrganismi, Cellule, Biologia marina, Bio-monitoraggio

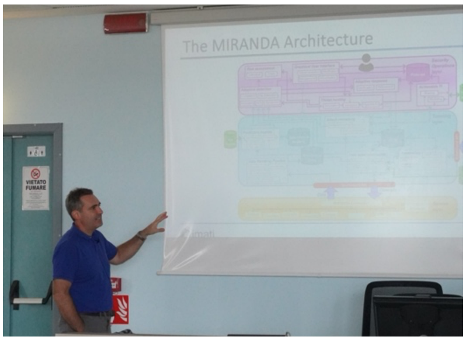
Programma Attività a.s. 2024-2025
Classi dell'IC Barabino
Presso Corso F.M. Perrone, 24
Modalità: visita ai laboratori e attività didattica della durata di 2 ore circa dalle ore 14:30 alle ore 16:30

Giovedì 27 marzo 2025
Accoglienza, check, divisione in gruppi e con lo staff CNR di IEIIT, IMATI ed Ufficio Comunicazione.
Su Crittografia, Sicurezza delle reti industriali, Information hiding, Sicurezza delle comunicazioni e del dato, Comunicare la ricerca

TerzaMissione
Per info [illegible]



2.8.2. PhD Summer School



Location: Turin, Italy

Date: 17th September 2025

Partner: CNR, POLITO

Attendees: 25

Presentation: [Industrial IoT security: approaches and challenges]

The contribution includes 1) a seminar on the security of IoT devices interconnected to cloud services and 2) an interactive lab about the generation of network-based attacks with Ettercap.

Table 7 Activities related to education and training

Phase	Activity	Status	Notes
Discover	–	–	
Nurture Education	Organize cyber-security laboratories for young students	On-going (M12-M18)	Le STEM interactive lab for your students. Interactive lab at the PhD Summer School.
Engagement	–	–	
Exploitation	–	–	

3. Dissemination

3.1 Timing of activities

In the first 18 months of the project, the consortium carried out dissemination activities suited to the project's early results and ongoing work. Several conference and journal papers were published, and the partners organized a workshop at an international conference. The consortium also took part in various research events to present the project's goals and discuss initial findings.

Education and training activities were supported through ongoing supervision of Master's and PhD theses, as well as the involvement of students in project-related research. Partners additionally contributed to summer schools and science classes on cybersecurity, helping to introduce the project's topics to younger audiences.

The consortium continued its collaboration with other EU-funded projects through clustering activities. This included joining relevant project communities, participating in online meetings, and taking part in joint workshops to exchange experiences and identify shared interests.

Overall, the schedule of dissemination activities proposed in D6.1 remains intact. The only deviation concerns the training activities planned for external stakeholders, which have been postponed until a public version of the MIRANDA platform becomes available. Likewise, webinars, software releases, and demonstrations, which are foreseen as active dissemination measures for the second half of the project, have not started yet but are already being prepared.

These efforts provided visibility for the project, encouraged collaboration, and set the stage for broader dissemination once more mature technical results are released.

3.2 Overview of activities

3.2.1. Publications

During the first reporting period, three peer-reviewed journal papers and five conference papers have been published in high-quality international venues, addressing key topics aligned with the project's scientific and technical objectives. These publications cover complementary aspects of cybersecurity research, including advanced threat detection techniques, frameworks for the control and orchestration of security functions, and the conceptual foundations and challenges of Cybersecurity Digital Twins for multi-ownership digital service chains. A special issue was also organized.

3.2.1.1. Open-Access Journal Publications

- Landauer, M., Alton, L., Lindorfer, M., Skopik, F., Wurzenberger, M., & Hotwagner, W. (2025). Trace of the Times: Rootkit Detection through Temporal Anomalies in Kernel Activity. Digital Threats: Research and Practice, 6(4), 1-26. doi: 10.1145/3770085

- Repetto, M. (2025). Otupy: A flexible, portable, and extensible framework for remote control of security functions. *Computers & Security*, 104597. doi: 10.1016/j.cose.2025.104597
- Repetto, M. (2026). Cybersecurity Digital Twins: Concept, blueprint, and challenges for multi-ownership digital service chains. *Journal of Information Security and Applications*, *96*, 104299. doi: 10.1016/j.jisa.2025.104299

3.2.1.2. Open-Access Conference Publications

- Kowalczyk M., Seweryn K., Kolodziej J., & Krzyszton M. (2025). Adversarial Robustness Of Multimodal Machine Learning Models. ECMS 2025 (pp. 248-254). doi: 10.7148/2025-0248
- Krzton K., Kolodziej J., Widlak A., Nawrocki M., & Sigut J. F. (2025). Vulnerabilities Of Machine Learning Algorithms To Adversarial Attacks In Medical Images. ECMS 2025 (pp. 255-261). doi: 10.7148/2025-0255

3.2.1.3. Non-Open-Access Conference Publications

- Tanzarella, S., & Repetto, M. (2025). Context Discovery for Digital Service Chain with OpenC2. In 2025 IEEE 11th International Conference on Network Softwarization (NetSoft) (pp. 579-584). doi: 10.1109/NetSoft64993.2025.11080629
- Tomas, P. R., Silva, S., Neto, M., Proença, J., Rosa, L., Cordeiro, L., Taleb T., & Cruz, T. (2025). Network Policy Enforcement in Cloud-Native Environments. In IFIP International Conference on Artificial Intelligence Applications and Innovations (pp. 195-208). doi: 10.1007/978-3-031-97317-8_15
- Canavese, D., Ferreira, A., Laborde, R., & Kandi, M. A. (2025). Towards an architecture for managing security under the EU Cyber Resilience Act. In International Workshop on Security and Trust Management (pp. 159-172). doi: 978-3-032-06155-3_9

3.2.1.4. Special Issue - ACIG journal

The main aim of this special issue was to publish the results of the state-of-the-art analysis, an early-stage and background research for the MIRANDA project.

The title of this special issue is “Cybersecurity in Digital Service Systems“.

The target journal is an open access “Applied Cybersecurity & Internet Governance (ACIG)” journal (https://www.acigjournal.com/).

This special issue encompasses theoretical work and practical approaches that advance research in all aspects of securing interconnected digital services in IT systems and infrastructures. Successful contributions may range from advanced technologies, applications, and innovative solutions for modelling, simulation, and predicting cyber threats in complex systems, to modern cryptographic methods, as well as the development of methods, conceptual and theoretical models, and simulations related to the secure operation of digital supply chains and services in IT systems.

The publication topics include (but are not limited to) the following:

- Modelling and simulation of cyber-threats in complex systems
- Prediction and detection of attack kill chains
- Advanced ML and AI techniques for detecting cyberattacks
- Models and protocols for security-related data collection, processing, and delivery
- Automated response and mitigation of cyberattacks
- Modern cryptographic methods
- Modern physical/cyber Digital Twins for simulation and prediction
- Secure and privacy-aware visibility over multi-ownership systems
- Secure and effective creation, sharing, and consumption of Threat Intelligence
- Federated Learning and Transfer Learning over multi-ownership and complex systems
- Coordinated and federated cybersecurity operations in complex systems
- Scalable identity and authentication protocols for sharing data and controls in federated environments
- Cyber-threat challenges for large digital service chains, including Smart City, Smart Grid, critical infrastructures, and supply chains
- Secure communication in Smart Grid installations using Mobile Ad Hoc Network protocols
- Privacy architectures and models for interconnected systems
- Secure attestation of digital resources across providers in complex systems
- Trust management and risk assessment across digital service chains

The final submission deadline for the papers was February 15, 2026, and the special issue is expected to be published in Fall 2026. We plan to accept at most 6-8 papers after a meticulous, double-blind review process. The guest editors of the special issue are Joanna Kolodziej from NASK and Matteo Repetto from CNR.

3.2.2. Participations, Forums, and Events

Throughout the reporting period, project partners participated in several scientific conferences and community events to present early research results and engage with relevant stakeholder groups. These participations supported the project's aim of sharing findings with the scientific community, industry representatives, and specific end-user groups, while also strengthening collaboration with peers working on related topics. The events covered a range of themes, including adversarial machine learning, cybersecurity, cloud-native environments, and regulatory developments, reflecting the interdisciplinary nature of the project's work. Table 8 summarizes the key participations, including the papers presented, locations, involved partners, and corresponding target audiences. These activities increased the project's visibility, facilitated knowledge with specialized communities, and establishing connections that will support future dissemination and collaboration efforts.

Table 8 Conference Participations

Name	Description	Location	Date	Partner	Target audience	Att.
ECMS 2025	Presentation of the paper: M. Kowalczyk et al.: Adversarial robustness of	Catania, Italy	6/24/2025	NASK	Industry, business partners; Research	40

	multimodal machine learning models				communities; Specific end user communities	
ECMS 2025	Presentation of the paper: Krzton, at al: Vulnerabilities of machine learning algorithms to adversarial attacks in medical images,	Catania, Italy	6/24/2025	NASK	Industry, business partners; Research communities; Specific end user communities	40
SecSoft 2025	Presentation of the paper: Tanzarella et al: Context Discovery for Digital Service Chain with OpenC2	Budapest, Hungary	27/06/2025	CNR	Research communities	30
AIAI 2025	Presentation of the paper: Tomas, P. et al. (2025). Network Policy Enforcement in Cloud-Native Environments. In IFIP International Conference on Artificial Intelligence Applications and Innovations	Limassol, Cyprus	29/06/2025	ONE	Research communities; Other; Industry, business partners	40
STM 2025	Presentation of the paper: Canavese et al.: Towards an architecture for managing security under the EU Cyber Resilience Act.	Toulouse, France	22/09/2026 - 26/09/2026	CNR	Research communities	30
IKT Sicherheitskonferenz	Student poster presentation about log analytics	Dornbirn, Austria	25/06/2025	AIT	Industry, business partners; Innovators; EU Institutions; National authorities	20

3.2.3. Joint Workshops

The MIRANDA consortium has actively contributed to the co-organisation of the 7th International Workshop on Cyber-Security in Software-defined and Virtualized Infrastructures (SecSoft), held on 27 June 2025 in Budapest, Hungary, co-located with the 11th IEEE International Conference on Network Softwarization (NetSoft 2025). SecSoft brought together researchers and practitioners from multiple EU-funded projects to address emerging challenges in the security, safety, trust, and privacy of softwarized and virtualised digital infrastructures. The workshop served as a platform for constructive discussion on situational awareness, advanced threat detection, and secure digital service frameworks, fostering crossproject collaboration and visibility of MIRANDA's research themes in the broader cybersecurity community.

Table 9 Joint workshops

Name	Description	Location	Date	Partner(s)	Target audience	Att.
SecSoft 2025	POLITO and CNR co-organized SecSoft 2025, a joint workshop of 9 cybersecurity projects including MIRANDA, featuring 12 papers, a keynote by Prof. Boutaba, a poster session, and 25–30 attendees.	Budapest, Hungary	27/06/2025	POLITO, CNR	Research communities	30

3.2.4. Open-source Software and Open Data

The MIRANDA consortium continues to follow its open-science strategy by making software components publicly available whenever possible and preparing the groundwork for the release of larger platform elements and datasets. In this reporting period, several standalone tools developed by partners have already been published as open-source software. These components support topics such as log analysis, threat intelligence, alert interpretation, and adversarial behaviour modelling and serve both as practical utilities and as reference implementations for research. A brief overview of the released tools is given in Table 10.

Table 10 Open-Source Tools

Name	Description
AttackMate	AttackMate is a framework for generating, managing, and orchestrating cyber-attack scenarios in controlled environments. It supports reproducible attack executions for evaluation, experimentation, and benchmarking of detection systems and provides modular components for defining attack steps, conditions, and triggers. URL: https://github.com/ait-testbed/attackmate
DetectMate	DetectMate is a modular environment for evaluating intrusion-detection and anomaly-detection approaches. It enables structured experiments, supports automated evaluation workflows, and offers reusable components for applying detection models, analysing results, and comparing different strategies. URL: https://github.com/ait-detectmate
LLM Log Parsing	This repository provides Large Language Model–based techniques for transforming raw log messages into structured representations. The approach aims to improve log understanding and reduce preprocessing overhead by leveraging modern language models for pattern extraction and normalization.

	URL: https://github.com/ait-aecid/LLM-log-parsing
OSINT Analysis (Taranis-AI)	An open-source tool for collecting, aggregating, and analysing open-source intelligence (OSINT) data. It supports structured threat intelligence workflows, integrates multiple information sources, and helps analysts identify relevant cybersecurity signals in large volumes of publicly available data. URL: https://github.com/taranis-ai/taranis-ai
Alert Analysis with LLMs	A tool that applies LLM-based methods to interpret alerts generated by security monitoring systems. It provides explanations, summarisation, and contextualisation of alerts to support analysts in prioritisation and triage tasks. URL: https://github.com/ait-aecid/llm-alert-interpretation
VEREFOO	VEREFOO (VErified REFinement and Optimized Orchestrator) is a framework designed to automatically allocate and configure packet filtering firewalls in a service graph defined by the network administrator, so as to fulfill the user-specified security connectivity requirements. VEREFOO combines automation, formal verification and optimization by formulating the firewall configuration problem with constraint programming, as a Maximum Satisfiability Modulo Theories (MaxSMT) problem. URL: https://github.com/netgroup-polito/verefoo
otupy	otupy (OpenC2 Tooling in Python) is an open-source Python framework that implements the OpenC2 architecture and language, enabling the definition, exchange, and execution of standardized cybersecurity command-and-control messages through a modular, extensible, and protocol-agnostic design. URL: https://github.com/mattereppe/otupy

In addition to these standalone tools, the consortium is preparing the open-source Community Edition of the MIRANDA platform, which will integrate selected components and provide a unified environment for experimentation and research. This release is planned for the beginning of the second half of the project and will follow the principles described in D6.1, including modular design, public availability, and documentation to support reproducibility and reuse.

Regarding open data, no datasets have been published yet, as data collection requires completed testbed setups and mature use-case scenarios. Work is currently underway to prepare these environments and define the data collection methodology. The consortium continues to follow the commitment outlined in the previous deliverable to release multiple datasets covering multi-step attack traces, accompanied by detailed documentation, metadata, and necessary anonymisation measures. These datasets will be published following FAIR principles and in alignment with the EU Data Strategy once collection and validation activities are completed.

3.2.5. Demos

Demonstrations are planned to begin once sufficient components of the platform and the related tools reach a level of maturity that allows for meaningful technical showcases. In line with the project plan, this activity is expected to start after M18. Preparations for demonstrations are already underway, including identifying suitable formats, defining demonstration scenarios, and planning recording and documentation procedures. Once available, demonstrations will provide stakeholders with hands-on insights into the MIRANDA platform, ranging from low-level data and analytics workflows to higher-level operational features. Recorded demonstrations will also be made available to support wider dissemination and long-term accessibility.

3.2.6. Education

During the reporting period, members of the consortium at POLITO and CNR have supervised and mentored six master's thesis students, who worked on MIRANDA research themes and technical work.

The supervised theses span core topics of MIRANDA's research agenda, from attack modelling and response strategies in complex digital infrastructures to practical implementations of cybersecurity standards and automated security workflows. Several theses investigated challenges associated with cyber-attack propagation and mitigation within digital service chains, providing analytical and methodological insights into threat detection in integrated service contexts. Others focused on advancing the use of OpenC2 as a standardized command and control language for cybersecurity automation, including the development of language profiles, design of secure authentication and authorization frameworks, and implementation of homogeneous control across diverse firewall environments, thus contributing directly to the state-of-the-art in interoperable security control mechanisms. Complementing these, work on software supply chain vulnerability modelling and automated network security workflows further extended the academic contribution to areas of strategic importance for the project.

3.2.7. Training and webinars

Training activities play an important role in the project's overall knowledge-transfer strategy, particularly for supporting security professionals who will ultimately work with the MIRANDA platform and its associated tools. In line with the dissemination plan, the consortium has focused during the first 18 months on preparing the foundations for effective training rather than conducting early sessions based on intermediate prototypes. The upcoming public Community Edition of the MIRANDA platform will provide a more stable and suitable basis for hands-on exercises, and training activities are planned to begin once this version becomes available. This approach ensures that future sessions will be practical, relevant, and aligned with the expectations of operational users. Preparatory work for training, including identifying suitable content, defining exercises, and outlining formats for interaction with end-user teams, is ongoing.

Webinars follow a similar planning logic. As remote formats designed for broader audiences, they will complement in-person training by combining presentations, demonstrations, and guided exercises. Since webinars rely on demonstrable platform functionality, the consortium intends to initiate them in the second half of the project, when the MIRANDA Community Edition can be featured as part of the learning material. Work is already underway to prepare the structure of future webinar sessions, possible Q&A formats, and mechanisms for collecting participant feedback to support continuous improvement.

3.2.8. Contributions to standards

Standardisation remains an important aspect of the project's long-term impact strategy, as well-defined interfaces and interoperable components are essential for encouraging wider adoption of MIRANDA technologies. During the first 18 months, the consortium focused on analysing relevant technical standards and identifying areas where MIRANDA's results can provide meaningful contributions. While no formal standardisation submissions have been made yet, preparatory work is already underway in selected areas.

In particular, partners are working on an OpenC2 extension, building on insights gained from early technical developments and from ongoing work on automated response and service-chain orchestration. This extension aims to improve the expressiveness and applicability of OpenC2 in scenarios related to dynamic security management and cyber-digital-twin environments. Once further developed and validated, this work is expected to form the basis for concrete contributions to the OpenC2 community and potentially to relevant standardisation groups.

As the project progresses and more mature results become available, the consortium will engage more directly with standardisation bodies identified in the dissemination plan. Contributions will focus on areas where MIRANDA technologies offer clear added value for interoperability, automation, and cybersecurity operations, ensuring that the project supports broader European and international efforts to harmonise practices and interfaces in the domain.

3.2.9. Clustering and EU-Wide Activities

Clustering with other EU-funded initiatives continues to be an important part of the project's strategy for increasing visibility, exchanging knowledge, and identifying opportunities for coordinated actions. During the first 18 months, the consortium engaged in several EU-wide activities and community events that brought MIRANDA into contact with a broad range of related research projects, industrial stakeholders, and institutional actors.

A key focus of this period was participation in the ECSCI (European Cluster for Securing Critical Infrastructures) community, which brings together more than 50 ongoing and completed EU projects on critical infrastructure security. MIRANDA partners were able to follow developments in the cluster, gain insights into emerging challenges, and position the project within this broader network.

Clustering activities also included collaboration with projects funded under the same call, where partners worked to identify shared interests and potential joint dissemination actions. Figure 3 shows a screenshot from an online meeting where common impact strategies were discussed with members of the INTACT, CyberNEMO, MEDIATE, and CASTOR projects. The consortium also engaged with related initiatives such as the Trustee and Encrypt projects, including interactions via social media channels that support ongoing visibility and informal knowledge exchange.

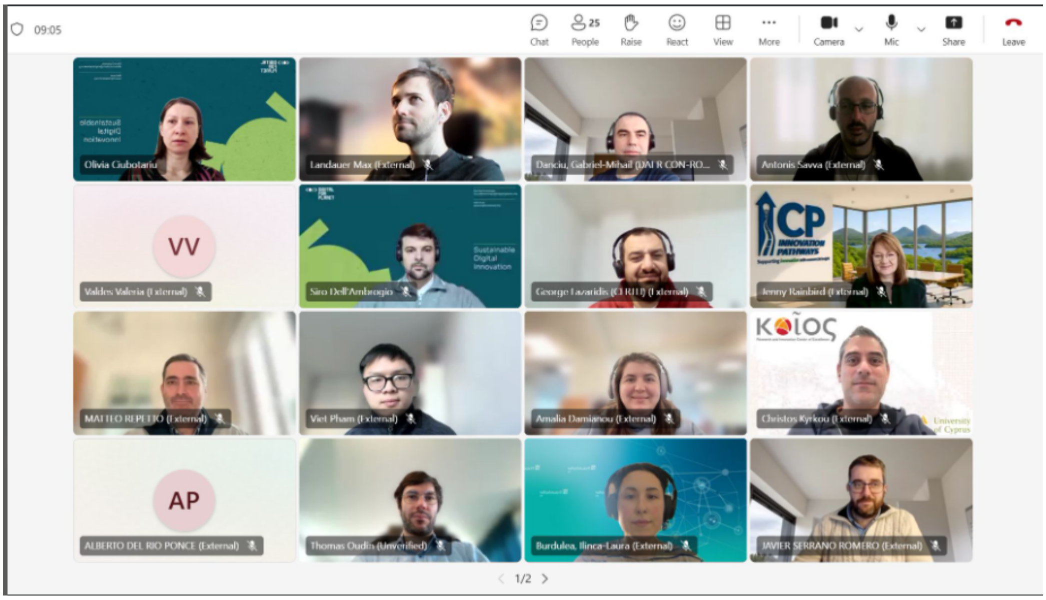

09:05
Chat
People
25
Raise
React
View
More
Camera
Mic
Share
Leave
Olivia Ciubotariu
Landauer Max (External)
Danciu, Gabriel-Mihail (JAI R CON-RO...
Antonis Savva (External)
VV
Valdes Valeria (External)
Siro Dell'Ambrogio
George Lazaridis (CERTH) (External)
Jenny Rainbird (External)
MATTEO REPETTO (External)
Viet Pham (External)
Amalia Damianou (External)
Christos Kyrkou (External)
AP
ALBERTO DEL RIO PONCE (External)
Thomas Oudin (Unverified)
Burdulea, Ilinca-Laura (External)
JAVIER SERRANO ROMERO (External)
1/2

Figure 3 Screenshot from online clustering meeting.

Beyond online coordination, partners also participated i in-person clustering opportunities. This included participation in the Eureka I2DT project meeting held on 5 May 2025 in Lisbon, enabling discussions with stakeholders addressing complementary research topics. Moreover, MIRANDA contributed to the joint EU projects workshop at SecSoft 2025, offering additional opportunities to exchange perspectives with projects focusing on network virtualization and cybersecurity.

Table 11 summarizes our main activities, which helped strengthen MIRANDA's connections within the European research ecosystem, facilitated mutual awareness among related initiatives, and laid the groundwork for deeper collaboration as more technical outputs become available in subsequent phases of the project.

Table 11 Clustering Activities

Name	Description	Location	Date	Partner(s)	Target audience	Att.
Security Research Event	Networking and clustering - similar projects/partners	Warsaw, Poland	25/06/2025	NASK	Innovators; Research communities	100
Cluster with EU projects funded under the same Call	Create synergies and find common communication/dissemination activities	Online	06/10/2025	SNR, SPH, AIT	Research communities; Innovators	20
Clustering with ECSCI community	Participation in the ECSCI cluster	Online	15/10/2025	CNR	Industry, business partners; Innovators; EU	20

					Institutions; National authorities	
TechWeek 2025	Workshop co-organized by OneSource and featured a Demo of the DeepGuardian tool in the scope of MIRANDA	Aveiro, Portugal	06/10/2025	ONE	Industry, business partners; National authorities; Regional authorities; Local authorities; Civil society; Research communities	20
Cluster with EU projects funded under the same Call	Joint effort and implement a common impact strategy	Online	16/01/2026	CNR, SPH, POLITO, AIT	Research communities; Innovators	20

4. Current Progress Toward Project Impact Assessment

During the first reporting period, MIRANDA has made solid, measurable progress towards its communication and dissemination Key Performance Indicators (KPIs), in line with the objectives and targets defined in the Communication and Dissemination Plan (D6.1). The consolidated view provided in this section reflects the complementary nature of communication and dissemination activities and their joint contribution to the overall project impact.

From a communication perspective, the project has successfully established a visible and consistent presence across its main channels. The project website, social media accounts, promotional materials, and participation in public events have ensured early awareness of MIRANDA’s vision, scope, and relevance among a broad range of stakeholders. Current trends indicate that all communication-related KPIs are progressing well and remain on track to meet within the planned timeframe. The number of public events attended, the communication materials produced, and people reached confirm the effectiveness of the adopted communication strategy in this early phase of the project.

From a dissemination perspective, at the current reporting stage, the achieved results are broadly in line with the expectations defined in the proposal and D6.1 for this point in the project lifecycle. No significant deviations have been identified that would indicate risks for meeting the planned dissemination objectives by the end of the project. It is worth noting that, even though the core technical development activities did not start at the very beginning of the project, dissemination through scientific publications is already well underway. Several papers have been published in high-quality journals and at international conferences, and several additional publications are currently in preparation or under review. This demonstrates the strong scientific engagement of the consortium and confirms that the project is well positioned to meet, and potentially exceed, the corresponding publication-related KPIs over the full project duration. Regarding clustering activities, workshops, and participation in relevant events, the project is also on track. The consortium has actively engaged in exchanges with related initiatives and networks, and further activities are planned for the upcoming reporting periods. These efforts contribute to increased visibility of the project and to knowledge exchange within the wider research and innovation community, in line with the project’s dissemination strategy.

At the same time, it is acknowledged that for certain KPIs, such as software and data publication or contributions to standardisation, no tangible results have been reported yet. As discussed in other sections of this deliverable, this situation is expected at the current stage of the project. These activities typically require more stable and mature technical results, which will become available in later phases. Nevertheless, preparatory work is already ongoing, and the consortium does not foresee any issues in addressing these KPIs as the project progresses.

Table 12 KPIs progress

Action		Target KPIs	Progress
Website	Web site visitors	≥ 5000	427*

	Number of views Average visit duration Downloads	– ≥ 3 min ≥ 200	1169* 3:23* N/A
Social media	Social media activity: - posts - followers - comments - unique visitors - views - impressions - reactions Promotional videos - no. of views - impressions - avg view duration	 ≥ 150 ≥ 200 ≥ 400 – – – – 3 ≥ 200 – –	(LinkedIn+X) 45+45 75+7 2+ 123**+N/A 288**+541 1798**+N/A 249**+N/A 3 182 (+94***) 741 1:11
Communication Activities	Number of MIRANDA presence in events Laboratories or seminars Number of reached people	≥ 12 3 ≥ 80	11 (10 presentations + 1 attendance) 3 (2 laboratories + 1 seminar) >660 (direct) ~ 30,000 (indirect)****
Communication Material	Promotional material (leaflets, white papers) No. copies or downloads	6 ≥ 500	4 N/A
Cumulative GitHub stars/forks		≥100/≥10	0/0*****
Scientific papers in intl. journals/conferences		≥8/≥12	3/5
Number of demos in events		≥6	0
Organization of joint workshops with EU projects/attendees		≥4/≥200	1/30
Webinars/Number of trained people		3/≥80	0/0
No. of trained students		≥6 BSc/MSc, ≥4 PhD	6/0******
Contributions to standards (profiles, extensions, algorithms, etc.)		≥6	0
Clustering events/attendees		-/-	5/100
Release data sets concerning multi-step attacks (logs, network traffic, configurations, documentation, etc.)		≥3	0

** Due to technical issues, data collection begins on April 14, 2025*

*** Figures related to last year only (Feb. 2025-Feb. 2026)*
**** Views of the original video from external YouTube channel (Primocanale)*
***** Figure includes estimated attendance of the Smart City expo from organizers (see note 1) and average audience of Primocanale broadcasting channel from public data.*[2]
****** The number of cumulative GitHub stars/forks is 0 because no GitHub project repository is yet available.*

******* Currently there are 4 PhD students who are actively working on the MIRANDA project. Their PhD program will finish by the end of the project, so they will be counted in the KPI computation in the next reporting period and will allow to reach the target successfully.*

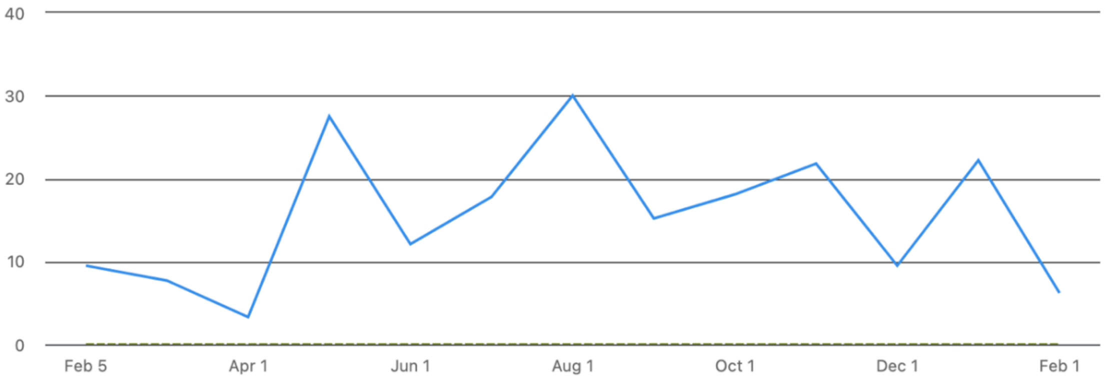


Figure 4 Engagement rate on LinkedIn in the last year

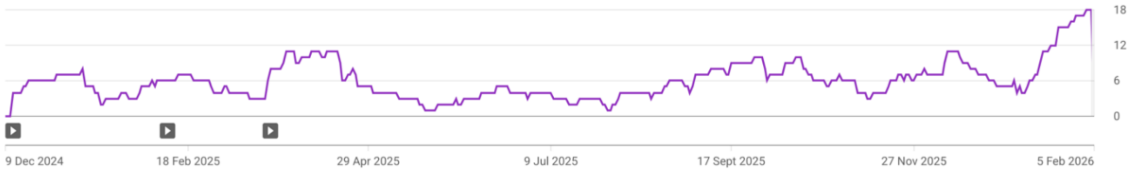


Figure 5 Audience on YouTube channel

[2] https://www.auditel.it/wp-content/uploads/2025/12/Regionale-Tv-Locali_2025.pdf

5. Updates to Communication and Dissemination Plans

5.1 Communication Plan

No major updates to the communication plan defined in Deliverable D6.1 are required at this stage of the project. The overall communication strategy, objectives, target audiences, and planned set of activities remain valid and appropriate for supporting the visibility and impact of the MIRANDA project.

Communication activities carried out during the first reporting period have been implemented as planned and are progressing on schedule. The established communication channels, including the project website, social media accounts, communication materials, and participation in public events, have proven effective in raising awareness of the project's vision, scope, and relevance among the identified stakeholder groups.

For the upcoming reporting period, the communication effort will continue to follow the strategy defined in D6.1, also trying to strengthen engagement on social media channels. This will be achieved through more frequent and targeted posts, and cross-promotion with sister projects and clusters.

5.2 Dissemination Plan

No major updates to the dissemination plan defined in D6.1 are required at this stage of the project. The overall strategy, objectives, and planned set of dissemination activities remain valid and appropriate for achieving the project's goals.

The only adjustment concerns the timing of certain dissemination actions, which depend on the availability of more tangible and mature technical results. Some activities targeting external stakeholders, such as training sessions, webinars, software releases, and live demonstrations, have been postponed to later phases of the project. This decision was made to ensure that these activities are based on stable, well-documented outcomes and can therefore deliver maximum impact and relevance for the intended audiences.

This postponement does not represent a reduction in scope or ambition of the dissemination plan, but rather a refinement of the schedule in line with the project's technical progress. Preparatory work for these activities is already ongoing, and the consortium remains confident that the planned dissemination measures will be implemented as foreseen once the corresponding results become available.

This project has received funding from the European Union's Horizon Europe Research and Innovation programme under grant agreement No. 101168144. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.