Deliverable D6.1

Communication and Dissemination Plan

Editor	J. KOLODZIEJ (NASK)
Contributors	NASK, CNR, AIT, ONE
Version	1.1
Date	March 28th, 2025
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

NASK	NAUKOWA I AKADEMICKA SIEC KOMPUTEROWA - PAŃSTWOWY INSTYTUT BADAWCZY
Joanna Kolodziej, Mateusz Krzysztoń	
AIT	Austrian Institute of Technology
Max Landauer, Markus Wurzenberger	
CNR	Consiglio Nazionale delle Ricerche
Matteo Repetto, Enrico Cambiaso	
ONE	OneSource
Jorge Proença, Luis Cordeiro	

Reviewers

LOG	LOGSTAIL
A. George Ziras, B. Ioannis Avdoulas	
DAEM	DIMOS ATHINAION EPICHEIRISI MICHANOGRAFISIS
A. Ilia Christantoni, B. Dimitra Tsakanika	

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 D6.1 document	Joanna Kolodziej (NASK)	1.10.2024
0.2	Revision of ToC	Max Landauer (AIT)	1.10.2024
0.3	Write several Sections of the Dissemination Chapter	Max Landauer (AIT)	9.10.2024
0.4	Write several Sections of the Dissemination Chapter	Max Landauer (AIT)	28.10.2024
0.5	Added the Communication plan	Matteo Repetto (CNR)	30.10.2024
0.6	Added Introduction	Joanna Kolodziej (NASK)	31.10.2024
0.7	Completed and revised ex. summary	Joanna Kolodziej (NASK)	6.11.2024
0.8	Addressed internal review comments	Max Landauer (AIT)	18.11.2024
0.9	Addressed internal review comments for Sec. 2	Matteo Repetto (CNR)	21.11.2024
1.0	Quality control	Matteo Repetto (CNR)	25.11.2024
1.1	Fixed errors in Fig. 4	Matteo Repetto (CNR)	28.03.2025

List of Acronyms

Acronym	Meaning
ACM	Association for Computing Machinery
C&D	Communication and Dissemination
CDT	Cybersecurity Digital Twin
DSC	Digital Service Chain
EC	European Commission
IEEE	Institute of Electrical and Electronics Engineers
IoT	Indicator of Compromise
TRL	Technology Readness Level
TTP	Tactics, Techniques, and Procedures
WP	Work Package

Executive Summary

MIRANDA is a Horizon Europe project that aims to design, develop, implement and validate a framework for collaborative cybersecurity operations in service supply chains. Communication and Dissemination (C&D) in MIRANDA are essential to ensure the impact of project results on key target audiences and to maximise project sustainability, engage stakeholders, and promote project results and achievements.

The Communication and Dissemination strategy and plan clearly show how all the communication and dissemination channels, activities, and tools work together to address the relevant stakeholder groups. It includes (a) an overview of the C&D needs, stakeholder mapping, and analysis; (b) shaping of the specific key messages and content strategy depending on the audience; (c) selection of the proper tools to convey the messages (e.g., website, webinars, video content, leaflets, digital visuals, learning resources, conferences, newsletters, articles, etc.) and overview of foreseen activities; (d) foreseen dissemination activities; (e) target indicators, monitoring and updating procedures; (f) ad hoc templates for MIRANDA deliverables and other documents.

A wide array of communication channels will be set up to engage in dialogue with relevant stakeholders and the general public and, consequently, to create a fertile environment for the different exploitation models. They include digital and hardcopy material that will be distributed through the project website and at physical events. The communication strategy envisions two intense phases at the project's beginning and end, where the project identity and final value proposition will be delivered, respectively. Communication in the first period will mainly target end users of MIRANDA (i.e., service providers and municipalities) and the general public; in the second period, the main target will shift to potential commercial partners, namely cyber-security vendors and operators. To effectively support all partners in communication activities during the first half of the project, several activities have already been undertaken in the early stage of the project: 1) the setup of the communication media, including the website and two social media accounts (X and LinkedIn); 2) the design of the project logo and its visual identity, including colour palette, background image, document templates and styles; 3) a rich set of material, including the initial versions of the flyer, the leaflet, the poster, and the roll-up, all delivering the same key messages in a uniform way yet tailored to the different media formats and their intended usage; 4) press release to be tailored by each partner in their own local language and published in their own website or through press agencies; 5) an initial presentation, focusing on common needs of Smart Cities and value proposition from MIRANDA.

In addition to communication, dissemination is an integral and continuously ongoing project activity. The main objectives of dissemination are thereby (1) to ensure that results are openly available to the widest audience, (2) to draw the attention of key users to the project, (3) to influence policies, guidelines, and standards, (4) to facilitate knowledge transfer and establish a foundation for future research, and (5) to ensure accountability and transparency. The dissemination plan addresses these goals through a series of activities which will begin during the project and continue until its completion, or potentially extend beyond it. These activities are summarized in order in the following. (1) Presentations of concepts, current gaps, and project results that are particularly designed to inform industrial stakeholders and municipalities aim to increase awareness about the project’s outcomes, gather feedback from

experts, direct actions by decision-makers, and kickstart collaborations. (2) Education is an activity that involves training students in summer schools, lectures, and workshops to spread knowledge and attract young academics to join the project as Master or PhD students. (3) Publications of scientific papers in top conferences and journals (including ACM, IEEE, and Springer, among others) are essential to boost the visibility of the project and its results, such as novel algorithms, concepts, and evaluations. Publications remain relevant even after the end of the project and prove to reach a global audience, particularly when they are available as gold open access, which is pursued by default in this project. (4) Joint workshops with other research projects enable the exchange of experience reports and ideas, foster the collaborative development of technologies, and extend the scope of the developed tools beyond their intended scope. (5) Training is carried out as hands-on exercises directed towards capacity building for users of the MIRANDA platform, such as security professionals. (6) Webinars are virtual educational sessions that aim at knowledge sharing and skill development through demonstrations, presentations, and exercises. (7) The software of individual tools and the entire MIRANDA platform are published as open-source code to increase visibility, enable researchers to reproduce results, and facilitate collaboration and interaction with the community. The consortium commits to publishing data sets as Open Data and open-source code alongside publications to align with Open Science principles. (8) Demonstrations validate the tools developed in the MIRANDA project and show the features of the MIRANDA platform. All dissemination activities are tracked during the project, and the corresponding key performance indicators are continuously monitored.

Table of Contents

List of Figures

List of Tables

1. Introduction

Modern digital systems rely heavily on services provided by third-party vendors, creating complex supply chains with many connections and often hidden relationships. The fragmentation of cybersecurity operations in such systems makes it difficult to detect threats (attacks) in a coordinated and effective manner and respond to them quickly.

MIRANDA is a Horizon Europe project that aims to design, develop, implement and validate a framework for collaborative cybersecurity operations in service supply chains. The framework is based on the Cybersecurity Digital Twin (CDT) paradigm. It enables the topology of complex service chains to be designed with limited trust. The CDT-based framework also enables effective threat prediction and the implementation and integration of tools for proactive and adaptive protection of individual components and the entire system.

Communication and Dissemination (C&D) in MIRANDA are essential to ensure the impact of project results on key target audiences and to maximize project sustainability, engage stakeholders, and promote project results and achievements.

This document (D6.1) defines the communication strategy, the essential elements of the plan for disseminating project work results, and qualitative and quantitative indicators for monitoring the implementation of the C&D strategy. The C&D activities list presented in Sections 2 and 3 are the parts of the 18-month progress report to the EU, accompanied by a review of the plans to allow for corrective action and adjustment to circumstances. A robust communication and dissemination strategy will be implemented through various networks and means that provide information and ground rules for the planned C&D activities of the project.

D6.1 aims to answer the following questions:

- What are the objectives of the communication and dissemination efforts?
- How should the C&D plan efficiency be measured?
- Who would be interested in knowing about the outcomes?
- What is the most effective way to reach the MIRANDA stakeholders?

This document is prepared at an early project stage (M3). It will be updated in D6.2 and D6.3 with the specific list of persons, organizations, events, and timeframe for each action and target group. D6.3 will also include an overview of the realized communication and dissemination activities in complement to the periodic reports.

1.1 Objectives of the Communication and Dissemination Plan

The C&D strategy and plan explains how and when the Consortium will ensure that MIRANDA is visible as a project and maximises impact in research, market uptake, policy and practical relevance. The overall aims of the strategy are:

- to contribute to networking and exchange of information and experiences between organisations and to enable partners to receive regular process updates from the demo sites;
- to support partners in effectively communicating and disseminating their work while facilitating a regular flow of information within the Consortium;

- disseminate widely and effectively MIRANDA outputs through various channels and translate technical language and research findings into appropriate messages for different audiences;
- to influence and educate relevant stakeholders to positively affect technology uptake, research and legislative framework development;
- to ensure capacity building by training and knowledge transfer between the various target groups.

The C&D plan will be divided into two areas:

- the communication activities will focus on promoting the project's activities and raising awareness to a broad public base, informing decision-makers.
- the dissemination activities will focus on spreading the technical results of MIRANDA to target audiences and seek collaborations with other projects in the area to continue knowledge building.

1.2 Identification of Stakeholders

The MIRANDA C&D strategy cannot be separated from a clear stakeholder analysis. Identifying the needs of the target groups is the main prerequisite to successfully shaping the messages. The collective experience of consortium partners will guarantee a qualitative audience analysis aimed at investigating: what is their knowledge of the subject, what is their motivation to become involved, what are the barriers to having them involved, who influences them and their impact on social or regulatory aspects.

Considering the wide range of applications and services developed in the MIRANDA project, the following audiences relevant to the project's vision, aims and objectives have been identified.

1.2.1. Citizens

Citizens are the broadest audience targeted by MIRANDA. As final consumers of digital services, they represent the final, yet equally important, link in the digital supply chain. Hence, they have the right to be informed and educated about relevant factors affecting their personal and private spheres. Citizens must know the security implications behind the digital services they use daily to make informed decisions when selecting providers and their offers.

Citizens are usually not interested in technical details, but they must be given enough context and simplified guidelines for navigating the complexities of the digital landscape. The main population segments of interest for MIRANDA are:

- Children and teenagers who approach technology as an integral part of their lives need a basic understanding and principles about security concepts and technologies to mature and grow in the digital era.
- Adults who are common users of digital services and seek to explore, in greater depth, the implications of putting personal and private data in digital services around them.

1.2.2. Service providers

This group includes technology providers that create services by deploying their in-house solutions and connecting them to external services, like cloud and networking infrastructures, public software repositories, data spaces and open data, web services, etc. They often do not manage cyber-security aspects by themselves but rely on external providers. In any case, they represent potential customers and integrators of MIRANDA technologies related to monitoring and enforcement.

Within this group, we can distinguish between organizations that operate services directly accessible to citizens (e.g., municipalities) and organizations that operate services intended for other businesses (e.g., cloud providers, telco operators, web services). As a specific group internal to the project, MIRANDA will consider municipalities that are largely involved in developing Smart Cities today.

Service providers are the main end users and will be key in the project's design phase when defining the specific use cases that explain how MIRANDA would change current practices. They will help get a better understanding of their needs. They will contribute to defining requirements, especially concerning human interfaces and integration into their existing business processes.

1.2.3. Security operators

Security operators are the groups that manage cyber-security. They can be internal staff of the service providers (e.g., part of the IT department) or external organizations that manage security on behalf of their customers. They usually operate a Security Operation Center (SOC), which interconnects to the digital assets of their customers. They are skilled in cyber-security and represent the main commercialization targets for MIRANDA operational technologies.

Security operators are also part of end-users, managing cyber-security processes. Within the project, they are part of the service providers' staff, but the largest group will be addressed regarding communication activities.

1.2.4. Technology providers

Technology providers include all developers of ICT technology that may be used to deploy and operate digital services. The main target includes developers of software applications, cyber-security appliances, and IoT devices. At the same time, general-purpose hardware and the manufacturing industry do not fall under the project's scope.

This group represents potential MIRANDA technology integrators into their products and tools since their origin. Hence, they can make MIRANDA technologies available in the market and boost their adoption by service and security operators.

1.2.5. Business associations and technology clusters

Industrial associations and technology clusters are among the main targets for promoting the adoption of MIRANDA outcomes since they represent an invaluable opportunity to reach the largest set of end users and build additional case studies during and after the project.

The most interesting associations and clusters already identified at the proposal stages are represented by:

- The Smart City Marketplace,[1] powered by the European Commission, with 47 lighthouse cities, 166 fellow cities, and 95 total projects, represents the largest community of stakeholders that MIRANDA could reach.
- The FIWARE[2] association, with almost 100 members, 50 incubator hubs, a product/service marketplace, and accelerator programs, is another strategic community that allows the reach of most of the potential markets for MIRANDA in Europe.
- The GAIA-X[3] association is the leading European cluster for data spaces that also offers the opportunity to go beyond the European boundaries thanks to 377 members worldwide and extend the scope to 15 other ecosystems beyond Smart Cities.

1.2.6. Researchers and Academia

This group corresponds to research and academic institutions that can foster interest and give methodology and fundamental skills to young researchers, students, trainees, potential users, and other interested practitioners. Additionally, being MIRANDA a strongly research-biased innovation project, its mission includes fostering more research for additional algorithms, protocols, and formal methods at lower TRL that can further improve the scope and outcomes of the project.

1.2.7. Policy Makers and Standardization Organizations

This target group includes public bodies at the national and European levels like EC Directorates and Units, Ministries and Governments, Regulatory Agencies, National CERTs/CSIRTs, European Cyber-Security Organisation (ECSO), as well as standardization associations (e.g., IDS, ETSI, ENISA, etc.). They can support us in adopting MIRANDA concepts and interfaces in future security architectures and paradigms and ensure consistent and seamless standardization of security interfaces and APIs. The Communication strategy aims to make them aware of existing limitations in the NIS/NIS2 directives and the additional measures necessary to improve collaboration within digital ecosystems in a common, secure, and scalable way.

[1] https://smart-cities-marketplace.ec.europa.eu/

[2] https://smart-cities-marketplace.ec.europa.eu/

[3] https://gaia-x.eu/

2. COMMUNICATION

The MIRANDA communication plan has been designed according to the common 5W approach (Who-Why-What-When-hoW):

- To define the **branding and MIRANDA positioning** (why to communicate);
- To select the main stakeholders that may be interested in the project implementation and results to make them aware of the project concept, approach, and expected outcomes (who to communicate to);
- To define, develop, and deliver **communication content and messages** for the selected channels to synchronize communication activities with the project's milestones (what to communicate);
- To schedule the timing of **communication activities** to efficiently promote the project alongside its different implementation phases (from design to development and demonstration (when to communicate);
- To identify proper communication **channels**, such as the project's public website, social media accounts, press releases, and promotional materials (how to communicate).

The overall communication strategy will revolve around three main streams of activities:

1. Raising **awareness and visibility** about MIRANDA's vision, mission, and objectives by promoting the project concept, innovation and business opportunities.
2. Engaging the **community** of stakeholders by keeping them informed about the progress and interacting with them to share experiences, collect feedback, envision market opportunities, educate citizens and researchers, and push policy-making and standardization bodies.
3. Nurturing **business opportunities** by strengthening communication with potential customers and business partners, promoting technical and methodological advances with respect to competitors, boosting technical/business partnerships, and fostering follow-up initiatives that build on MIRANDA's outcomes.

The MIRANDA communication strategy is pictorially described in the funnel of Figure 1. The following will be detailed with respect to key messages, stakeholder analysis, timing of activities, and channels. To achieve its objectives, MIRANDA will implement a communication strategy that combines online and offline channels, content marketing strategies, online marketing tools, services, growth hacking techniques, analytics tools, media relations, advertising campaigns, press releases dissemination, presence at top events and work with intermediary institutions and stakeholders and influencers among others' efforts.

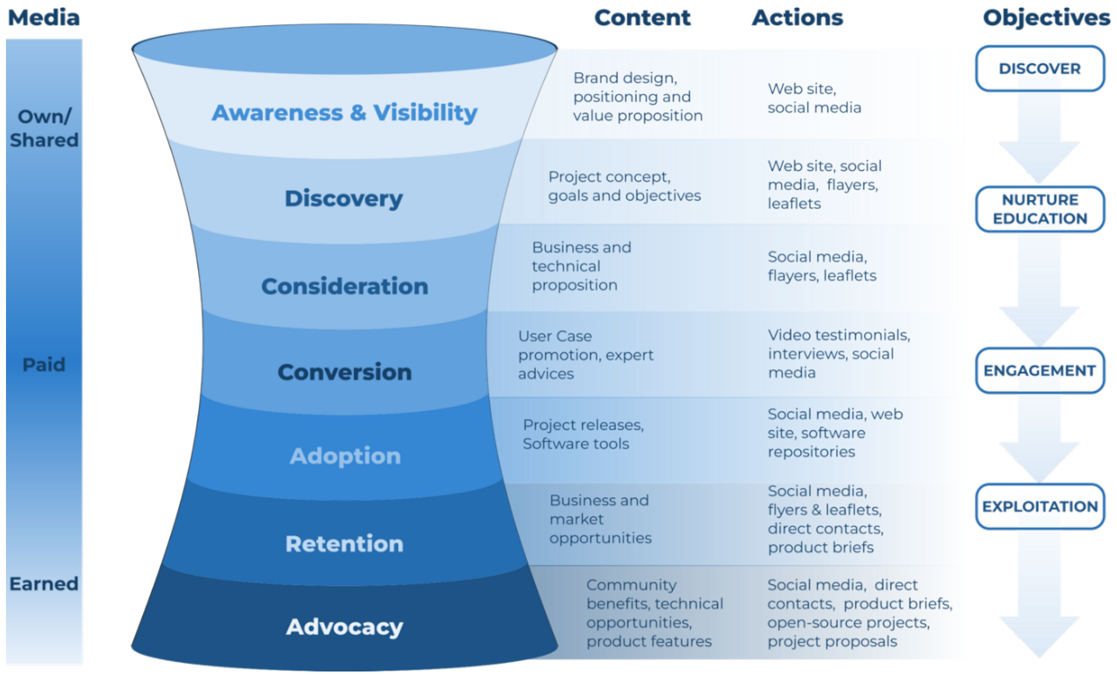

Media
Own/ Shared
Paid
Earned
Content
Actions
Objectives
Awareness & Visibility
Brand design, positioning and value proposition
Web site, social media
DISCOVER
Discovery
Project concept, goals and objectives
Web site, social media, flayers, leaflets
NURTURE EDUCATION
Consideration
Business and technical proposition
Social media, flayers, leaflets
Conversion
User Case promotion, expert advices
Video testimonials, interviews, social media
ENGAGEMENT
Adoption
Project releases, Software tools
Social media, web site, software repositories
Retention
Business and market opportunities
Social media, flyers & leaflets, direct contacts, product briefs
EXPLOITATION
Advocacy
Community benefits, technical opportunities, product features
Social media, direct contacts, product briefs, open-source projects, project proposals

Figure 1. Communication funnel

2.1 Brand Pillars

The main pillars of the MIRANDA brand are related to the core values of the project (see Figure 1):

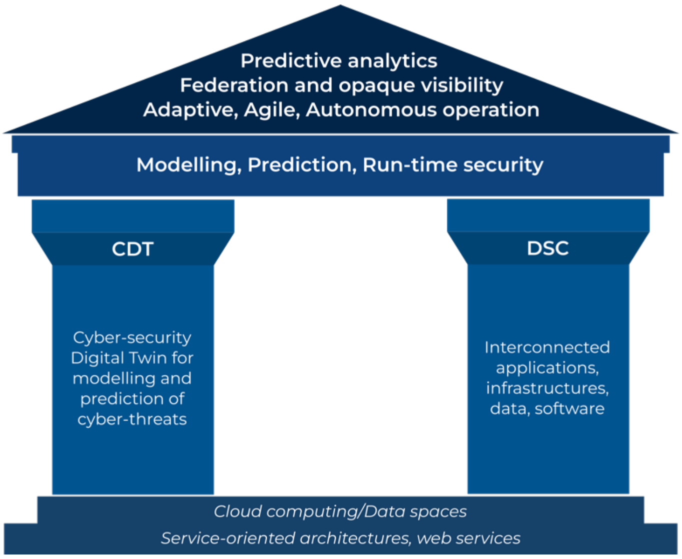

Predictive analytics
Federation and opaque visibility
Adaptive, Agile, Autonomous operation
Modelling, Prediction, Run-time security
CDT
Cyber-security Digital Twin for modelling and prediction of cyber-threats
DSC
Interconnected applications, infrastructures, data, software
Cloud computing/Data spaces
Service-oriented architectures, web services

Figure 2. The "temple" of the MIRANDA Communication strategy.

- **Security of interconnected, multi-ownership Digital Service Chains (DSCs)**. While modern digital services often build upon third-party components, many providers are often unaware of what is behind their upstream suppliers' resources. Dynamic service composition paradigms make the service mesh unpredictable and ever-changing at run-time. The communication strategy will also highlight the difference between vertical supply chain models (typically used for development and manufacturing) and horizontal models (used to deploy and operate complex services).

- **Cyber-security Digital Twin (CDT)**. MIRANDA develops a Cybersecurity Digital Twin (CDT) to model and capture the security posture of interconnected multi-ownership systems, which is used to detect, hunt, and remediate threats and attacks. MIRANDA's Cybersecurity Digital Twin is not a plain model of digital assets used to identify security issues. It is a combined model of the current execution environment and attacks, which provides pervasive visibility, proactive identification of vulnerabilities and attacks, and adaptivity to ever-evolving environments.

The MIRANDA approach revolves around three main layers: **modelling**, **prediction**, and **run-time security**:

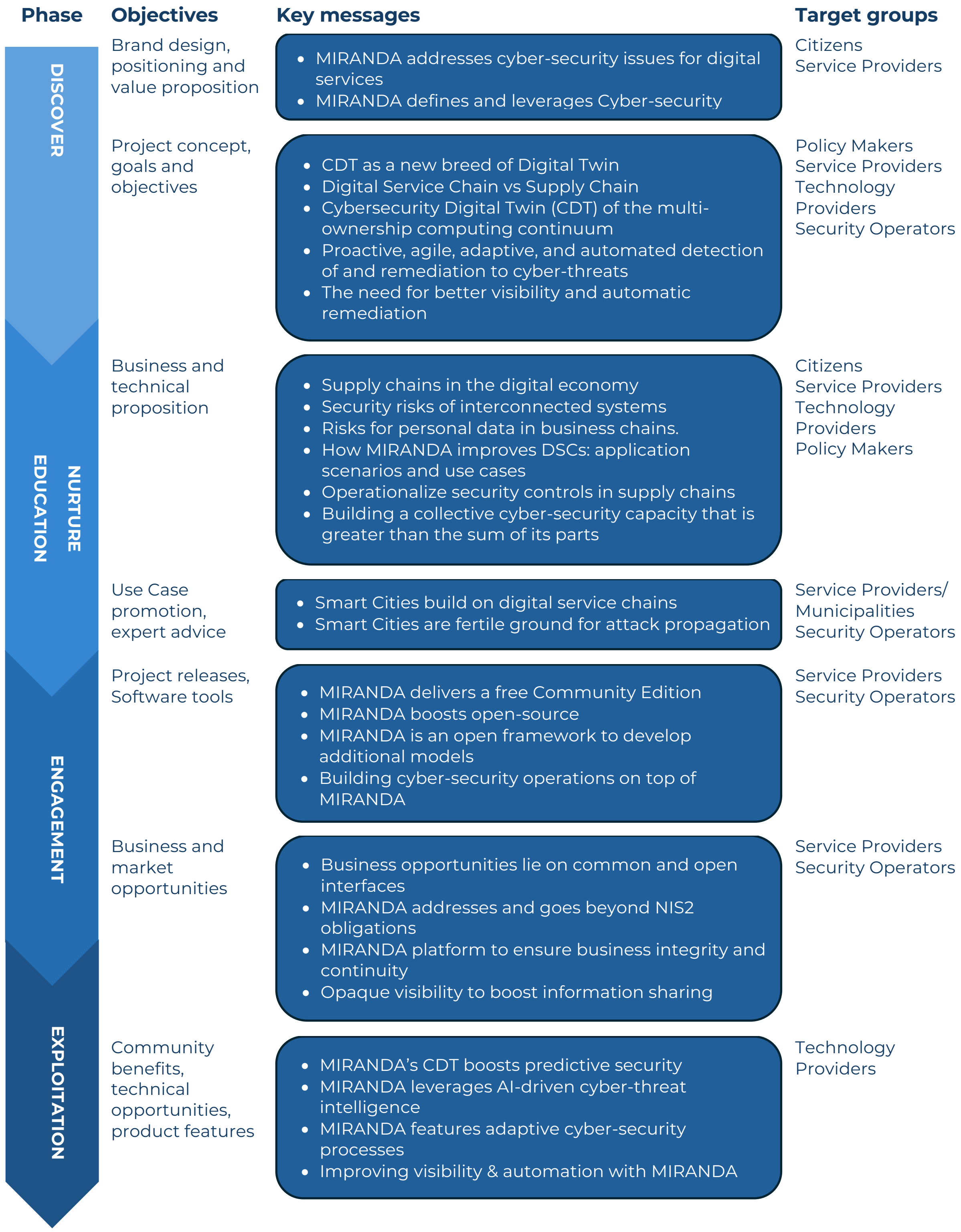
- **Modelling** is based on a true digital twin, which exchanges a bidirectional flow of information with the real system (made of ICT assets and cyber-security tools). The interaction is split into a control and a data flow, mediated by authentication and access control.
- **Prediction** is the major benefit that every Digital Twin should provide. For a CDT, prediction is mean in terms of its capability to anticipate attack paths at design time and every time a change occurs in the underlying system or the attack landscape.
- **Run-time security** builds on the CDT capabilities. It improves existing monitoring, detection, response, and hunting processes by delivering new tools for threat hunting, detection of lateral movements, and eradicating the root causes of attacks.

The expected outcomes from the MIRANDA approach are the improvements of existing cyber-security operations in terms of:

- **Predictive analytics**. A CDT's modelling and prediction capabilities are the base pillars for shifting from reactive to proactive cybersecurity by anticipating vulnerable links in the chain, developing attack strategies, and lateral movements between services.
- **Adaptive, agile, and autonomous response**. MIRANDA advocates and pursues the transition from context-less IoCs to more generic TTP descriptions, specifically aiming to tailor cyber-security processes to different environments and operating conditions easily. Adaptivity and agility are key characteristics that must also be reflected in the ability of the system to operate autonomously, with minimal user intervention for re-configuration in case of changes to the system topology and composition, as well as the attack landscape.
- **Federation and opaque visibility** across domains. The involvement of multiple providers poses confidentiality and privacy issues that hinder full knowledge of the whole system. MIRANDA's CDT is explicitly conceived to address such issues by federation mechanisms that allow the sharing of cyber-security data and models based on the trust level between domains, including the possibility of verifying their integrity and reputation at run-time.

2.2 Key Messages

The main communication milestones and key messages are described in Figure 3 below and are aligned with the different phases and objectives of the communication strategy.



Phase	Objectives	Key messages	Target groups
DISCOVER	Brand design, positioning and value proposition	• MIRANDA addresses cyber-security issues for digital services • MIRANDA defines and leverages Cyber-security	Citizens Service Providers
	Project concept, goals and objectives	• CDT as a new breed of Digital Twin • Digital Service Chain vs Supply Chain • Cybersecurity Digital Twin (CDT) of the multi-ownership computing continuum • Proactive, agile, adaptive, and automated detection of and remediation to cyber-threats • The need for better visibility and automatic remediation	Policy Makers Service Providers Technology Providers Security Operators
NURTURE EDUCATION	Business and technical proposition	• Supply chains in the digital economy • Security risks of interconnected systems • Risks for personal data in business chains. • How MIRANDA improves DSCs: application scenarios and use cases • Operationalize security controls in supply chains • Building a collective cyber-security capacity that is greater than the sum of its parts	Citizens Service Providers Technology Providers Policy Makers
	Use Case promotion, expert advice	• Smart Cities build on digital service chains • Smart Cities are fertile ground for attack propagation	Service Providers/ Municipalities Security Operators
ENGAGEMENT	Project releases, Software tools	• MIRANDA delivers a free Community Edition • MIRANDA boosts open-source • MIRANDA is an open framework to develop additional models • Building cyber-security operations on top of MIRANDA	Service Providers Security Operators
	Business and market opportunities	• Business opportunities lie on common and open interfaces • MIRANDA addresses and goes beyond NIS2 obligations • MIRANDA platform to ensure business integrity and continuity • Opaque visibility to boost information sharing	Service Providers Security Operators
EXPLOITATION	Community benefits, technical opportunities, product features	• MIRANDA's CDT boosts predictive security • MIRANDA leverages AI-driven cyber-threat intelligence • MIRANDA features adaptive cyber-security processes • Improving visibility & automation with MIRANDA	Technology Providers

Figure 3. Main project Communication milestones and key messages.

In summary, we first establish the brand design, positioning and value proposition by reflecting the main traits of the project in its logo and name. We then inform the project concept, vision, objectives, approach, and methodology by elaborating on the meaning of Digital Service Chain and Cyber-security Digital Twin and their intended usage to improve cyber-security operations.

The next phase is devoted to educating the culture of cyber-security, both the youngest generation and adults and stakeholders. This includes specific activities highlighting the security implications of interconnecting services from different providers, the difficulty of establishing coordinated monitoring and response in multi-ownership environments, the risk for everyone when using digital services in their everyday lives, and possible pathways towards more collaborative approaches across digital service chains.

The education phase is further reinforced by story-telling of envisioned application scenarios beyond the project use cases, including other industrial sectors where chaining services is becoming an increasing practice. After preliminary software tools and results are available, the engagement phase will focus on potential customers by showing the technical and business opportunities behind MIRANDA. This will leverage open-source software and design to foster early adoption in research projects and lighthouse initiatives around Europe, aiming at further spreading the MIRANDA vision and approach.

As the last phase, which is expected to last after the project ends, exploitation will be supported by giving prominence to the main innovations delivered by MIRANDA, as well as pushing the necessary policy framework to fill existing gaps towards collaborative and shared cyber-security between providers, even beyond critical infrastructures and services. The target is commercial exploitation and further research and innovation activities that could extend the project's scope and capabilities.

2.3 Timing of activities

Communication actions have already started at M1, with the design of the project logo and main branding material, the set-up of social accounts, and the deployment of the website. The timeline for Communication actions shows a different intensity during the project implementation based on the following considerations:

- to increase the number of actions when more valuable content is available (i.e. when the project starts and after the delivery of concrete results starting from M30);
- to not overwhelm the intended audience with large bulks of messages in a short time, hence trying to spread them in several months;
- to maintain continuous presence and interaction with target groups, avoiding giving the impression that the project is not active or discontinued, even when no significant new content is available.

Figure 4 shows the timeline of communication actions for the project's duration. Each activity is highlighted in the same colour as the corresponding phase in which it is implemented. Differently from the previously shown pipeline that gives the impression of purely sequential activities, **their implementation is partially parallel and overlapped** to follow the timeline when the appropriate content is available and to distribute the effort over the whole programme.

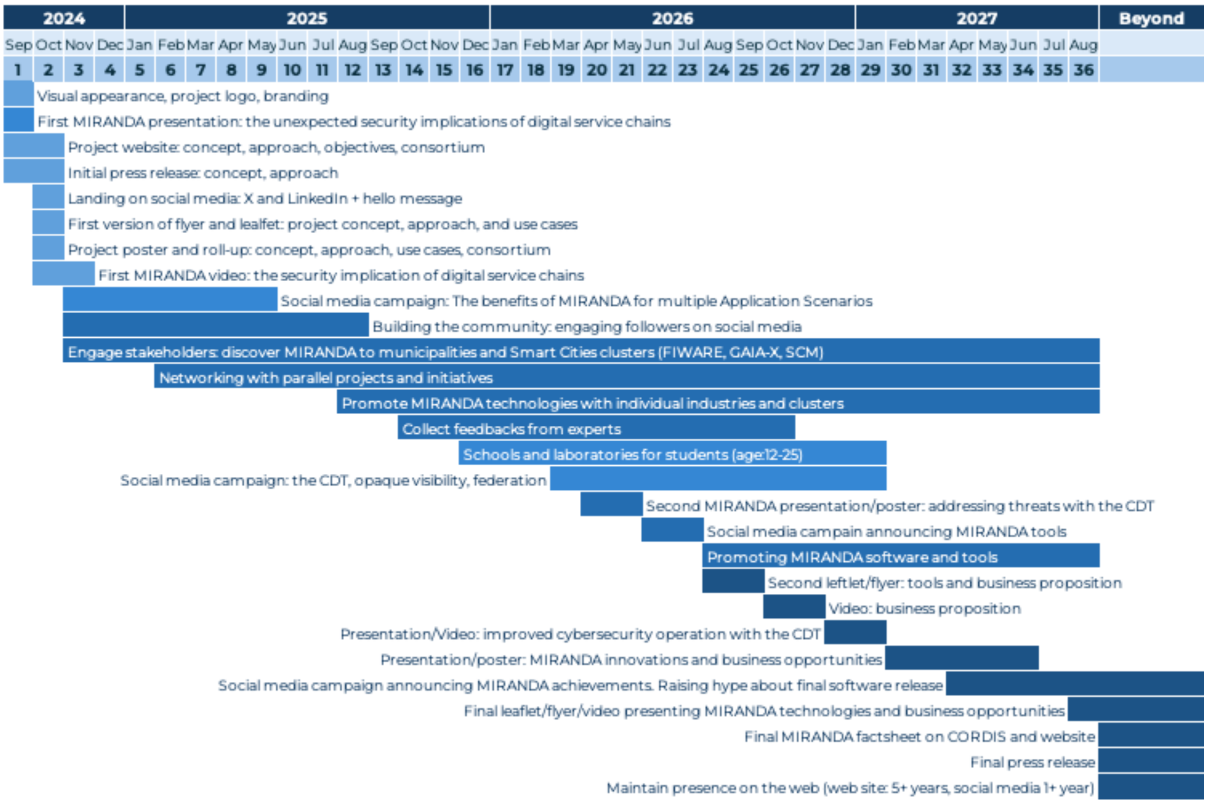


Figure 4. Timing of the Communication actions.

Communication activities in MIRANDA 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. During the **intermediary period**, the effort will shift towards engagement of the stakeholders, community building and education against the project vision. The 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**.

For what concerns direct contacts with stakeholders, Table 1 lists the planned meetings and events that will be attended by project partners in the following 18 months.

Table 1. Planned Communication activities in meetings and events.

Name	Location	Date	Partner	Target group
FIWARE Global Summit	Naples, Italy	18th-19th September 2024	CNR	Municipality, Service providers
City of Genoa/RAISE association	Genoa	End 2025	CNR	Municipality, Service Providers, Technology Providers
EDU25	Genoa	Spring 2025	CNR	Citizens (young people)
IKT Sicherheitskonferenz	Austria	25th-26th June 2025	AIT	Military staff, cyber security professionals

Smartland (roadshow/roundtable training session)	Bologna, Italy	2nd October 2024	MINDI	Marketing and Sales staff
JRC ERIGRID 2.0	Ispra, Italy	7th-8th October 2024	MINDI	Scientific Institution
Smartland (roadshow/roundtable training session)	Catania, Italy	9th October 2024	MINDI	Marketing and Sales staff
Jazz'inn 2024 SPAZI QUATTRO ZERO	Meran, Italy	7th-13th October 2024	MINDI	Companies, Institutions, Communities
Milano Digital Week 2024 (widespread collective event)	Milan, Italy	10th -14th October 2024	MINDI	Companies, Institutions, Communities
Smartland (roadshow/roundtable training session)	Milan, Italy	22nd October 2024	MINDI	Marketing and Sales staff
Smart City Expo World Congress	Barcelona, Spain	5th – 7th November 2024	MINDI, DAEM	Companies, Institutions, Communities
"C'è un domani da creare" (Education and training University event)	Salerno/Rome, Italy	6th-7th November 2024	MINDI	Students, Professors, Telco HR, Telco C-Level
Assemblea annuale Anci (congress)	Italy	20th-21st November 2024	MINDI	Public Administration, Local Government

2.4 Communication channels

MIRANDA will use digital and physical channels to reach the broadest audience at the right time. Figure 5 shows the main communication channels that will be used to deliver specific communication messages.

The content will be delivered through a traditional website as the main point of presence on the Internet and social media to have more direct, interactive, and immediate communication with the community. The content will be replicated in different channels by adapting the language, technical details, and length to the specific media. All communication materials (leaflets, flyers, posters, roll-ups) will be made available on the project website for download and printed for showing and distribution at in-person events. Presentations will also be made available for download. The availability of new communication materials will be announced on social media.

	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-security issues for DSCs with the CDT	Meet technology providers Give presentations about business 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 5. Communication channels and key activities

2.5 Target Key Performance Indicators and Expected Impacts

Key performance indicators have been taken from the proposal and revised to maximize the impact of the Communication actions. The main objective is to ensure continuous, seamless, and non-intrusive message delivery without overwhelming the target groups and being perceived as spam.

Table 2. KPI for Communication activities.

Action	Target KPIs	Expected impact
Web site visitors Average visit duration Downloads	≥ 5000 ≥ 3 min ≥ 200	Increased number of software downloads and followers Parallel initiative setup with similar objectives Project invited to attend cluster and industrial meetings
Promotional material (leaflets, white papers) No. copies or downloads	6 ≥ 500	More people are reached during poster, demo, and exhibition sessions Potential adopters not involved in cyber-security are made aware of DSC implications
Social media activity: - posts - followers - comments	≥ 150 ≥ 200 ≥ 400	Build a large and heterogeneous community of stakeholders People are triggered to download and read new technical/business material People are encouraged to provide feedback, comments, and suggestions that help improve the technology and business proposition
Promotional videos No. of views	3 ≥ 200	Communication messages reach the largest audience (especially among the youngest people) Drawn the attention of more people This is a better opportunity to stick key messages in mind
Number of MIRANDA presence in events	≥ 12	New collaboration opportunities are identified (during and after the project) Business opportunities for industrial partners Funding opportunities for research partners
Laboratories or seminars Number of reached people	3 ≥ 80	People become more aware of security implications in everyday life People become more prone to insecure posture (default password, disclosed passwords and private data, trusting phishing messages, …)

2.6 Use of the EU emblem

As MIRANDA partners are the beneficiaries of EU funding, the European Union emblem shall be used in all project dissemination materials/press releases/media contacts to acknowledge the support received under the EU programme.

The programme's name (Horizon Europe) shall be used as a verbal brand, i.e. references to it will be made without a regulated visual mark or logo. Basic rules:

- The minimum height of the EU emblem shall be 1 cm.
- The name of the European Union shall be used in conjunction with the name of the programme or fund and be spelt out in full.

- The typeface to be used with the EU emblem can be any of the following: Arial, Calibri, Garamond, Trebuchet, Tahoma, Verdana. Italic and underlined variations and the use of font effects are not allowed.
- The positioning of the text in relation to the EU emblem is not prescribed in any particular way, but the text should not interfere with the emblem in any way.
- The font size used should be proportionate to the size of the emblem. The font should be reflex blue (the same blue colour as the EU flag), black or white, depending on the background.
- The following MIRANDA statement about EU financing shall be used throughout the whole project duration when communicating about the project:

This project has received funding from the European Union's Horizon Europe Research and Innovation Programme under grant agreement No. 101168144.

The mandatory statement may also be extended with the following disclaimer, which is mandatory for deliverables and scientific publications:

However, the views and opinions expressed are 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.

When displayed with another logo, the EU emblem must have appropriate prominence.

Both elements: (1) the statement above and (2) the EU emblem should be used according to the rules when communicating about the project (in promotional materials, project templates, project deliverables, project website, social media, etc.).

If it would not be possible to include both elements e.g. when publishing articles in magazines (due to lack of space or especially in cases where we have no control of the final publication format or contents), please make sure to include the phrase: at least

The project is co-funded by the European Union

2.7 Preliminary Communication Activities

Even if part of the Communication strategy itself, some activities have already been implemented in the very early stage of the project. They are essential to support the following actions throughout the project. Such activities include visual branding, the website, social media accounts, and preliminary communication material.

2.7.1. Project logo and visual branding

The MIRANDA logo was designed to reflect the brand pillars in a stylized way, which draws attention and distinguishes the project from any other existing initiative, even with the same name. It was explicitly designed to be highly evocative and easily remember to recognize the project branding immediately.

The project logo uses the following font from Microsoft: **Bauhaus 93.**[4] The selection of a colour palette based on dark blue with white contours immediately evokes cyber-security images and artwork on the Internet, which often use a similar palette. The logo colour scheme contains 3 main colours (Figure 6). Two versions have been produced using these three colours to guarantee readability for both dark and light backgrounds.

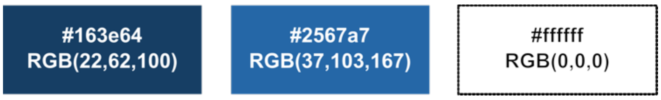


Figure 6. MIRANDA logo colour scheme

The logo comprises a logotype, which embeds an ideogram in its lettering. The latter is designed to evoke the two pillars of "digital service chains" and "cyber-security digital twin". The ideogram is built from the lowercase "n" of the "Miranda" logotype, which is metaphorically duplicated and reversed to recall the idea of links in a chain. One of such "links" is indeed specular and blurred, which is representative of the concept of digital twin, which models the real system with a certain degree of approximation and uncertainty. The ideogram blends the concept of "service chain" and "digital twin" together by using the same symbols to represent both. Additionally, the ideogram inside the MIRANDA logo (and specifically the reversed and blurred "n") intentionally breaks the perfect grid of the logotype to draw the attention of those who look at it and to give the sensation of something that falls out; this strengthens the concept of a digital twin that operates a part of the real system. At the same time, the main and blurred "n's" of the ideogram hug one another, which is highly evocative of both a chain and the bidirectional interaction between the real system and its digital twin. The spacing is also calibrated to give equilibrium to the whole graphics by using the same spacing between letters and the ideogram.

The logo should be used in its main version when possible. The square format can be used if it is not possible due to technical reasons/graphical reasons. The square format splits the ideogram from the logotype, giving prominence to the former. The logotype is split into the left top and right bottom parts by aligning the last letter of the first part and the first letter of the second part. The readability of the logotype is still maintained in this version, but the whole logo is inscribed in a perfect square, as required by some social media and typographic formats.

Finally, the ideogram alone can be used for visual branding when the project identity is already well-known by other means (e.g., as a favicon on the website, sort of stamp in dissemination materials and deliverables, or icon in graphs).

The selection of the colour palette is more suitable for light backgrounds; however, the white contour allows the use of the logo with no problem, as well as dark backgrounds. For special

[4] https://learn.microsoft.com/it-it/typography/font-list/bauhaus-93

black-and-white or greyscale composition cases, a black/white version is also provided for all logo formats (normal, square, ideogram-only).

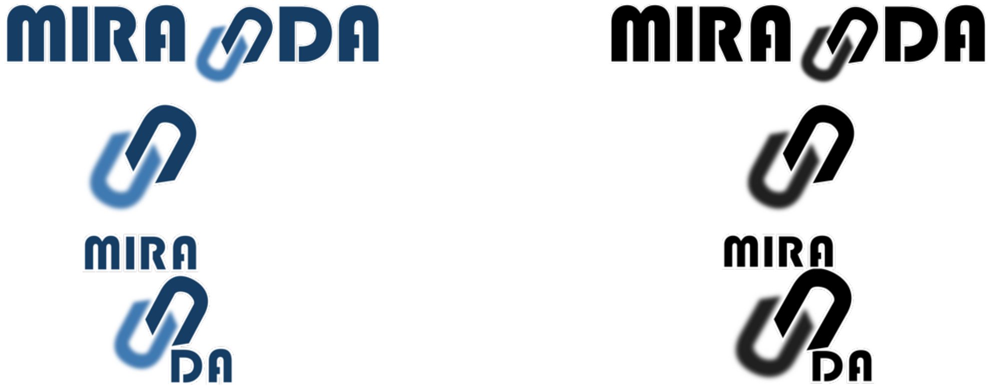
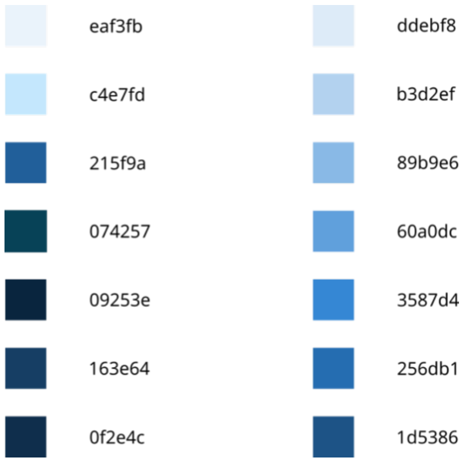


Figure 7. MIRANDA project logos: main, ideogram only, square (from top to bottom). On the right side, the b/w version is shown.

Besides the project logo, visual branding includes a colour palette for communication and dissemination material and a background picture highly representative of the project scope.

The colour palette includes several gradations of blue for lighter to darker tones, which are used both for background and foreground elements.



eaf3fb	ddebf8
c4e7fd	b3d2ef
215f9a	89b9e6
074257	60a0dc
09253e	3587d4
163e64	256db1
0f2e4c	1d5386

Figure 8. The colour palette used in Communication material.

Finally, representative images of the project scope and approach have been prepared. A background image is available that iconizes the concept of digital service chains and their protection. Blurred on the background, the city landscape evokes the project's main application domain, i.e., Smart Cities. The shadowed landscape can also be used separately if a monochrome background is needed to give more prominence to foreground components. This image is shown in Figure 9 and uses similar colour tones to simplify adding foreground information on top, like writings and icons.

Figure 9. Background image for communication and dissemination material.

A foreground image is also available, highlighting the elements already represented in the background picture, using different colours for services and security agents. It is shown in Figure 10. This can be used as an evocative representation of the MIRANDA scope.

Figure 10. Evocative image depicting the MIRANDA scope.

Finally, a more brilliant image with a broader chromatic range is also available to depict the project concept and approach. This image is shown in Figure 11.

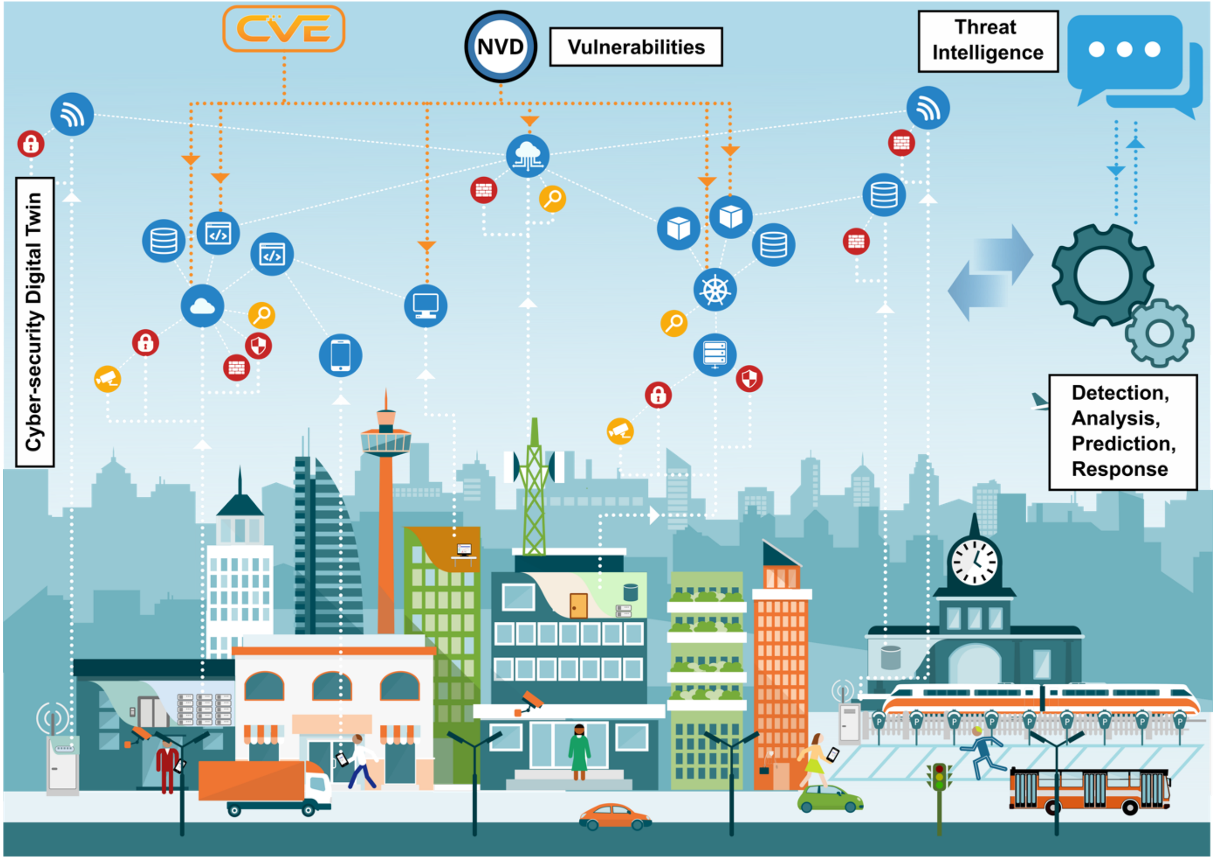

CVE
NVD
Vulnerabilities
Threat Intelligence
Cyber-security Digital Twin
Detection, Analysis, Prediction, Response

Figure 11. Image representing MIRANDA's concept and approach.

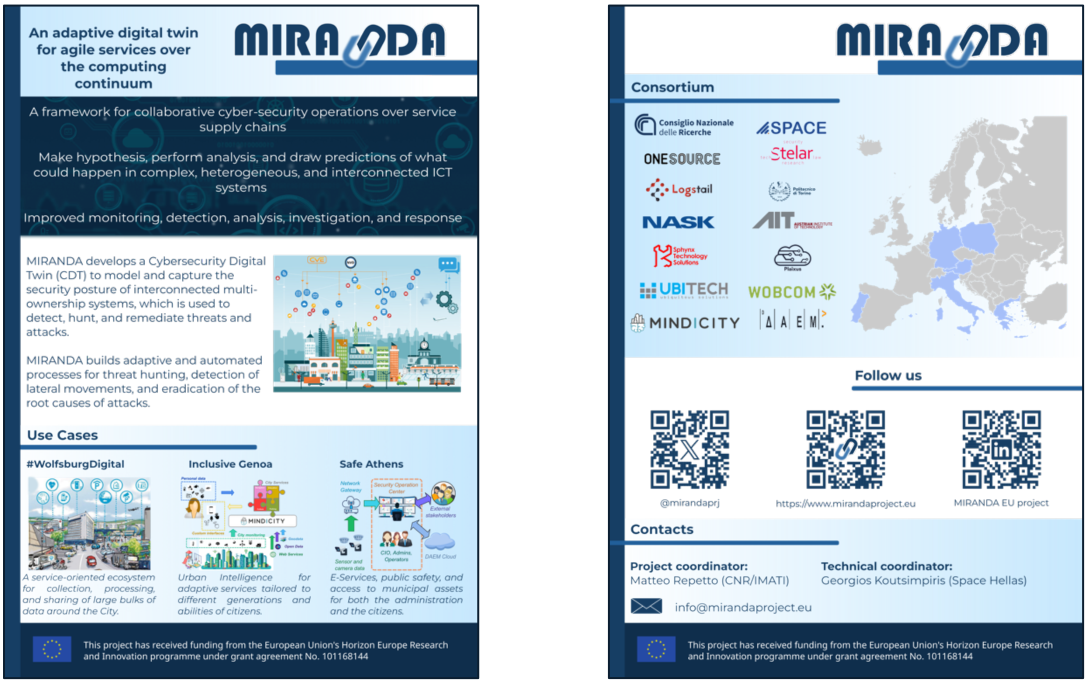
2.7.2. Leaflet and flyers

The leaflet and flyer contain almost the same information to ensure consistency of the communication messages across the different materials. However, they differ in the graphical design, even if they are the same size since they are conceived for different purposes.

The flyer contains less text and is designed to draw people's attention while walking and quickly looking at different stands or expositors. The flyer only contains concise messages and privileges images over text descriptions. The Consortium composition is given prominence, as well as the QR codes to access social media and the website.

The leaflet is conceived to be read without waste by people who want to dig deeper into the project concept and approach. It tries to deliver the most messages possible in a balanced way. The cover and back follow similar principles to the leaflet by focusing on a single message and giving reference links; the folded side contains the Consortium, which draws attention as soon as the leaflet is unfolded, while the internal part uses all the page to arrange in the best way the key messages.

The first version of the project leaflet and flyer focuses on the project concept, objectives, and approach. They are conceived to raise interest and curiosity and to provide the necessary links and contact points to discover more about the project.



An adaptive digital twin for agile services over the computing continuum

MIRANDA

A framework for collaborative cyber-security operations over service supply chains

Make hypothesis, perform analysis, and draw predictions of what could happen in complex, heterogeneous, and interconnected ICT systems

Improved monitoring, detection, analysis, investigation, and response

MIRANDA develops a Cybersecurity Digital Twin (CDT) to model and capture the security posture of interconnected multi-ownership systems, which is used to detect, hunt, and remediate threats and attacks.

MIRANDA builds adaptive and automated processes for threat hunting, detection of lateral movements, and eradication of the root causes of attacks.

Use Cases

#WolfsburgDigital

A service-oriented ecosystem for collection, processing, and sharing of large bulks of data around the City.

Inclusive Genoa

Urban Intelligence for adaptive services tailored to different generations and abilities of citizens.

Safe Athens

E-Services, public safety, and access to municipal assets for both the administration and the citizens.

This project has received funding from the European Union's Horizon Europe Research and Innovation programme under grant agreement No. 101168144

MIRANDA

Consortium

Follow us

@mirandaprj

https://www.mirandaproject.eu

MIRANDA EU project

Contacts

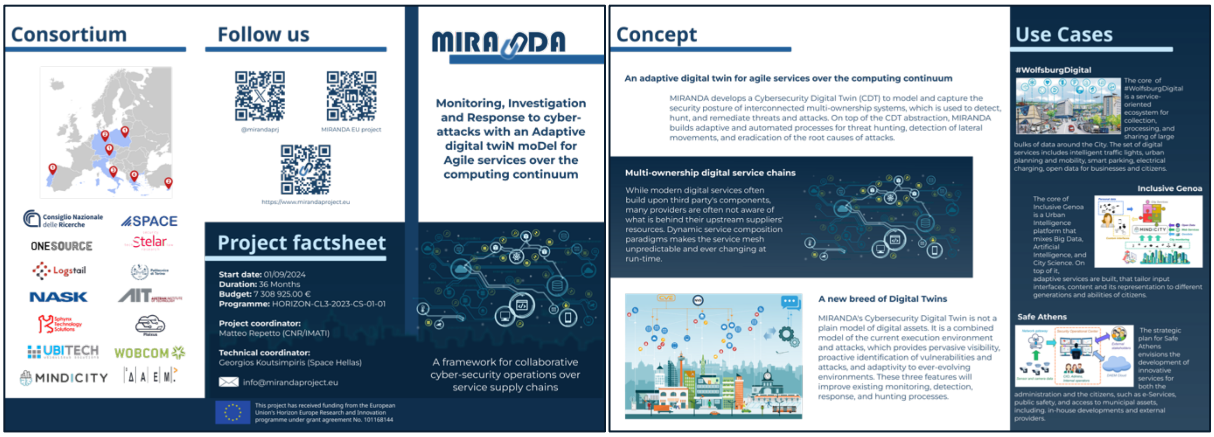
Project coordinator:
Matteo Repetto (CNR/IMATI)

Technical coordinator:
Georgios Koutsimpiris (Space Hellas)

info@mirandaproject.eu

This project has received funding from the European Union's Horizon Europe Research and Innovation programme under grant agreement No. 101168144

Figure 12. First version of the MIRANDA flyer.



Consortium

Follow us

@mirandaprj

MIRANDA EU project

https://www.mirandaproject.eu

Project factsheet

Start date: 01/09/2024
Duration: 36 Months
Budget: 7 308 925.00 €
Programme: HORIZON-CL3-2023-CS-01-01

Project coordinator:
Matteo Repetto (CNR/IMATI)

Technical coordinator:
Georgios Koutsimpiris (Space Hellas)

info@mirandaproject.eu

This project has received funding from the European Union's Horizon Europe Research and Innovation programme under grant agreement No. 101168144

MIRANDA

Monitoring, Investigation and Response to cyber-attacks with an Adaptive digital twiN moDel for Agile services over the computing continuum

A framework for collaborative cyber-security operations over service supply chains

Concept

An adaptive digital twin for agile services over the computing continuum

MIRANDA develops a Cybersecurity Digital Twin (CDT) to model and capture the security posture of interconnected multi-ownership systems, which is used to detect, hunt, and remediate threats and attacks. On top of the CDT abstraction, MIRANDA builds adaptive and automated processes for threat hunting, detection of lateral movements, and eradication of the root causes of attacks.

Multi-ownership digital service chains

While modern digital services often build upon third party's components, many providers are often not aware of what is behind their upstream suppliers' resources. Dynamic service composition paradigms makes the service mesh unpredictable and ever changing at run-time.

A new breed of Digital Twins

MIRANDA's Cybersecurity Digital Twin is not a plain model of digital assets. It is a combined model of the current execution environment and attacks, which provides pervasive visibility, proactive identification of vulnerabilities and attacks, and adaptivity to ever-evolving environments. These three features will improve existing monitoring, detection, response, and hunting processes.

Use Cases

#WolfsburgDigital

The core of #WolfsburgDigital is a service-oriented ecosystem for collection, processing, and sharing of large bulks of data around the City. The set of digital services includes intelligent traffic lights, urban planning and mobility, smart parking, electrical charging, open data for businesses and citizens.

Inclusive Genoa

The core of Inclusive Genoa is a Urban Intelligence platform that mixes Big Data, Artificial Intelligence, and City Science. On top of it, adaptive services are built, that tailor input interfaces, content and its representation to different generations and abilities of citizens.

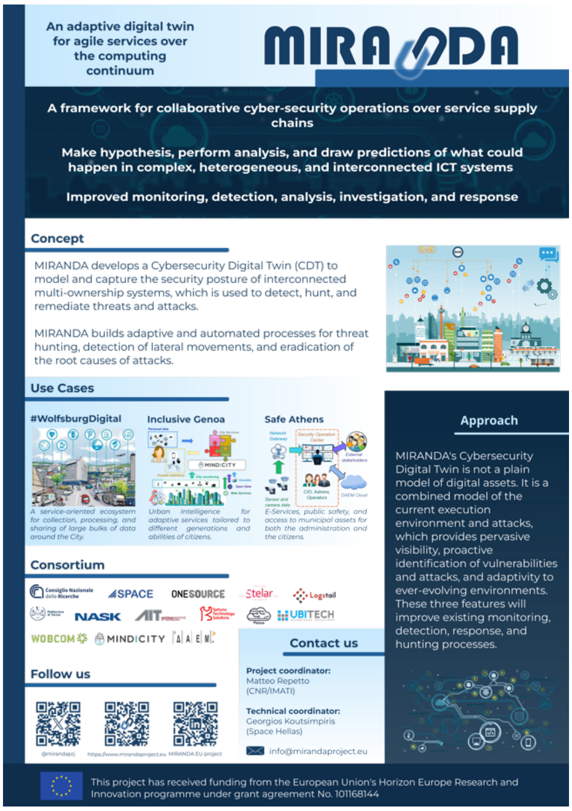
Safe Athens

The strategic plan for Safe Athens envisions the development of innovative services for both the administration and the citizens, such as e-Services, public safety, and access to municipal assets, including. in-house developments and external providers.

Figure 13. The first version of the MIRANDA leaflet.

2.7.3. Poster and roll-up

The MIRANDA poster and roll-up are schematic and intended to give a rough idea of the project identity and visual branding. They also contain information about the scope and approach and are designed to draw attention from a quite large distance rather than being read in detail. The content is the same as the flyer/leaflet to maintain consistency among the different media.



An adaptive digital twin for agile services over the computing continuum

A framework for collaborative cyber-security operations over service supply chains

Make hypothesis, perform analysis, and draw predictions of what could happen in complex, heterogeneous, and interconnected ICT systems

Improved monitoring, detection, analysis, investigation, and response

Concept

MIRANDA develops a Cybersecurity Digital Twin (CDT) to model and capture the security posture of interconnected multi-ownership systems, which is used to detect, hunt, and remediate threats and attacks.

MIRANDA builds adaptive and automated processes for threat hunting, detection of lateral movements, and eradication of the root causes of attacks.

Use Cases

#WolfsburgDigital

A service-oriented ecosystem for collection, processing, and sharing of large bulks of data around the City.

Inclusive Genoa

Urban Intelligence for adaptive services tailored to different generations and abilities of citizens.

Safe Athens

E-Services, public safety, and access to municipal assets for both the administration and the citizens.

Approach

MIRANDA's Cybersecurity Digital Twin is not a plain model of digital assets. It is a combined model of the current execution environment and attacks, which provides pervasive visibility, proactive identification of vulnerabilities and attacks, and adaptivity to ever-evolving environments. These three features will improve existing monitoring, detection, response, and hunting processes.

Consortium

Follow us

@mirandaprj https://www.mirandaproject.eu MIRANDA EU project

Contact us

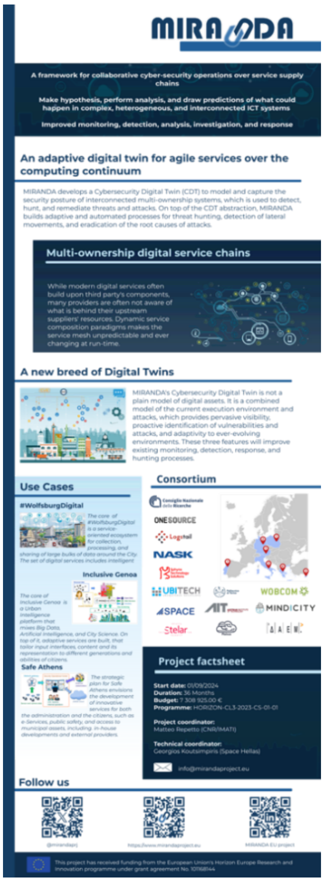
Project coordinator: Matteo Repetto (CNR/IMATI)

Technical coordinator: Georgios Koutsimpiris (Space Hellas)

info@mirandaproject.eu

This project has received funding from the European Union's Horizon Europe Research and Innovation programme under grant agreement No. 101168144

Figure 14. First version of the MIRANDA poster for communication activities.



A framework for collaborative cyber-security operations over service supply chains

Make hypothesis, perform analysis, and draw predictions of what could happen in complex, heterogeneous, and interconnected ICT systems

Improved monitoring, detection, analysis, investigation, and response

An adaptive digital twin for agile services over the computing continuum

MIRANDA develops a Cybersecurity Digital Twin (CDT) to model and capture the security posture of interconnected multi-ownership systems, which is used to detect, hunt, and remediate threats and attacks. On top of the CDT abstraction, MIRANDA builds adaptive and automated processes for threat hunting, detection of lateral movements, and eradication of the root causes of attacks.

Multi-ownership digital service chains

While modern digital services often build upon third party's components, many providers are often not aware of what is behind their upstream suppliers' resources. Dynamic service composition paradigms makes the service mesh unpredictable and ever changing at run-time.

A new breed of Digital Twins

MIRANDA's Cybersecurity Digital Twin is not a plain model of digital assets. It is a combined model of the current execution environment and attacks, which provides pervasive visibility, proactive identification of vulnerabilities and attacks, and adaptivity to ever-evolving environments. These three features will improve existing monitoring, detection, response, and hunting processes.

Use Cases

#WolfsburgDigital

The core of #WolfsburgDigital is a service-oriented ecosystem for collection, processing, and sharing of large bulks of data around the City. The set of digital services includes intelligent

Inclusive Genoa

The core of Inclusive Genoa is a Urban Intelligence platform that mixes Big Data, Artificial Intelligence, and City Science. On top of it, adaptive services are built, that tailor input interfaces, content and its representation to different generations and abilities of citizens.

Safe Athens

The strategic plan for Safe Athens envisions the development of innovative services for both the administration and the citizens, such as e-Services, public safety, and access to municipal assets, including in-house developments and external providers.

Consortium

Project factsheet

Start date: 01/09/2024
Duration: 36 Months
Budget: 7 308 925.00 €
Programme: HORIZON-CL3-2023-CS-01-01

Project coordinator: Matteo Repetto (CNR/IMATI)

Technical coordinator: Georgios Koutsimpiris (Space Hellas)

info@mirandaproject.eu

Follow us

@mirandaprj https://www.mirandaproject.eu MIRANDA EU project

This project has received funding from the European Union's Horizon Europe Research and Innovation programme under grant agreement No. 101168144

Figure 15. First version of the MIRANDA roll-up.

2.7.4. Presentation

According to the Communication plan, the initial effort is especially addressed to raise the attention of operators of digital services. A first presentation has therefore been prepared to present existing issues to technical people who are not cyber-security experts (e.g., technology providers, cybersecurity vendors, business associations). It was explicitly designed not to bring technical content but to present the main issues with simple, intuitive, and informal language. The presentation uses graphics and animations and will also be used to prepare the first communication video to maintain consistency in the messages and visual forms. A few screenshots from the presentation are shown in Figure 16. It is worth noting the usage of the MIRANDA ideogram to maintain a discreet visual identity across the slides.

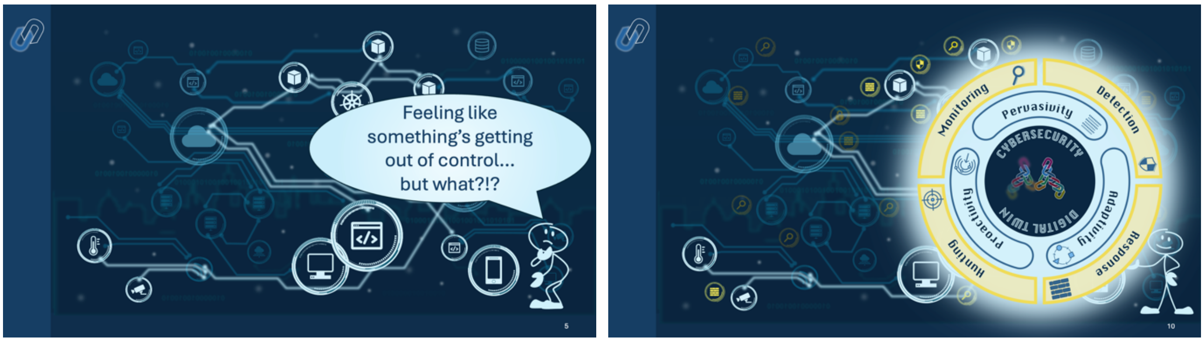


Figure 16. Screenshots from the MIRANDA presentation.

2.7.5. Website

The project website is the main landing point for visitors who want to know more about MIRANDA. It was designed with accessibility in mind to help visitors identify where they could find the information/material they are looking for.

In the project's first phase, the website will only host an extended description of the project's objectives, concept and approach, and preliminary dissemination material. As soon as deliverables and concrete results are available, they will be inserted into the website as direct or indirect downloads (e.g., links to the GitHub repository).

The MIRANDA website was developed with WordPress, including Web 2.0 features accessible through smartphones and tablets. It runs the necessary plugins to be GDPR compliant and to keep track of visits so that statistics about its impact can be derived later on.

The website has a home page with the following content:

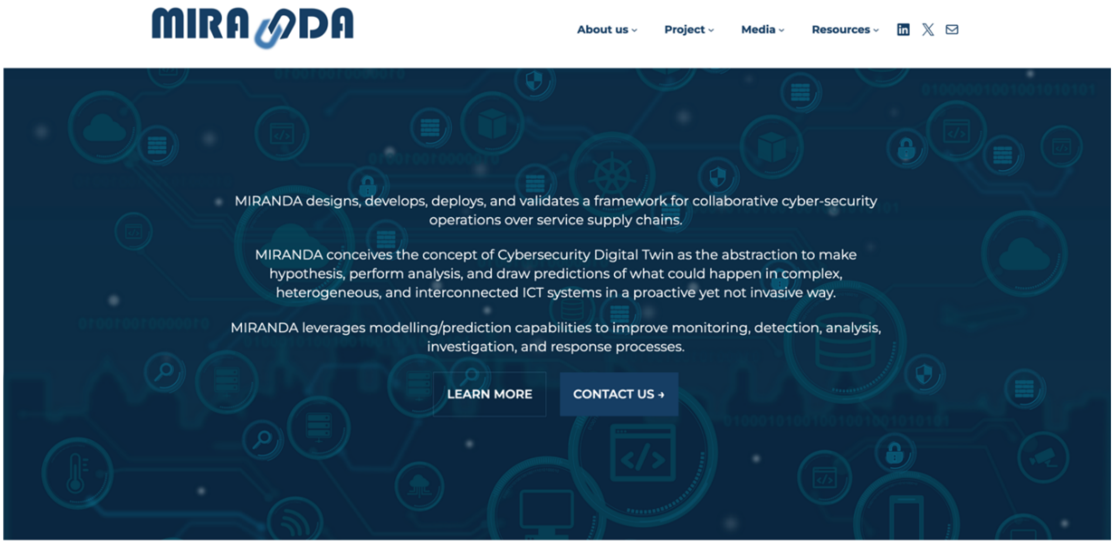
- Menu to access more specific pages
- Link to social media
- Contact email
- Key messages
- Acknowledgement to the funding entity and disclaimer

The rest of the site is structured in the following way:

- **About**: This section contains the main information about the consortium and the project as a whole, namely:

  - **Project** factsheet: key facts about the project (Horizon Europe call, number of partners, funding);
  - **Consortium**: the list and logos of all partners;
  - **Contact us**: contact details (project/technical coordinators, email).
- **Project**: This section contains the technical description of the project in terms of:
  - **Objectives**: what the project is pursuing;
  - **Concept**: why the project is addressing specific issues;
  - **Approach**: how the project implements its objectives.
- **Media**: this section collects all communication material about the project:
  - **Press releases**;
  - **Flyers/Leaflets**;
  - **Posters/Roll-ups**;
  - **Presentations**;
  - **Videos** (still not available).
- **Resources**: this section is intended to deliver the main outcomes and results from the project, including:
  - Technical public **deliverables**;
  - Open-source **software** (still not available).
- **Cookie policy**: stating the EU policy

New sections will be added according to the project's evolving needs, and the revised Communication plan will be elaborated on M18.

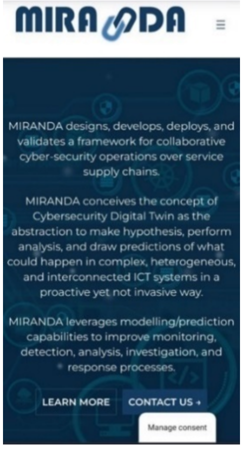


MIRANDA designs, develops, deploys, and validates a framework for collaborative cyber-security operations over service supply chains.

MIRANDA conceives the concept of Cybersecurity Digital Twin as the abstraction to make hypothesis, perform analysis, and draw predictions of what could happen in complex, heterogeneous, and interconnected ICT systems in a proactive yet not invasive way.

MIRANDA leverages modelling/prediction capabilities to improve monitoring, detection, analysis, investigation, and response processes.

Figure 17. The home page, as it pops up in conventional web browsers.



MIRANDA designs, develops, deploys, and validates a framework for collaborative cyber-security operations over service supply chains.

MIRANDA conceives the concept of Cybersecurity Digital Twin as the abstraction to make hypothesis, perform analysis, and draw predictions of what could happen in complex, heterogeneous, and interconnected ICT systems in a proactive yet not invasive way.

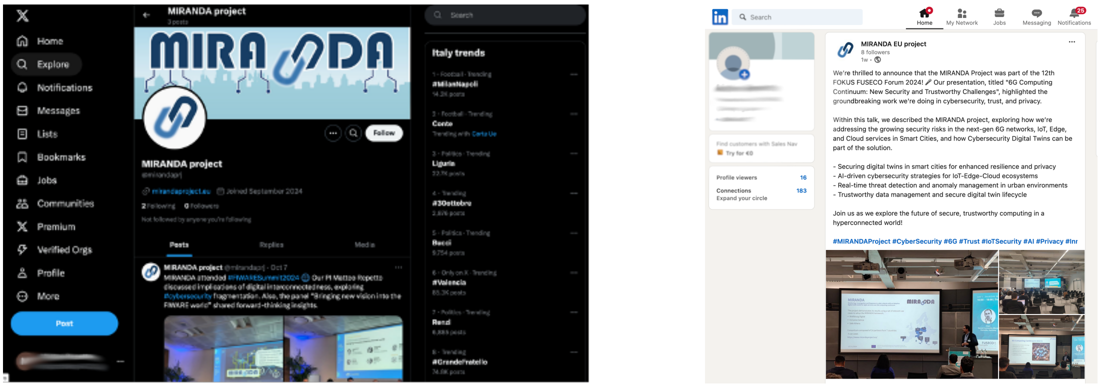
MIRANDA leverages modelling/prediction capabilities to improve monitoring, detection, analysis, investigation, and response processes.

Figure 18. The web page appearance on mobile devices.

2.7.6. Social media

X and LinkedIn accounts have been created for the project. The X account will be used to deliver very short messages about the project itself and relevant topics (sister projects, events, discussions). It is intended to reach the broadest audience, both technical and non-technical people. The LinkedIn account will give more detailed insights, especially on technical or business matters, to establish the project positioning and foster discussion.

The Communication leader (CNR) will maintain and enrich the social media channels according to the project's course of action and ongoing project activities and ensure the collection of relevant material and information from all partners. All partners are committed to contributing to social networking, and they will be given the opportunity, in turn, to lead the preparation of messages of their interest for an entire month. CNR will coordinate the publication on social media dynamically and proactively, also according to related events and initiatives in the MIRANDA community.



MIRANDA project

miarandaproject.eu Joined September 2024

2 Following 0 Followers

MIRANDA project @mirandaprj · Oct 7

MIRANDA attended #FIWARESummit2024 🌐 Our PI Matteo Repetto discussed implications of digital interconnectedness, exploring #cybersecurity fragmentation. Also, the panel "Bringing new vision into the FIWARE world" shared forward-thinking insights.

MIRANDA EU project

8 followers

1w ·

We're thrilled to announce that the MIRANDA Project was part of the 12th FOKUS FUSECO Forum 2024! 🎤 Our presentation, titled "6G Computing Continuum: New Security and Trustworthy Challenges", highlighted the groundbreaking work we're doing in cybersecurity, trust, and privacy.

Within this talk, we described the MIRANDA project, exploring how we're addressing the growing security risks in the next-gen 6G networks, IoT, Edge, and Cloud services in Smart Cities, and how Cybersecurity Digital Twins can be part of the solution.

- Securing digital twins in smart cities for enhanced resilience and privacy
- AI-driven cybersecurity strategies for IoT-Edge-Cloud ecosystems
- Real-time threat detection and anomaly management in urban environments
- Trustworthy data management and secure digital twin lifecycle

Join us as we explore the future of secure, trustworthy computing in a hyperconnected world!

#MIRANDAProject #CyberSecurity #6G #Trust #IoTSecurity #AI #Privacy #Inr

Figure 19. X and LinkedIn accounts for MIRANDA.

2.7.7. Press release

An initial press release template has been prepared by CNR and delivered to partners for replicating in other countries and languages. The template includes:

- An initial part which announces the kick-off of the MIRANDA project. Each partner is expected to tailor this part, describing its involvement in the project.
- A main part which describes the project concept and objectives simply, that could be understood by non-technical people.
- The final part provides the contact information.

3. Dissemination

This section provides information on planned dissemination activities. We first describe the objectives and scheduling of the dissemination activities. We then identify relevant stakeholders and audience groups. We describe each dissemination activity and state initial dissemination strategies and short-term plans. Finally, we state the KPIs of the dissemination activities.

3.1 Objectives

Dissemination aims to maximize the mid-and long-term impact of the project. It is, thereby, essential to share the project results with the right audiences so that they can use the information effectively, even after the project has ended. We summarize the key objectives of the dissemination activities described in this document. In the following sections, these objectives are mapped to audience groups and dissemination activities:

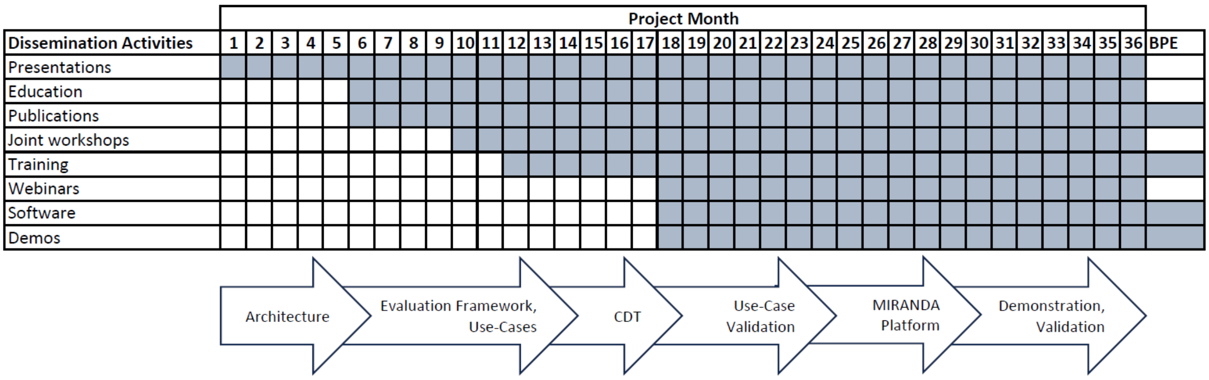
- **O1**: Ensure that project results (scientific findings, tools, etc.) are widely and openly available in a self-contained form (publications, software repositories) during and after the end of the project.
- **O2**: Draw the attention of key users (businesses, customers, stakeholders) to the project to facilitate cooperation or market exploitation in alignment with the project’s exploitation strategy. This has the positive effect of gaining direct feedback from users to understand their needs better and design the developed tools towards prevalent gaps.
- **O3**: Influence policies, guidelines, and standards based on the insights gained during the project.
- **O4**: Establish a foundation of research results and facilitate knowledge transfer, allowing future research endeavours or business initiatives to build upon the fostered knowledge efficiently.
- **O5**: Ensure accountability and transparency of the conducted research for reporting to stakeholders and funding agencies.

3.2 Dissemination Plan

This section provides the dissemination plan. It first describes which dissemination activities are used at which stage in the project to share results with stakeholders effectively. Moreover, it describes the target audience groups and map them to specific dissemination activities and objectives.

3.2.1. Schedule of Dissemination Activities

Effective dissemination implies that adequate dissemination activities are used at the right time. Moreover, specific content suitable for that type of dissemination is required depending on the type of dissemination activity. Since certain artefacts, such as code or data, are not available from the beginning of the project but are rather generated in the course of the project and the respective work packages, the dissemination activities are arranged in a staggered manner, as depicted in Figure 20, which shows the dissemination activities in the rows and the project months in the columns and indicates the start and end of each activity through colored boxes. Note that some of the activities last beyond the project end (BPE); this refers to activities that generate standalone artefacts that are available in a useful format indefinitely (in particular, publications printed in proceedings that are openly accessible online) or artefacts that can be adopted and modified by the community, such as code that is released on a public platform.



	Project Month																																				
Dissemination Activities	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	BPE
Presentations	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	
Education						▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	
Publications						▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
Joint workshops										▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	
Training												▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
Webinars																		▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	
Software																		▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
Demos																		▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨

Architecture
Evaluation Framework, Use-Cases
CDT
Use-Case Validation
MIRANDA Platform
Demonstration, Validation

Figure 20. Schedule of Dissemination Activities (BPE = Beyond Project End)

The figure also shows how the different stages of the project relate to dissemination activities. In the first stage of the project, where the requirements and architectures are defined, it is only possible to hold presentations on the high-level project scope due to the lack of any more technical insights that have yet to be researched at that point in time. Starting from M6, when there is a clear picture of the overall system architecture and the consortium starts working on the technical work packages, evaluation framework, and use cases, it is possible to pursue the publication of results and transfer of knowledge. From M10 on, the consortium plans to get in touch with other project consortia working on related projects in the cyber security domain for the purpose of knowledge exchange. Starting in M12, when an initial version of the MIRANDA platform is available, training on the Cyber Digital Twin (CDT) will be conducted. At a later stage, training will take place on the fully integrated MIRANDA platform M18 marks the start of all remaining dissemination activities: webinars that enable training and knowledge transfer on a large scale, also focusing on industrial and governmental settings in addition to technical security teams: software and data that are published as open-source tools in documented form on public platforms; and demonstrations of the integrated MIRANDA platform and case studies to stakeholders.

3.2.2. Targeted audiences

For effective dissemination, it is essential to share relevant project results with those stakeholders interested in the respective findings in a way that has the highest benefit for them. Accordingly, it is important to map the dissemination activities mentioned in the previous sections to certain groups of audiences. We generally differentiate between three main channels of dissemination:

- **Scientific dissemination**. This channel aims to provide output of scientific relevance, such as conference publications, journal papers, concepts, open-source code, and data sets, to academics such as researchers, universities, companies with research departments, students, etc.
- **Industrial dissemination**. This channel aims to provide technologies and other output that businesses can use, such as platforms, tools, documentation, and policies, to companies, industries, and all other key users and stakeholders interested in the MIRANDA project.
- **Education and training**. Other than the scientific and industrial dissemination channels, this channel focuses on transferring knowledge from the project consortium to stakeholders, particularly potential users, students, security professionals, and use case providers.

These channels may be further split up into specific audience groups. Table 3 provides an overview of the considered audience groups and maps, in addition to dissemination means, the related objectives stated in Section 3.1 to each group.

Table 3. Relevant dissemination activities and objectives for different audience groups

Audience Group	Primary dissemination activities	Related objectives
Researchers, academia, the scientific community	Publications, education, joint workshops, software	O1, O4, O5
Businesses, Technology providers for smart cities	Training, webinars, demos, software	O2, O3, O5
Security teams, cyber security professionals	Software, training, webinars	O2
Policy makers, decision-makers	Demos, joint workshops	O2, O3
Standardization bodies	Publications, joint workshops	O1, O3
General audience	Presentations	O2

3.2.3. Coordination of Work within the Consortium

Successful dissemination requires the collaboration and involvement of all partners. Remote teleconferences will be conducted during the regular virtual general assembly meetings. Dedicated sessions on WP6 will be scheduled throughout the project's runtime, and the status and action points of active tasks will be discussed in the entire consortium as they affect all partners. In case specific topics need to be discussed, for example, planning activities or preparation of deliverables, dedicated telcos will be scheduled with the involved task leaders and other relevant participants to ensure efficient completion. The consortium also welcomes joint publications of two or more partners. If necessary, T6.2 will support joint work on publications by providing access and advice for relevant platforms for collaborative paper writing.

For every dissemination activity mentioning MIRANDA, the shared Dissemination Activity Form (Annex 1: Communication and Dissemination Activity Forms) should be completed at least 2 weeks after the event. Information collected on this form will be used for reporting purposes and to ensure that all target groups are effectively reached and that all dissemination activities within MIRANDA are reported to the EC. In addition, suitable artefacts, particularly presentations (or those parts of a presentation regarding MIRANDA), must be shared with the project partners through the dissemination folder at MIRANDA's project SharePoint.

3.3 Dissemination Activities

This section describes the dissemination of the activities in detail and provides suggestions for possible dissemination targets.

3.3.1. Participation in Conferences, Forums and Events

Participation in external events, conferences, and fairs will also be addressed to boost the visibility of the Consortium and its results. The Project foresees participation in at least 12 international conferences and fairs, ensuring that all relevant stakeholder groups will be exposed to MIRANDA's messages. All partners are encouraged to seek opportunities to increase the project's impact through presentations about MIRANDA at external events. PowerPoint presentations should use the specially developed MIRANDA PowerPoint templates available in the MIRANDA Template folder on the project's online SharePoint. Where appropriate, presentation content will be developed in close cooperation with the Coordinator or the relevant Work package leaders to ensure accuracy and consistency across the project as a whole.

Given that conference publications require a substantial amount of novel, scientifically sound content, they are only expected to be published starting from M6, at this point, technical work packages are assumed to have already sufficiently progressed to yield new approaches beyond the state-of-the-art. However, we expect that the initial preparation and design of the concepts presented in these papers start earlier than M6 since system requirements and architectures are already defined before the start of the technical work packages. Contrary to fully scientific conferences, speeches and presentations at forums and events do not require technical depth but aim to spread awareness about the project through higher-level discussions, such as use cases. Accordingly, presentations at such venues will be pursued starting from M1.

There are also differences between scientific and industrial venues in terms of audience. In particular, scientific conferences primarily target the audience of researchers and academia. The selection of conferences targeted by the academic partners of the consortium will be based on their topics of interest as well as their ranking. High-ranked conferences are preferred since they provide greater reach and higher visibility of published results. At the same time, conferences with a specific focus on the key topics of the MIRANDA project, such as intrusion detection and prevention, security for smart cities, threat modelling, and supply chain security, provide an excellent platform to reach the desired target audience. On the other hand, the selection of relevant forums and events will be based on the exhibitors and participants. In particular, technology providers for smart cities, as well as other industry and business stakeholders in the cyber security domain, are regarded as key stakeholders that are interested in the results of the MIRANDA project and capable of providing beneficial insights for the consortium, thereby creating synergies and fostering collaboration between academia and industry. Table 4 presents an initial and non-exhaustive list of conferences selected as potential targets for scientific publications at conferences. The table also states some key topics in the calls for papers extracted from the respective conference websites that are highly relevant to the MIRANDA project. The list of venues is non-exhaustive because there are many conferences on security topics and submission deadlines throughout the year. Generally, the consortium pursues publication at renowned conferences (Tier 1 - Tier 2[5] or A* -A[6] based on the ranking system used) since they usually enable higher visibility in the community, higher scientific impact, and are more likely to yield high-quality reviews and feedback useful for the project. Several technical developments planned in the project, such as detection algorithms, are suitable for publication at such venues. However, we recognize that several topics researched as part of the project, such as use cases, are more suitable to be presented in workshops as positioning papers comprising more high-level concepts without the need to go into technical details.

Table 4. Initial list of scientific conferences and relevant topics of interest

Name	Selected topics of interest
European Symposium on Research in Computer Security (ESORICS)	Intrusion Detection, Security and Privacy in the IoT and Cyber-Physical Systems, Access Control
IEEE International Conference on Software Quality, Reliability and Security (QRS)	Cloud Computing and Smart City, AI-based Techniques for Software Quality, Reliability, and Security, Natural Language Processing and Large Language Models
IEEE Symposium on Security and Privacy (IEEE S&P)	Distributed systems security, Attacks with novel insights, techniques, or results, Intrusion detection and prevention
International Symposium on Research in Attacks, Intrusions and Defenses (RAID)	Intrusion detection and prevention, Computer, network, and cloud computing security, Cyber-physical systems security and threats against critical infrastructures, IoT security
Annual Computer Security Applications Conference (ACSAC)	Hardware and Supply Chain Security, Resilience, Machine Learning Security, Application Security, Cloud and Virtualization Security
Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)	Vulnerabilities in decentralized systems Result in correlation and cooperation, Targeted attacks, Operational experiences
ACM/SIGAPP Symposium On Applied Computing (SAC)	Smart Cities and Critical Infrastructures, Data Spaces and Trusted Data Sharing, Knowledge and Natural Language Processing,

[5] https://people.engr.tamu.edu/guofei/sec_conf_stat.htm
[6] https://portal.core.edu.au/conf-ranks/

Usenix Security Symposium	Cloud computing security, Intrusion and anomaly detection and prevention, Network infrastructure security, Cyber-physical systems security, Embedded systems security, Secure computer architectures
ACM Conference on Computer and Communications Security (CCS)	Software Security, Web Security, Network Security, Hardware, Side Channels, and Cyber Physical Systems, Applied Cryptography
ACM ASIA Conference on Computer and Communications Security (AsiaCCS)	Real-world aspects of security and privacy
World Forum on the Internet of Things (WF-IoT)	AI/Machine Learning Technologies; Cybersecurity, Security, Privacy, and Trust; Digital Twins in IoT Applications; Transportation, Connected Vehicles, and Multi-modal Systems
IEEE International Conference on Network Softwarization (NetSoft)	Network virtualization, Network and cloud security, Resilience, reliability, and robustness of softwarized networks
IEEE International Conference on Computer Communications	Artificial Intelligence/Machine learning for networking, Cyber-physical network systems, Network security and privacy

The consortium also plans to organize scientific conferences and workshops themselves. POLITO, with the collaboration of CNR, is planning to organize the 7th International Workshop on Cyber-Security in Software-defined and Virtualized Infrastructures (SecSoft) in conjunction with the 11th IEEE International Conference on Network Softwarization (NetSoft) in June 2025, Budapest. This venue will be an excellent opportunity to disseminate early results from the project in the form of publications and spread information about the MIRANDA project to an international scientific audience.

In addition to scientific conferences, MIRANDA aims to reach an audience outside the scientific area through active participation in fairs and exhibitions. The primary target audience comprises end users, businesses, technology providers for smart cities, policymakers, and decision-makers. Table 5 displays an initial and non-exhaustive list of industrial events and forums that interest the project, particularly to spread knowledge about the novel technologies currently developed within the project. From the websites of these conferences, we list the topics of interest most relevant to the project in the table.

Table 5. Initial list of forums and events and relevant topics of interest

Name	Selected topics of interest
InfoSecurity Europe	Cybersecurity Legislation, Ransomware, Crisis Management, Digital Security by Design

InfoSec World	Ransomware Impact, Protection, and Recovery, Red Teaming, Cyber-Resilience Strategy for Operational Survivability, Security Automation
European Cybersecurity Forum	New technologies to address digital challenges in cyber security, shaping public policies, contributing to the development of concrete strategies and solutions
EU Cyber Security Conference	Security by design, supply chain integrity, Artificial Intelligence
Smart City fairs (e.g., GAIA-X Summit)	Trusted decentralized digital ecosystems, Federated and Secure Data Infrastructure
Security BSides	Innovative attack/defense strategies, Virtualization and cloud computing, Opensource software, Network Security & Cryptography
IKT Sicherheitskonferenz	Cloud security, cyber situational awareness, intrusion detection and classification, cyber exercises, OT security, legal aspects
EuCNC	Network digital twins for AI/ML, Security threats for AI/ML, Network security and cybersecurity trends, Critical communications and public safety
Italian Conference on Cybersecurity (ITASEC)	AI and Cybersecurity, Information Security, Infrastructure Security, Software and Platform security, Attacks and defense models and methods
CCGRID 2025 – IWOSEMCS Workshop	New topics on cybersecurity in mobile applications, smart systems, data and information management, vulnerabilities of AI-based systems
ECMS 2025	New models and simulators of secure, intelligent systems

3.3.2. Open-access Publications

Like conference publications, open-access journals require substantial amounts of scientifically novel insights that go beyond the state of the art; accordingly, publications of that depth and quality are only expected to be feasible starting from M6. MIRANDA project expects at least 8 publications in international scientific Journals. The consortium commits to Open Science and thus pursues publishing all accepted publications with Gold Open Access to reach the broadest possible audience. Examples of relevant journals and publications are stated in Table 6, which also displays some of the key topics extracted from the journal website and considered relevant for the work conducted in the MIRANDA project. Depending on the specific tool or matter covered in the respective publication, some of the listed journals might be more relevant than others; the respective authors should make the final decision. The list of journals is non-exhaustive because many journals focus on security topics or other topics related to the project's scope. However, the consortium generally targets high-ranked journals of well-known publishers such as ACM, IEEE, Elsevier, or Springer.

Table 6. Initial list of journals and relevant topics of interest

Name of the Journal	Selected Topics of Interest
Springer International Journal of Information Security	Security Infrastructures, Intrusion Detection, Tamper Resistant Software, Applied Cryptography.
Elsevier Computers & Security	Computer security, audit, control and data integrity in industry, commerce and academia.
ACM Transactions on Privacy and Security	Security Technologies, Fundamentals, Secure Systems, Privacy Methods, Security and Privacy Applications, Privacy and Security Policies.
IEEE Transactions on Reliability	Reliability for systems of systems, network availability, mission success, safety.
ACM Transactions on Intelligent Systems and Technology	Artificial Intelligence Systems that offer important Services in the real world.
IEEE Transactions on Dependable and Secure Computing	Intrusion detection and tolerance, Cyber-Physical Systems, Threat-assessment and intrusion-detection models, Fault-tolerant, secure, and safe middleware.
IEEE Transactions on Network and Service Management	Service Provisioning, Reliability and Quality Assurance, Information and Communication Models, Policies, Applications and Case Studies.
Elsevier Sustainable Cities and Society	Smart cities and resilient environments, smart grid and intelligent infrastructure, Critical infrastructure protection, including security, privacy, forensics.
IEEE Internet Computing	Distributed computing, security, privacy, and trust.
Elsevier Journal of Information Security and Applications	Security management and policies, Network and mobile security, Hardware and physical security, Cryptographic protection.
ACM Digital Threats: Research and Practice	Network security, Adversary tactics, Threat landscape studies, Adversary attack patterns, Threat information management and sharing.
IEEE Access	Cloud, Edge and Virtualization; Edge Intelligence for Internet of Things; Cybersecurity Digital Twins; Security, Privacy, and Trust Management in Smart Cities.
Computer Networks	Communication protocols, Network Security and Privacy.
ACM Computing Surveys	Comprehensive, readable surveys and tutorial papers on recent developments in security and management of intelligent scalable ICT systems.
IEEE Transactions on Services Computing	Secure services-oriented research and technologies.

3.3.3. Joint Workshops

Several other research projects are investigating intrusion detection, digital twins, and attack emulation. While these research projects target various other use cases than smart cities, the insights into specific technologies, comparative studies of approaches, and ideas for novel solutions can greatly benefit the MIRANDA project. In particular, exchanging experience reports and ideas with other research projects could foster the development of new technologies that are relevant even beyond their intended scope, speed up the decision-making process for use cases, and avoid redundancies.

Starting from M10, the overall system requirements and use cases will have been defined, and we will have a good idea about the upcoming technical developments since all technical work packages are progressing, so we plan to conduct at least four joint workshops with research projects to facilitate information exchange. Table 7 lists an initial enumeration of projects suggested by members of the consortium to be contacted for such workshops.

Table 7. Initial list of journals and relevant topics of interest

Project Name (Funding)	Project Summary	Relevance to MIRANDA and possible Synergies
NEWSROOM (European Defence Fund, GA no. 101121403)	Improve Cyber Situational Awareness (CSA) through an integrated platform, research on Collaborative Intrusion Detection Systems (CIDS) and Cyber Threat Intelligence (CTI), evaluations in cyber range environments.	Simulation of IT/OT and attacks in cyber ranges is related to cyber digital twins, common algorithms for (FL/TL-based) intrusion detection, attack classifications, and CTI sharing.
RIGOUROUS (HORIZON-JU-SNS-2022 GA no. 101095933)	The RIGOUROUS project aspires to identify and address the major cybersecurity, trust and privacy risks threatening the network, devices, computing infrastructure, and next-generation services.	Digital City Twining Platform Use Case aims to secure the communication between the IoT gateways and the platform's microservices running at the cloud's edge and among the microservices running across multiple (edge) clouds.
NERO (European Cybersecurity Competence Centre GA no. 101127411	NERO is an advanced Cybersecurity Ecosystem designed to address the distinct aspects of cybersecurity awareness, training, and education. It comprises five interrelated frameworks and offers a bespoke Cybersecurity Awareness programme.	Addressing the increasing number and sophistication of cyber threats and their potential to harm individuals and organizations. Aiming to reduce the awareness gap with cybersecurity solutions Demonstration includes use case in transportation sectors.

6G-PATH (Smart Networks and Services Joint Undertaking GA no. 101139172)	The 6G-PATH goal is to help foster the further development and integration of new and improved tools and products from EU companies with 5G/6G while also measuring relevant key performance indicators (KPIs) and key-value indicators (KVIs).	Fosters the development and integration of tools and products with 5G/6G. Use cases and trials include security coordination in smart cities, providing mission-critical communication utilizing 5G and 6G technologies for first responders, emergency response and inter-agency collaboration.

Historically, joint workshops among research projects often occur as part of scientific conferences. The 7th International Workshop on Cyber-Security in Software-defined and Virtualized Infrastructures (SecSoft), which takes place in conjunction with the 11th IEEE International Conference on Network Softwarization (NetSoft) and is organized by POLITO in collaboration with CNR, is a suitable venue for such a gathering of members of several research projects. The workshop will take place in June 2025 in Budapest and will be targeted for a joint workshop with some of the aforementioned projects.

In addition to workshops with research projects, requirements analysis workshops are planned to be carried out as part of T2.3, which Space Hellas leads. These workshops should involve all stakeholders relevant to the discussion topics, such as end users, technology providers, legal experts, and external stakeholders. The main idea behind these workshops is that the consortium receives direct feedback from key users of the MIRANDA platform as well as compliance with expectations and regulations.

3.3.4. Open-source Software and Open Data

The MIRANDA consortium is committed to Open Science, meaning that in addition to a gold open access model for publications, we pursue the release of all software and data that is useful to the wider community and where no restrictions regarding commercial products are in place on a public platform as open-source code and open data. This is in line with the EU's open science policies. The endeavour of publishing source code requires that functional and validated tools are available; accordingly, this activity is only expected to occur from M18 forward, at which point the tools for the initial version of the MIRANDA platform are developed, and the platform itself is assembled. This project's dissemination strategy for source code proposes to publish both standalone tools and an integrated platform in a Community Edition. There are several benefits from such a strategy, among which are the following:

- Increase visibility of the project and its outcomes. Code repositories such as GitHub, as well as code repositories such as Zenodo, are easily found through Internet search machines; thus, providing open-source code for relevant problems and open data for evaluations in the security domain increases the chance of externals working on similar topics to come across the MIRANDA repositories and thus learn about the project.
- Artifacts are a valuable contribution to scientific publications. Reproducibility of results is essential for sound scientific work, and providing working examples as open access

codes, as well as open data for the basis of evaluations accessible with low entry barriers, is vital to allow others to use and extend novel approaches. Many top tier conferences have thus recently established artifacts track and invite authors of accepted publications to have their source code evaluated. Positive evaluations are usually acknowledged by the publishers, further increasing the visibility of the paper and the technology.

- Facilitate collaboration and interaction with the community. Anyone may contribute to the published tools and create forks for projects that require adaptations. Many security professionals regularly contribute to open-source tools, improving the software and making it more suited for wide-range use in real-world use cases. Crowdsourcing, in particular, is the strategy that is being pursued for cyber-digital-twin software.
- Permanently storing software components even after the end of the project. Given that code repositories such as GitHub and data repositories such as Zenodo are independent from the context of the project and store all published code and data indefinitely, there is no need to be concerned about providing long-term storage from within the project itself. All published code and data will be documented to be useful as standalone tools, enabling future research projects to leverage new developments.

Overall, the strategy is to publish the developed software of the project in a common MIRANDA GitHub repository as a Community Edition; however, a selection of tools should also be published as standalone repositories so that it is easier for others to take up these technologies for other platforms or use-cases, or just to replicate some results described in a publication that introduced the respective algorithms. To a certain extent, publishing services or testbeds could also be required as part of the code. While it is generally impossible to share a running testing environment through platforms such as GitHub, it is common to provide scripts for automatic software setup and configuration to recreate technical infrastructure that enables such evaluations easily. Publishing tools that support threat emulation may also be necessary to repeat validations. However, restrictions regarding publishing software that could be used for malicious activities could prevent the consortium from fully publishing certain pieces of software. Because, at this moment, it is not possible to estimate the full functionality of the tools that will be developed in the course of the project, this matter will be evaluated once the tools are ready, and a decision will be made based on standard and EU guidelines and policies.

The MIRANDA consortium committed to publish at least three data sets containing traces of multi-step attacks as open data. To enable others to gain the most out of these data sets, they will be published with a full description of the context of the collection, the involved service chains, configurations of services, and documentation. The traces should contain raw log data collected from systems and applications, network traces, labels for attack cases to facilitate evaluations, and contextual data if necessary. The data will be checked for sensitive content before publishing to ensure that only anonymized data is handled. The consortium will align these activities with the EU Data Strategy, which proposes collecting data from testing environments in standard formats and publishing them on open data repositories using FAIR principles. The exact license for publishing source code and data will be described in the Data Management Plan.

3.3.5. Presentations and Demos

In addition to presentations that are held as part of paper publications at scientific conferences, the consortium also plans to present the project's outcomes to industrial stakeholders, municipalities, and other end users. The purpose of this dissemination activities includes the increase of the awareness of relevant stakeholders about the project's outcomes, the gathering of feedback from stakeholders and kickstarting of collaborations that can go beyond the project and the generation of impact by fostering the adoption of MIRANDA's technologies in commercial products. The presentations are designed towards specific audiences that are present on each occasion. However, the presentation activities are generally suitable for reaching broad audiences, ranging from industries and providers to policymakers and academics. The contents of the presentations will also be selected in such a way as to meet the needs and expectations of the respective audience groups. Accordingly, the presentations could focus on specific tools developed as part of the project when technology providers working on related products attend the presentation. Still, they could also be more high-level and focus on the current gaps in industrial practice and the MIRANDA platform when addressing the presentation to decision-makers. Since the concept and use cases can be highly relevant for certain stakeholders, the dissemination activity focusing on presentations can start in M1. In the course of the project, the implementation of the platform and specific tools will be the main topics of the presentation. In contrast, evaluations of the platform will be the main content towards the end of the project. Following this strategy, this dissemination activity lasts until the end of the project in M36.

Demonstrations are closely related to presentations. In many cases, demonstrations will be held as part of presentations. However, following the overall project plan, the consortium expects it will take until M18 to have sufficient insights, technologies, and concepts ready for demonstration. Accordingly, the demonstration activity will only start in M18. Similar to presentations, the demonstrated technologies will be selected based on the expectations and needs of the audience and shaped based on the format of the venue. In particular, demonstrations can range from very low-level and hands-on displays, for example, diving into the collected data and running analysis scripts on them to yield quantitative results, to high-level demonstrations that show the platform's features and automated workflows supporting operators in their decision-making. Demonstrations will also be recorded for repeated screenings; this makes it easier to distribute the demonstrations on a larger scale as they can be simply provided over online communication and on-demand basis. Another advantage is that these videos will be available even after the end of the project, which means that they can be useful to technology providers and other stakeholders adopting MIRANDA's technologies in the future.

3.3.6. Education

Novel algorithms and concepts are developed with scientific methodologies as part of MIRANDA. This is an ideal situation to educate young researchers, particularly those pursuing a Master's or PhD degree in the research areas of digital twins, cyber security, intrusion detection, threat modelling, etc. POLITO and CNR are planning to organize summer schools and seminars for students with topics correlated to the MIRANDA project. The main audience planned for these activities is the full student body of the Master's degree in Cybersecurity at the Polytechnic University of Turin (Polito). Organizing such workshops and lectures generates many synergies for the project. First, the tools and concepts developed within the project are distributed among academics, raising awareness that can spread even beyond the audience of these summer schools. Second, through workshops where the students are tasked with challenges relevant to the project, new solutions and innovative ideas could be generated and brought into the project. Third, the project members organizing these workshops will obtain direct feedback about the project’s findings, results, and their relevance to the scientific community. Fourth, summer schools are an excellent opportunity to find highly capable young researchers interested in the project's topics and prove their motivation to contribute. As such, summer schools and seminars facilitate hiring new employees with in-depth knowledge about the project through workshops. Moreover, students searching for topics for their Master’s or PhD theses attending summer schools or seminars may decide to join the project temporarily and conduct research on one of the topics.

The consortium is committed to enabling students to complete their Master's or PhD theses during the project and even stated this in the list of key performance indicators. This is accomplished by identifying mostly isolated tasks, such as the development of a novel analysis method or creation of a data set, shaping the problem statement to be suitable for a Master’s thesis, and providing students just the information that is required to fulfil that task under the supervision of project members. This ensures that students are not overwhelmed by the developments in the entire project and provides them with the space to focus on their contributions. Furthermore, presentations of results in the consortium act as a useful feedback mechanism to the students, who can train to defend their thesis and critically reflect upon their contributions in the light of the use cases. PhD students, on the other hand, PhD students are involved in the project over a longer time span and may be directly engaged with specific tasks or work packages fitting their area of research. This provides these students not just deep insights into theoretical concepts but also a stage to interact with international researchers and get acquainted with the processes and schedules of an international research project, which is invaluable for their future careers as a scientist. This activity starts at M6 when work in technical work packages starts, and students can be ideally integrated into the project team.

3.3.7. Training and Webinars

Knowledge transfer is one of the main objectives of the dissemination activities pursued in this project. Training is one of the primary means to achieve effective and long-lasting knowledge transfer. Other than education, which focuses on academic audiences, training is a more hands-on exercise primarily directed towards capacity building for security professionals who are some of the main users of the MIRANDA platform and the technologies developed during the project. Through early integration and interaction with these key personnel, the consortium can gain relevant insights into the requirements of important stakeholder groups, specifically regarding the design and capabilities of tools and platforms developed within the project. Training is planned to be held from M12 onwards because, at this point, the initial version of the MIRANDA platform and some tools are available, which are necessary for hands-on exercises. Throughout the remaining runtime of the project, the consortium will establish a persistent channel with the security teams of the use-case owners and continuously perform training. This ensures that, towards the end of the project, security teams can effectively use the MIRANDA platform and continue to do so even after the end of the project.

Webinars are virtual educational sessions combining the advantages of demonstrations, presentations, and hands-on exercises for knowledge sharing and skill development. Similar to training, security professionals are one of the target groups of webinars; however, given that webinars are remote exercises provided on-demand, they reach a wider audience and are, therefore, directed towards industries and agencies such as ENISA. Throughout the webinars, participants have the chance to engage with the presenters, for example, through Q&A sessions as well as live polls. At the end of the webinars, participants' satisfaction will also be evaluated to ensure that the benefit of all involved stakeholders is maximized in subsequent sessions.

3.3.8. Contributions to Standards

Uptake of MIRANDA technologies during and after the Project implementation is one of the main objectives pursued as part of the project. Regulatory and standardization aspects are essential to achieving this objective since fast and reliable integration through well-defined and commonly accepted interfaces and compliance with regulations and policies are essential to ensure that third parties are willing to use the technologies developed within the project. Any lack of adherence to such standards will create burdens for stakeholders, such as the need to adapt interfaces or convert data formats, which could lead to misfunction or to a situation where stakeholders do not adapt the technologies. Table 8 lists standardization bodies, potential contributions from the MIRANDA project, and the expected impact of such contributions on the market.

Table 8. Initial list of journals and relevant topics of interest

Standardization Body	Planned contribution	Expected Impact
ISO/IEC	The considerations taken as part of the project for the purpose of integrating tools for automated data processing and analysis into real-world smart city environments are of high value to stakeholders. The insights gained during MIRANDA are thus planned to contribute to respective standards, such as “Privacy protection — Privacy guidelines for smart cities (ISO/IEC TS 27570:2021)". Additionally, relevant standards from the 27000 family (e.g., 27001 for information security management, 27701 for privacy management, 27017/27018 for cloud security) and 29151 for protecting personally identifiable information (PII) will be considered to strengthen data privacy and security practices across the project.	High
IEC	IEC 62351 for industrial network cybersecurity, IEC 62443 for industrial automation and control system security, and IEC 62264 for integrating enterprise and control systems will support secure integration of MIRANDA’s Digital Twin and supply chain elements in critical infrastructure contexts.	High

CEN/CENELEC JTC 13	Develops European cybersecurity and data protection standards, ensuring harmonized compliance for MIRANDA's deployment in smart city environments. Relevant standards cover general cybersecurity and specific applications for urban and critical infrastructure.	High
OASIS Cyber Threat Intelligence TC	Standardized formats for describing cyber threat intelligence, such as those provided by Structured Threat Information Expression (STIX), are widely used to exchange threat information and facilitate automatic processing through machine-readable attributes. MIRANDA plans to contribute to these standards by extending the models with more context information.	Medium
OASIS OpenC2 TC	Standardized languages for command and control of technologies, such as OpenC2, have gained high traction recently and have become a common way to orchestrate cyber defence measures. Given that OpenC2 has a central role in MIRANDA, profiles and language extensions developed during the project will be added to the standard whenever applicable.	High
ETSI TC Cyber	The European Union has created the NIS directive to improve the cyber security postures of member states, covering a wide range of economies. With its focus on smart cities, MIRANDA can implement parts of the NIS directive.	High
TCG TPM Group	MIRANDA will work on methods for privacy-preserving attestation, which will contribute to the respective standards.	Low
European Self-Sovereign Identity Lab (SSI)	MIRANDA will work on TPM-based decentralized identities and contribute to the respective standards.	Low
ENISA (European Union Agency for Cybersecurity)	Provides best practices and guidelines for smart city cybersecurity and privacy, offering frameworks to enhance urban resilience. MIRANDA can use these as benchmarks to ensure adherence to evolving EU security and privacy regulations.	Medium

3.4 Target Key Performance Indicators and Expected Impacts

This section summarizes the key performance indicators (KPI) for dissemination activities.

Table 9 states for each dissemination action a quantitative KPI and the expected impact of reaching that KPI. Note that the project proposal stated the number of cumulative GitHub downloads (≥50) and documentation views (≥200) as a KPI; however, this metric is not adequate since it is not possible to reliably track downloads and views on GitHub. We, therefore, replace this KPI with the cumulative GitHub stars (≥100) and forks (≥10), which are measured automatically through GitHub and are a more common measure to compare the popularity of repositories. Specifically, every user account on GitHub can award any repository with at most one star to indicate their endorsement of the project. Forks, on the other hand, are copies of the repository that are commonly used to express interest in the project and are the first step in providing contributions through pull requests.

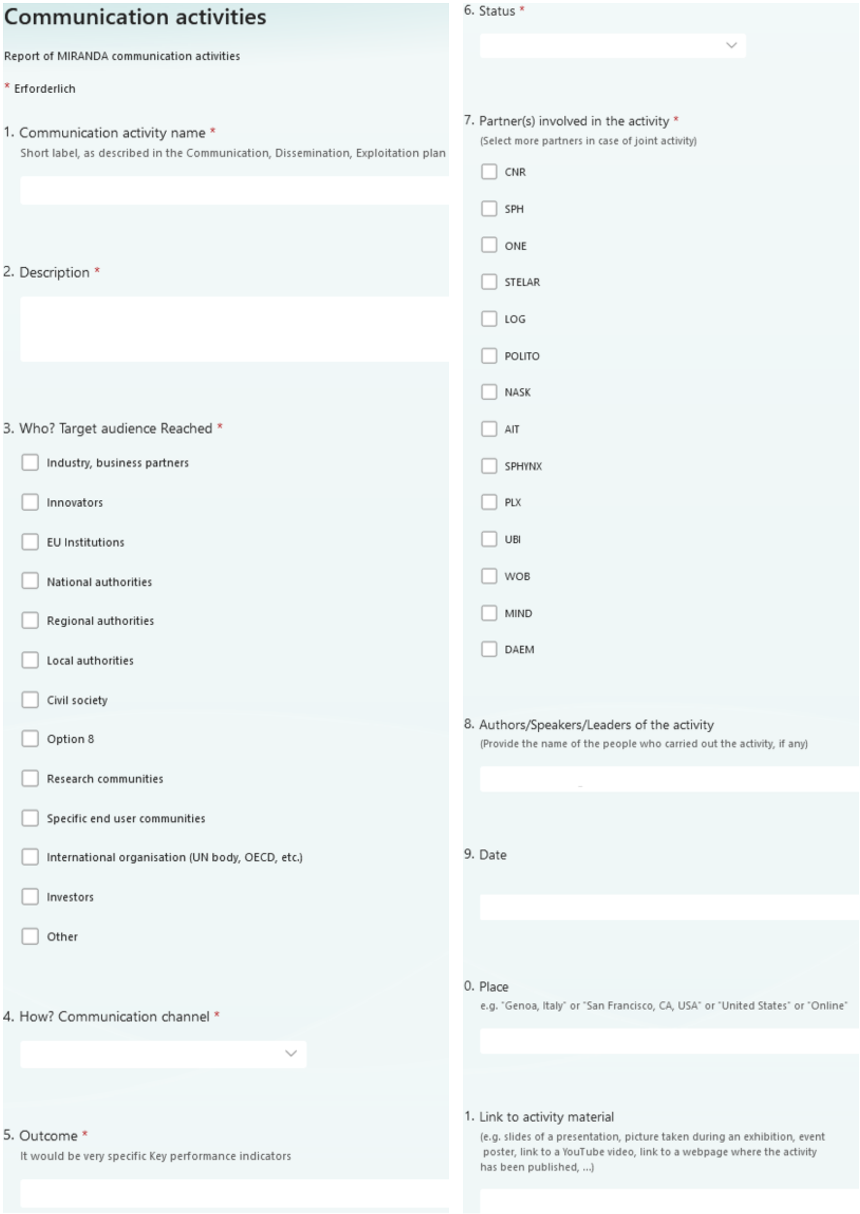
Table 9. Dissemination Key Performance Indicators

Action	Target KPI	Expected Impact
Cumulative GitHub stars/forks	≥100/≥10	Enhanced project visibility and community engagement Validation of project relevance and usability Increased collaboration and knowledge sharing Alignment with Open Science and Open Source Goals
Scientific papers in intl. journals/conferences	≥8/≥12	Increased project credibility and scientific recognition Dissemination of project results to a broad audience ranging from academics to professionals Increased opportunities for adoption of concepts by industrials or policies by decision-makers Alignment with Open Science and Open Access Strategies
Number of MIRANDA demos in events	≥12/≥6	Increased awareness and visibility of the project to relevant stakeholders Enhanced stakeholder engagement and feedback Facilitation of cooperation and partnerships Increased potential for commercialization
Organization of joint workshops with EU projects/attendees	≥4/≥200	Enhanced knowledge sharing of technical content and administrative matters Strengthening of the European Research Network through collaboration Facilitates the development of cross-sectional solutions
Webinars/Number of trained people	3/≥80	Increased and scalable knowledge transfer and capacity building Speed up and increase the likelihood of adoption of solutions by the industry Enhanced stakeholder engagement and directed design of solutions towards needs

No. of trained students	≥6 BSc/MSc, ≥4 PhD	Skill development of future researchers Gathering of innovative and new perspectives and ideas Increased potential of scientific dissemination through publications The likelihood of adoption of solutions in industries increases when students transfer to industry after completion of their thesis
Contributions to standards (profiles, extensions, algorithms, etc.)	≥6	Facilitate broad adoption and interoperability Increased recognition of project results in industrial practice and regulatory frameworks Create foundations for future research and development

4. Annex 1: Communication and Dissemination Activity Forms

This section contains the forms used to collect communication and dissemination activities within the project. Figure 21 shows the communication activities form, and Figure 22 shows the dissemination activities form accessible through the project's SharePoint.



Communication activities

Report of MIRANDA communication activities

* Erforderlich

1. Communication activity name *
Short label, as described in the Communication, Dissemination, Exploitation plan

2. Description *

3. Who? Target audience Reached *
- □ Industry, business partners
- □ Innovators
- □ EU Institutions
- □ National authorities
- □ Regional authorities
- □ Local authorities
- □ Civil society
- □ Option 8
- □ Research communities
- □ Specific end user communities
- □ International organisation (UN body, OECD, etc.)
- □ Investors
- □ Other

4. How? Communication channel *

5. Outcome *
It would be very specific Key performance indicators

6. Status *

7. Partner(s) involved in the activity *
(Select more partners in case of joint activity)
- □ CNR
- □ SPH
- □ ONE
- □ STELAR
- □ LOG
- □ POLITO
- □ NASK
- □ AIT
- □ SPHYNX
- □ PLX
- □ UBI
- □ WOB
- □ MIND
- □ DAEM

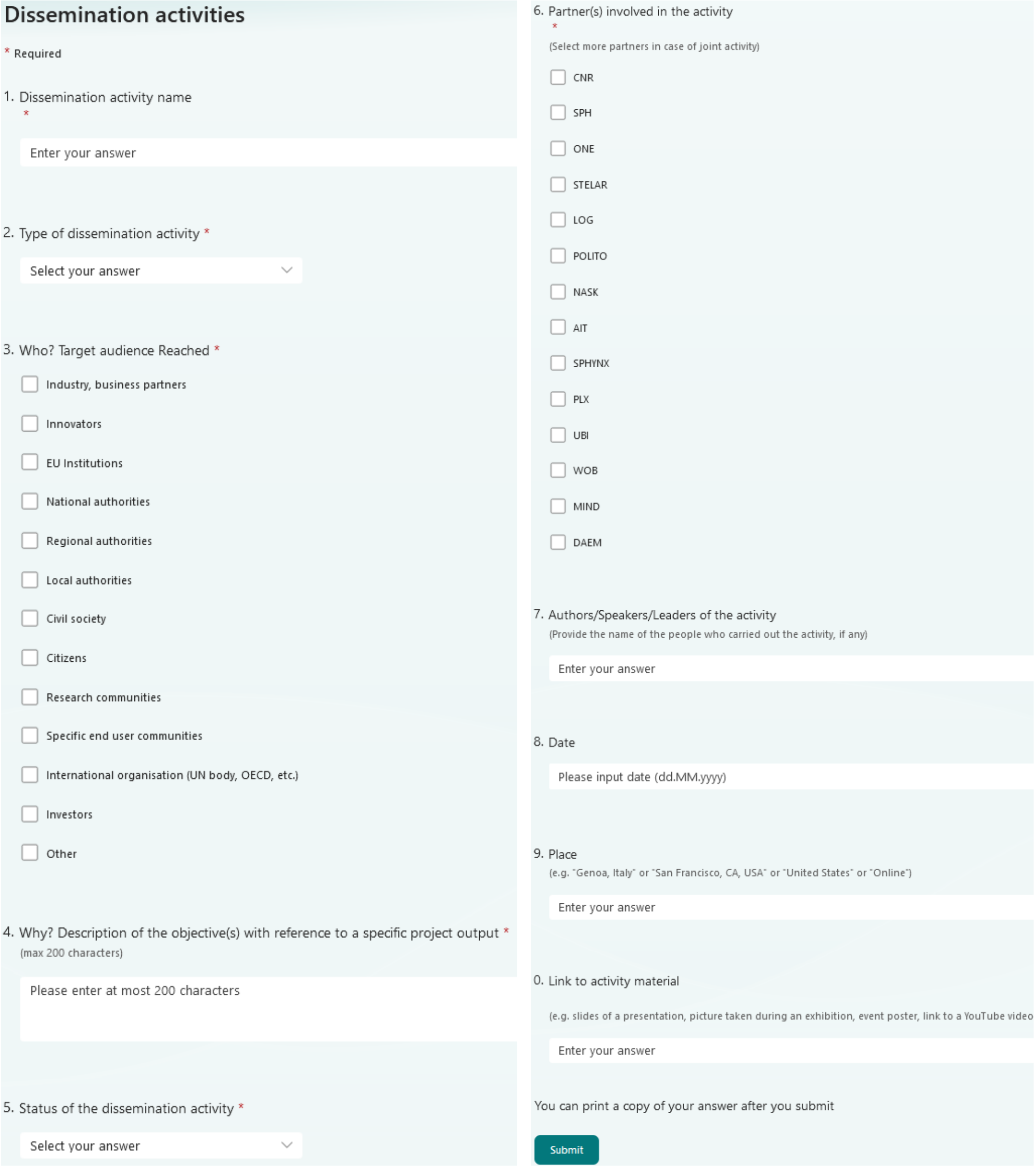
8. Authors/Speakers/Leaders of the activity
(Provide the name of the people who carried out the activity, if any)

9. Date

0. Place
e.g. "Genoa, Italy" or "San Francisco, CA, USA" or "United States" or "Online"

1. Link to activity material
(e.g. slides of a presentation, picture taken during an exhibition, event poster, link to a YouTube video, link to a webpage where the activity has been published, ...)

Figure 21. Communication Activities Form



Dissemination activities

* Required

1. Dissemination activity name *

Enter your answer

2. Type of dissemination activity *

Select your answer

3. Who? Target audience Reached *

□ Industry, business partners
□ Innovators
□ EU Institutions
□ National authorities
□ Regional authorities
□ Local authorities
□ Civil society
□ Citizens
□ Research communities
□ Specific end user communities
□ International organisation (UN body, OECD, etc.)
□ Investors
□ Other

4. Why? Description of the objective(s) with reference to a specific project output *
(max 200 characters)

Please enter at most 200 characters

5. Status of the dissemination activity *

Select your answer

6. Partner(s) involved in the activity *
(Select more partners in case of joint activity)

□ CNR
□ SPH
□ ONE
□ STELAR
□ LOG
□ POLITO
□ NASK
□ AIT
□ SPHYNX
□ PLX
□ UBI
□ WOB
□ MIND
□ DAEM

7. Authors/Speakers/Leaders of the activity
(Provide the name of the people who carried out the activity, if any)

Enter your answer

8. Date

Please input date (dd.MM.yyyy)

9. Place
(e.g. "Genoa, Italy" or "San Francisco, CA, USA" or "United States" or "Online")

Enter your answer

0. Link to activity material

(e.g. slides of a presentation, picture taken during an exhibition, event poster, link to a YouTube video

Enter your answer

You can print a copy of your answer after you submit

Figure 22. Dissemination Activities Form

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.