An innovative Virtual Reality based intrusion detection, incident investigation and response approach for enhancing the resilience, security, privacy and accountability of complex and heterogeneous digital systems and infrastructures.

D6.1 – Dissemination and Communication Strategy

Editors:	Anna Maria Anaxagorou
Beneficiary:	ITML
Version:	1.0
Status:	Final
Delivery date:	29/02/2024
Dissemination level:	PU (Public)

CyberSecDome has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101120779.

Deliverable Factsheet

Grant Agreement No.:	101120779
Project Acronym:	CyberSecDome
Project Title:	An innovative Virtual Reality based intrusion detection, incident investigation and response approach for enhancing the resilience, security, privacy and accountability of complex and heterogeneous digital systems and infrastructures.
Call:	HORIZON-CL3-2022-CS-01 (Cybersecurity)
Start date:	01/09/2023
Duration:	36 months

Deliverable Name:	D6.1 Dissemination and Communication Strategy v1.0
Related WP:	WP6 Dissemination, Exploitation and Sustainability
Due Date:	29/02/2024

Editors:	Anna Maria Anaxagorou (ITML)
Contributor(s):	Vina Rompoti (ITML)
Reviewer(s):	Marc-Oliver Pahl (IMT), Panagiotis Katrakazas (MAG)
Approved by:	All partners

Disclaimer

This document reflects the opinion of the authors only. While the information contained herein is believed to be accurate, neither the CyberSecDome consortium as a whole, nor any of its members, their officers, employees or agents make no warranty that this material is capable of use, or that use of the information is free from risk and accept no liability for loss or damage suffered by any person with respect to any inaccuracy or mission.

Executive Summary

This deliverable is produced under WP6 and specifically Task 6.1 “Communication and dissemination activities”. It aims to develop and execute a dissemination and communication strategy to maximise the visibility of CyberSecDome and its results. Therefore, it focuses on planning, carrying out and monitoring the communication and dissemination activities during the project.

Communication and dissemination are two actions that may utilise the same tools and channels but have different purposes and objectives. The main goal is to plan a communication and dissemination strategy defining the meaning and scope of the terms “Communication” and “Dissemination”. “Communication” begins at the project’s inception and continues until its end, aiming to inform the public and target audiences about the project while “Dissemination” starts when project results are available and aims to transfer knowledge to specific target groups.

The document describes the communication strategy and objectives, and introduces the visual identity, tools, and materials while suggesting measures for monitoring communication efforts. Additionally, it illustrates the dissemination strategy, target groups, and dissemination tools and measures to ensure stakeholder engagement.

Document History

Version	Date	Author(s)	Comments
0.1	23/01/2024	Anna Maria Anaxagorou	ToC
0.2	09/02/2024	Anna Maria Anaxagorou, Vina Rompoti	Draft ready for review
0.3	15/02/2024	Anna Maria Anaxagorou, Vina Rompoti	Final version to be sent to the reviewers
0.4	23/02/2024	Anna Maria Anaxagorou, Vina Rompoti	Version after the review processes
0.5	28/02/2024	Armend Duzha	Quality check
1.0	29/02/2024	Anna Maria Anaxagorou	Final version to be sent for submission

Contributors

Organization	Author(s)	Organisation
Document Leaders	Anna Maria Anaxagorou	ITML
Contributors	Vina Rompoti	ITML

Table of Contents

List of Figures

List of Tables

Acronyms and Abbreviations

AI	Artificial Intelligence
CDEB	Communication, Dissemination, Exploitation and Business Growth
CR	Cyber Range
DT	Digital Twin
ECCC	European Cybersecurity Competence Centre
GA	Grant Agreement
IPR	Intellectual Property Right
KER	Key Exploitable Result
KPIs	Key Performance Indicators
ML	Machine Learning
NCC	National Coordination Centres
OS	Open Science
TG	Target Group
TL	Task Leader
VR	Virtual Reality
WP	Work Package

1 Introduction

CyberSecDome plays a crucial role in advancing cybersecurity innovation and fostering collaboration within the European industrial landscape. Our approach is guided by the principles of transparency, accessibility, and inclusivity. We aim to engage diverse stakeholders in dialogues around cybersecurity challenges and solutions. Through innovative communication methods and targeted dissemination activities, we seek to maximize the impact of the project's research findings and technological advancements.

1.1 Purpose and Scope

In this deliverable, the main goal is to present an overview of the communication and dissemination strategy for the CyberSecDome project, providing a roadmap for effectively sharing project objectives, activities, and achievements with key stakeholders such as academic researchers, industry partners, policymakers, and public.

The scope of the strategy involves targeted communication efforts and measures aimed at enhancing awareness of the importance of cybersecurity and the application of state-of-the-art solutions and best practices. Through collaboration with stakeholders via various channels, such as workshops, events, webinars, and publications, with the objective of sharing knowledge, ideas, and promote information exchange. With these joint efforts we attempt to enhance cybersecurity resilience and contribute to a safer digital environment.

1.2 Contribution to other Deliverables

This deliverable serves as the backbone for the dissemination and communication activities throughout the CyberSecDome project. By outlining the strategy and objectives for how information will be shared, this document directly impacts the success of other deliverables and work packages within the project. It ensures that key project outcomes, research findings, and achievements are effectively communicated to stakeholders, thereby contributing to the fulfilment of specific project milestones outlined in other deliverables. Moreover, the communication and dissemination strategy outlined here helps maintain stakeholder engagement, fosters collaboration, and enhances the overall visibility and impact of the project.

1.3 Structure of the Document

The document offers a detailed layout of CyberSecDome's communication and dissemination strategy, divided into two main sections: communication and dissemination. Within each section, key elements such as objectives, target groups, activities, and monitoring measures are thoroughly addressed to provide a comprehensive understanding of the project's outreach activities. Moreover, the document is searching into topics like the project's visual identity, communication tools, and its contribution to other deliverables, offering stakeholders a holistic perspective on CyberSecDome's engagement efforts. This structured format ensures clarity and accessibility, facilitating efficient navigation for stakeholders seeking detailed insights into the project's engagement initiatives.

2 The CyberSecDome Project

Digital infrastructures have become the most important pillars that uphold our economy, our democracy, and our daily lives. A digital infrastructure consists of servers, data centres, telecom exchanges, radio access networks, satellites, databases, data stores, information technology services, cloud applications, and IoT device endpoints. More recent wars like the one in Ukraine have shown that **disrupting critical infrastructure** can be a strategic objective that could be achieved even before ground invasions are conducted[1]. Cyber-attacks (such as Ransomware, DDoS, etc.) against digital infrastructure may **cause digital disruption**, which can in turn result in huge financial losses[2], reduced trust in societal services, and even loss of human life[3]. Therefore, the need for protecting digital infrastructures from ever-evolving cybersecurity threats is continuously increasing.

The CyberSecDome project offers a solution that combines and completes a suite of security tools for addressing the aforementioned challenges. It provides a set of AI-Empowered security tools used to ensure that digital infrastructures operate properly even in adverse circumstances and recover quickly from potential cyber-attacks. The tools will be used to predict and detect incidents, automate pen-testing, assess ongoing risks, respond to attacks, and recover digital infrastructure services in a very efficient manner. As a major additional asset, CyberSecDome provides its users with an interactive advanced VR-based interface that enhances their understanding of the digital infrastructure to protect and enable them by providing so-called situational awareness about the detected attacks and risk analysis on ongoing risks.

CyberSecDome's vision is to **democratize and combine AI technology** to provide a **better prediction of cybersecurity threats** and **related risks** and an **efficient and dynamic selection of incident response** against cybersecurity attacks that may target the digital infrastructure. CyberSecDome aims also to use VR professionally to provide **situational awareness** of detected incidents, ongoing risks, and selected responses in real-time.

[1] Geneva Internal Platform *gigWatch, Ukraine conflict: Digital and cyber aspects*, online article available at: https://dig.watch/trends/ukraine-conflict-digital-and-cyber-aspects. Accessed 15/02/2024.

[2] Bitcom, *German businesses under attack: losses of more than 220 billion euros per year*, online article, available at: https://www.bitkom.org/EN/List-and-detailpages/Press/German-business-losses-more-than-220-billion-euros-per-year. Accessed 15/02/2024.

[3] Patrick Howell O'Neill (2020), *Ransomware did not kill a German hospital patient | MIT Technology Review*, MIT Technology Review, available at: https://www.technologyreview.com/2020/11/12/1012015/ransomware-did-not-kill-a-german-hospital-patient/. Accessed 15/02/2024.

3 Communication Strategy

The communication strategy is a detailed plan for communicating with the target audience. It includes who you are talking to, why you are talking to them, how and when you will talk to them, what form of communication the content should take and what channels you should use to share it. Communication plays an important role in maximizing the impact of a project and it is mandatory that project partners contribute to promote project's results. The communication strategy of CyberSecDome will focus on promoting every specific action in the project itself and its results to multitude of audiences including the media and public.

3.1 Communication Objectives

CyberSecDome's communication will be implemented aiming to fulfil specific communication objectives. Main goals for communication are:

Raise Awareness: Increase awareness of CyberSecDome among key stakeholders, including industry experts, researchers, policymakers, and the public.

Influence Opinion: Shape positive opinions of CyberSecDome by highlighting its impact on enhancing digital security and contributing to innovative solutions.

Knowledge Communication: Communicate project findings, methodologies, and technological advancements to facilitate knowledge exchange within the cybersecurity community.

Communication of Results: Effectively communicate project results, research publications, and deliverables to relevant audiences, maximizing the project's contribution to the cybersecurity landscape.

Showcase Achievements: Showcase project achievements, milestones, and success stories to demonstrate the tangible outcomes and impact of CyberSecDome.

Stakeholder Engagement: Foster engagement with project stakeholders, including consortium members, industry partners, and end-users, to ensure active participation and collaboration. CyberSecDome adopts an approach that involves stakeholders through workshops, events, conferences, webinars, and interactive sessions.

Engaging Through Various Channels: Emphasize engagement through social media, mainstream media, newsletters, flyers and the official website.

Promote Collaboration: Encourage collaboration and partnerships with external organizations, institutions, initiatives, and projects working in related fields.

Measurable Performance Tracking: Our aim is to achieve our KPIs at the highest level within the project's duration by tracking metrics such as website traffic and social media analytics monthly using software platforms registered for the project. Additionally, we will monitor the number of publications, presentations, and attendees at knowledge exchange events. These specific metrics provide a tangible way to evaluate the success of our communication efforts. Detailed KPIs measurable numbers are fully presenting in Section 4.5.

3.2 Communication Target Groups

Identifying target groups is a crucial step in developing an effective communication strategy for CyberSecDome. Those target groups should be identified from the start of the action until the end of the project. In this deliverable "target groups" are being presented into 2 separate actions. In the below paragraph potential target groups for the project's communication efforts have been identified; taking into account to whom will promote and communicate our results. By using a multi schema of social media channels (Twitter-LinkedIn-YouTube), we have developed a broader target group as much as we can, according to the project results.

1. **General Public:**
    - Raise awareness among the public about the importance of cybersecurity.
    - Foster a sense of digital security awareness and responsibility.
2. **Industry Experts and Professionals:**
    - Cybersecurity professionals and experts who can contribute insights and expertise.
    - IT professionals interested in the latest advancements in cybersecurity.
3. **Researchers and Academia:**
    - Researchers in the field of cybersecurity and related fields.
    - Academic institutions and professors involved in cybersecurity education.
4. **Policymakers and Government Agencies:**
    - Policymakers and government officials responsible for cybersecurity regulations and policies.
    - Government agencies involved in national and international cybersecurity initiatives.
5. **Business and Industry Partners:**
    - Companies and organizations in various industries with an interest in improving digital security.
    - Potential industry partners for collaboration and integration of CyberSecDome solutions.
6. **End-Users and Consumers:**
    - Individuals and organizations using digital systems and technologies.
    - Consumers interested in understanding and enhancing their own cybersecurity practices.
7. **Media Outlets and Journalists:**
    - Mainstream media outlets are interested in covering cybersecurity advancements.
    - Technology and cybersecurity journalists who can amplify project visibility.
8. **International Cybersecurity Community:**
    - Engage with the broader international cybersecurity community through conferences, forums, and collaborative initiatives.
9. **Regulatory Bodies and Compliance Organizations:**
    - Organizations responsible for cybersecurity regulations and compliance standards.
    - Bodies that set industry standards for cybersecurity practices.
10. **Investors and Funding Bodies:**
    - Attract potential investors interested in supporting cybersecurity innovations.
    - Engage with funding bodies and organizations that support research and development in cybersecurity.
11. **Educational Institutions:**
    - Universities and educational facilities offering courses related to cybersecurity.
    - Students following careers in cybersecurity.
12. **Non-Governmental Organizations (NGOs):**
    - NGOs focused on digital rights, online safety, and cybersecurity advocacy.
    - Organizations working towards a safer digital environment.
13. **External Pilot Participants (Open Call)**:
    - Engage individuals and organizations from various sectors in the open call to be potential pilots for CyberSecDome.

CyberSecDome aims to establish effective channels for aligning the project with the EU's cybersecurity priorities. This will involve initiating scoping activities with key working groups to facilitate discussions on digital infrastructure security issues funded by the European Commission, ensuring that a variety of voices are present. Adapting communication strategies to meet the interests and needs of the target groups mentioned above will enhance the effectiveness of CyberSecDome's outreach efforts. Therefore, workshops, webinars, and engagement events organized by CyberSecDome will serve as platforms to initiate open discussion sessions, aiming to engage key working groups and potential stakeholders. Incorporating surveys and questionnaires into these interactive sessions could offer tangible results and provide valuable feedback on the project's offerings and tools. These discussions will provide research priority recommendations for the specific topics: resilience of digital infrastructure, cyber-incident prediction, response and risk analysis, AI-empowered security processes, VR/DT-based interfaces for cybersecurity operation etc.

3.3 Communication Activities and Timing

The framework and timeline for the communication activities in the CyberSecDome project will have the following key points:

1. **Initiation and Duration:** Communication activities start at the beginning of the project and continue throughout its duration.
2. **Various Participation:** The activities involve both physical representation at project-specific events and participation in broader cybersecurity-related events across Europe throughout the project's timeline.
3. **Online Engagement:** Online communication is emphasized through social media, the project's website, and other online ways almost in daily basis.
4. **Publication Strategy:** Communication efforts extend to the publication of project updates in a variety of outlets, including regional, national, and EU-wide scientific and general journals staying to a predefined schedule aligned with project milestones.
5. **Partners contribution:** All partners contribute to communication efforts by providing input and engaging with audiences, ensuring the fulfillment of communication objectives within specified timeframes.
6. **Communication and Dissemination Oversight:** Supervision of communication activities includes analysing social media metrics, with regular reporting.
7. **Milestones:** Essential checkpoints are integrated into the project timeline to ensure progress tracking and alignment with project objectives.

The purpose is to establish a comprehensive and coordinated approach to communication that ensures the project's objectives are met and key audiences are effectively engaged throughout the project's lifecycle.

3.4 Monitoring of Communication Measures

In order to ensure the efficacy of our communication strategies, CyberSecDome has implemented a robust monitoring framework. This systematic approach involves the continuous evaluation of various key performance indicators (KPIs) to ensure that is aligns with our overarching objectives. The following aspects will be closely monitored:

1. **Online Presence and Engagement:** Monthly monitoring of website traffic, social media metrics (followers, engagement, retweets, LinkedIn profile views), and push announcements to ensure effective online engagement and visibility.

2. **Newsletter Distribution:** Tracking the frequency and distribution of newsletters to ensure that we continually capture and maintain the interest of our audience and consistent dissemination of project progress and achievements.

3. **Material/Promotional for Engagement:** Monitoring the creation and distribution of various promotional materials to ensure consistent engagement and dissemination of project information. This involves tracking the downloads of CyberSecDome electronic brochures , views for videos on YouTube and the downloads of supporting materials to supplement project communication efforts.

4. **Participation in events:** Active involvement in relevant events, conferences and workshops is crucial to showcase the project's developments, network with key stakeholders and raise awareness about the project. Partners will continuously contribute by keeping the CyberSecDome presence active, disseminating the project's results at different events annually ensuring we achieve our planned participations.

5. **Communication Plan Updates:** Regular updates and revisions of the communication, dissemination, and exploitation plan to reflect lessons learned and evolving project needs. The consortium seeks to deliver 3 versions of the communication plan, which will be shared internally for partners' reference.

6. **Joint cluster synergies and Engagement with Stakeholders/Established links:** Tracking engagement and collaboration efforts with stakeholders, including participation in events, workshops, and collaborative activities.

7. **Communication Starter Pack:** Monitoring the distribution and utilization of the communication starter pack among project partners to ensure consistent branding and messaging. A full guide about communication strategy, measures, and planned actions distributed to all project partners.

3.5 CyberSecDome Visual Identity

The visual identity of CyberSecDome is a carefully designed to represent the project's mission, values, and commitment to cybersecurity excellence. The project is named CyberSecDome because it proposes the deployment of a "Cyber Security Dome" around digital infrastructure or systems. The CyberSecDome aims to ensure the continuity of operations of complex and heterogeneous systems despite potential disruptions caused by cyber-attacks. This dome is envisioned as a protective layer around digital infrastructure, comprising interconnected, overlapping, and nested dome structures. The dome incorporates both real and virtual infrastructures, along with AI-Empowered Security Tools and interfaces such as Virtual Reality (VR) based Interactive Collaborative User Interface (VR-Interface) and eXtended Reality (XR) interfaces. Through these elements, the CyberSecDome provides enhanced cybersecurity capabilities, including dynamic response and recovery strategies, while considering the interconnected nature of digital infrastructure.

3.5.1 Project Logo

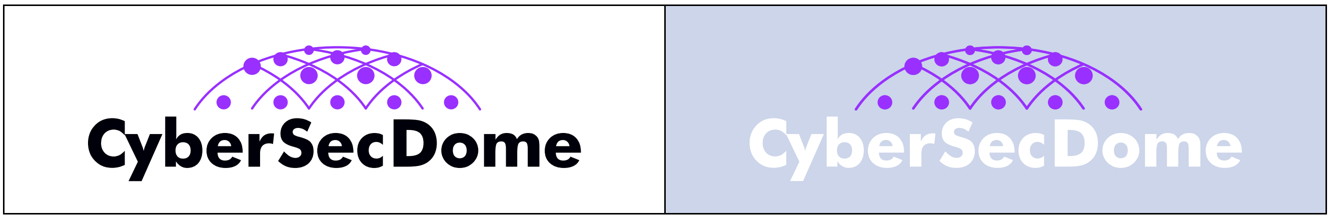


Figure 1 - CyberSecDome Logo

The CyberSecDome project logo features a black wordmark complemented by a symbolic dome in a vivid purple color, precisely crafted to encapsulate the project's mission and identity.

Logo Elements:

- **Wordmark:** "CyberSecDome" is designed for clarity and impact, representing the project's name.
- **Dome Symbol:** Positioned above the wordmark, the dome symbolizes protection, innovation, and the primary scope of the project.

Color Palette:

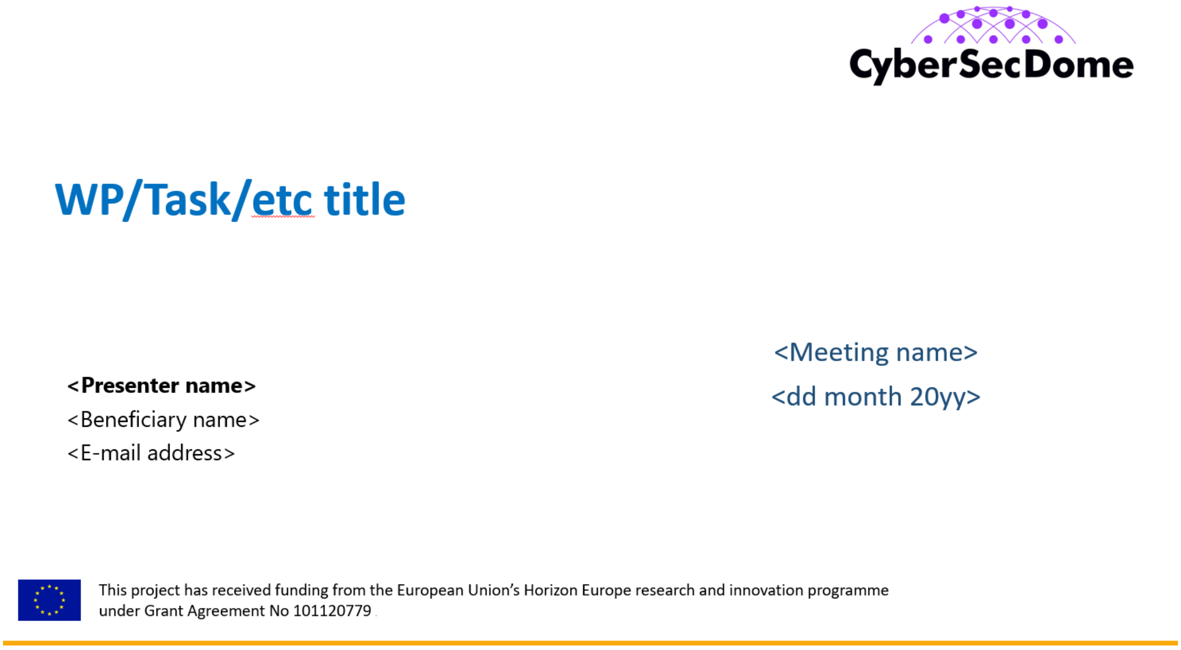
- **Black Wordmark (#000000):** The primary color for the project's name, black signifies sophistication and strength, offering a sleek and professional appearance. It represents the project's commitment to robust cybersecurity solutions, adding authority and clarity for easy recognition.
- **Vivid Purple #9930ff:** The primary color used in the logo reflects the project's branding and ensures visual consistency across various communication materials and the website. This cohesive color palette plays a significant role in establishing a recognizable visual identity for CyberSecDome.
- **White Wordmark (for dark backgrounds):** An alternative version of the logo features a white wordmark, ensuring visibility and contrast on dark backgrounds.

Usage Guidelines:

- **Consistency**: Maintain the logo's integrity by reproducing it consistently in the specified color and layout.
- **Clear Background**: Ensure sufficient contrast and visibility when using the logo on different backgrounds.

The CyberSecDome logo, with its identifiable typography and symbolic dome, serves as a visual representation of our commitment to cybersecurity and technological advancement, strengthening the project's identity across communications.

3.5.2 Project Templates



CyberSecDome

WP/Task/etc title

<Presenter name>
<Beneficiary name>
<E-mail address>

<Meeting name>
<dd month 20yy>

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101120779

Figure 2 - CyberSecDome Presentation Template

3.5.3 Project Materials

During the project's first months, we achieved significant progress in our dissemination efforts. We successfully developed and published the press release, flyer, and rollup, which have been already utilized at booths and events. These materials play a crucial role in communicating the project's objectives, activities, and achievements to various stakeholders.

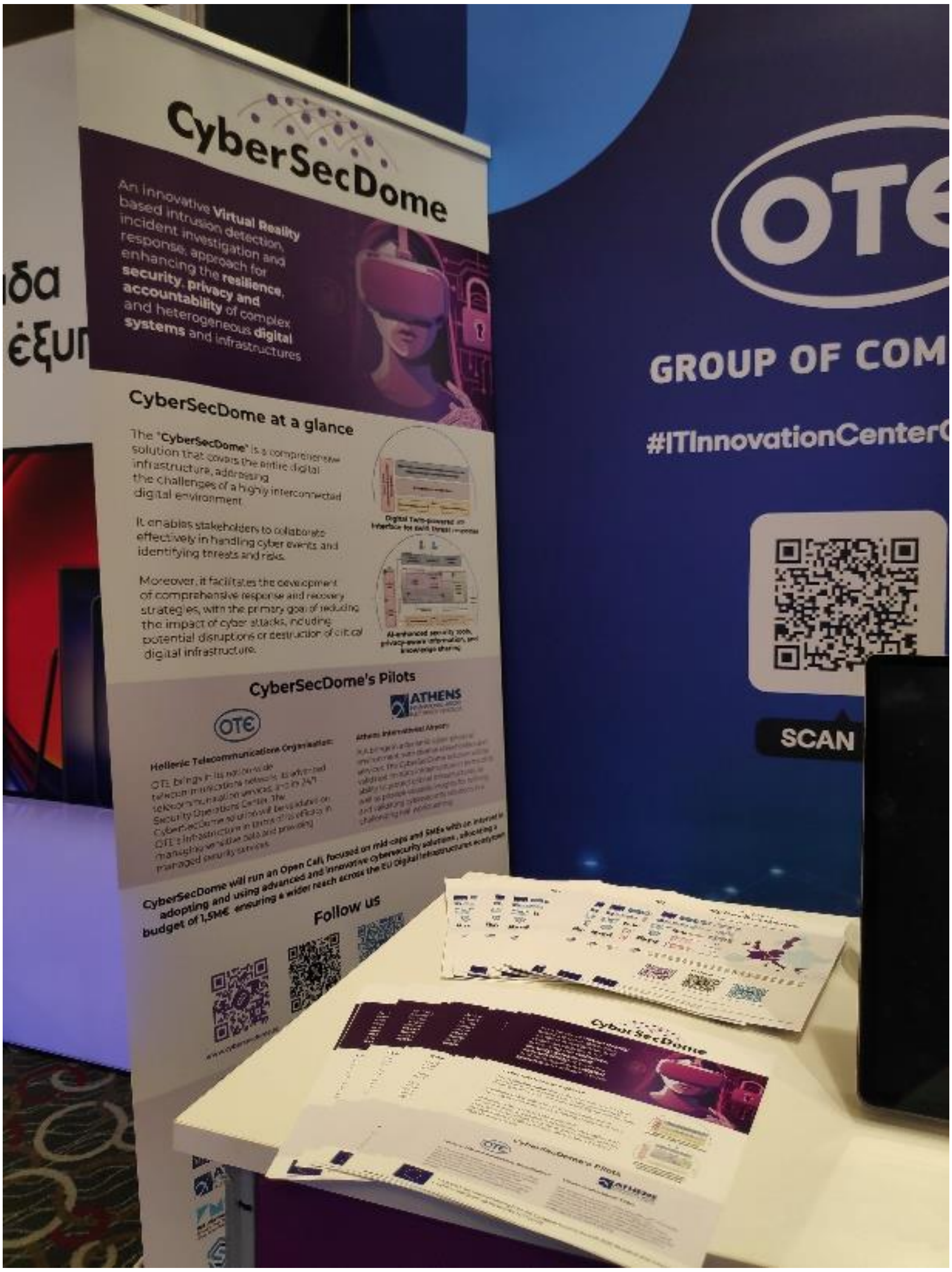
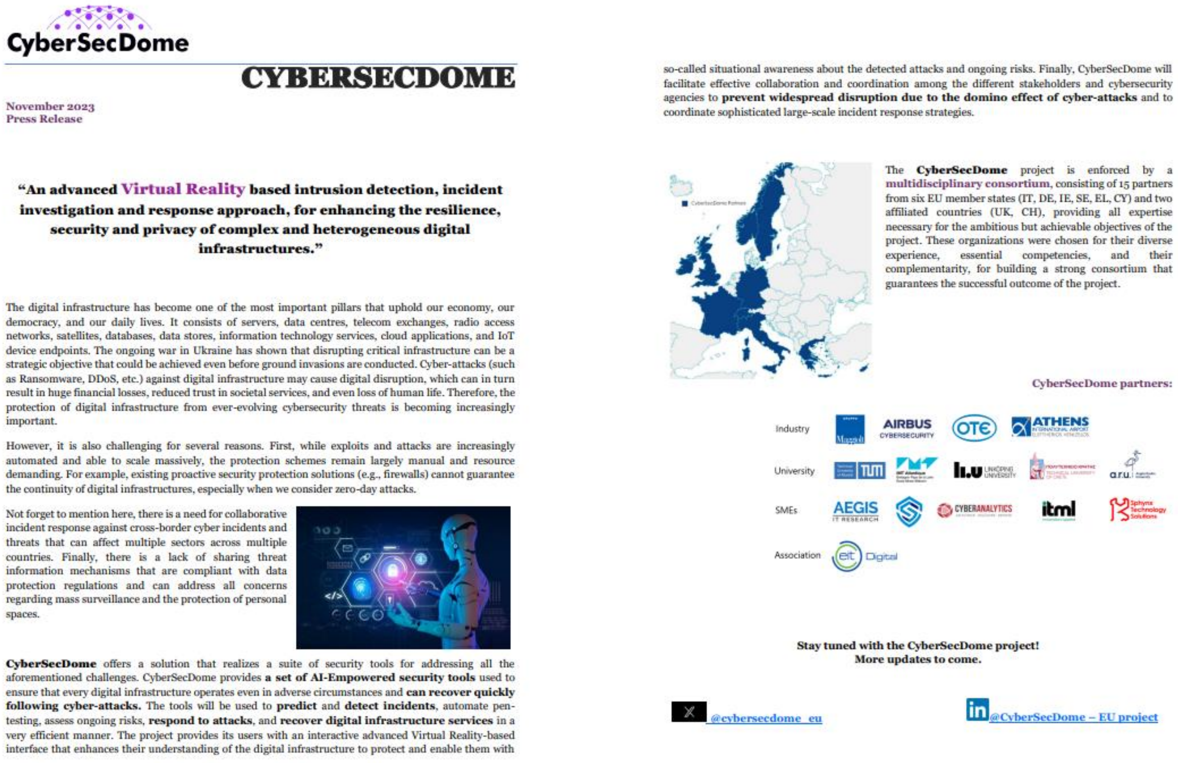

CyberSecDome
An innovative Virtual Reality based intrusion detection, incident investigation and response, approach for enhancing the resilience, security, privacy and accountability of complex and heterogeneous digital systems and infrastructures
CyberSecDome at a glance
CyberSecDome's Pilots
OTE
ATHENS
Follow us
OTE
GROUP OF COM
#ITInnovationCenter
SCAN

Figure 3 - CyberSecDome Booth presence



CyberSecDome

CYBERSECDOME

November 2023
Press Release

"An advanced Virtual Reality based intrusion detection, incident investigation and response approach, for enhancing the resilience, security and privacy of complex and heterogeneous digital infrastructures."

The digital infrastructure has become one of the most important pillars that uphold our economy, our democracy, and our daily lives. It consists of servers, data centres, telecom exchanges, radio access networks, satellites, databases, data stores, information technology services, cloud applications, and IoT device endpoints. The ongoing war in Ukraine has shown that disrupting critical infrastructure can be a strategic objective that could be achieved even before ground invasions are conducted. Cyber-attacks (such as Ransomware, DDoS, etc.) against digital infrastructure may cause digital disruption, which can in turn result in huge financial losses, reduced trust in societal services, and even loss of human life. Therefore, the protection of digital infrastructure from ever-evolving cybersecurity threats is becoming increasingly important.

However, it is also challenging for several reasons. First, while exploits and attacks are increasingly automated and able to scale massively, the protection schemes remain largely manual and resource demanding. For example, existing proactive security protection solutions (e.g., firewalls) cannot guarantee the continuity of digital infrastructures, especially when we consider zero-day attacks.

Not forget to mention here, there is a need for collaborative incident response against cross-border cyber incidents and threats that can affect multiple sectors across multiple countries. Finally, there is a lack of sharing threat information mechanisms that are compliant with data protection regulations and can address all concerns regarding mass surveillance and the protection of personal spaces.

CyberSecDome offers a solution that realizes a suite of security tools for addressing all the aforementioned challenges. CyberSecDome provides **a set of AI-Empowered security tools** used to ensure that every digital infrastructure operates even in adverse circumstances and **can recover quickly following cyber-attacks.** The tools will be used to **predict** and **detect incidents**, automate pen-testing, assess ongoing risks, **respond to attacks**, and **recover digital infrastructure services** in a very efficient manner. The project provides its users with an interactive advanced Virtual Reality-based interface that enhances their understanding of the digital infrastructure to protect and enable them with so-called situational awareness about the detected attacks and ongoing risks. Finally, CyberSecDome will facilitate effective collaboration and coordination among the different stakeholders and cybersecurity agencies to **prevent widespread disruption due to the domino effect of cyber-attacks** and to coordinate sophisticated large-scale incident response strategies.

The **CyberSecDome** project is enforced by a **multidisciplinary consortium**, consisting of 15 partners from six EU member states (IT, DE, IE, SE, EL, CY) and two affiliated countries (UK, CH), providing all expertise necessary for the ambitious but achievable objectives of the project. These organizations were chosen for their diverse experience, essential competencies, and their complementarity, for building a strong consortium that guarantees the successful outcome of the project.

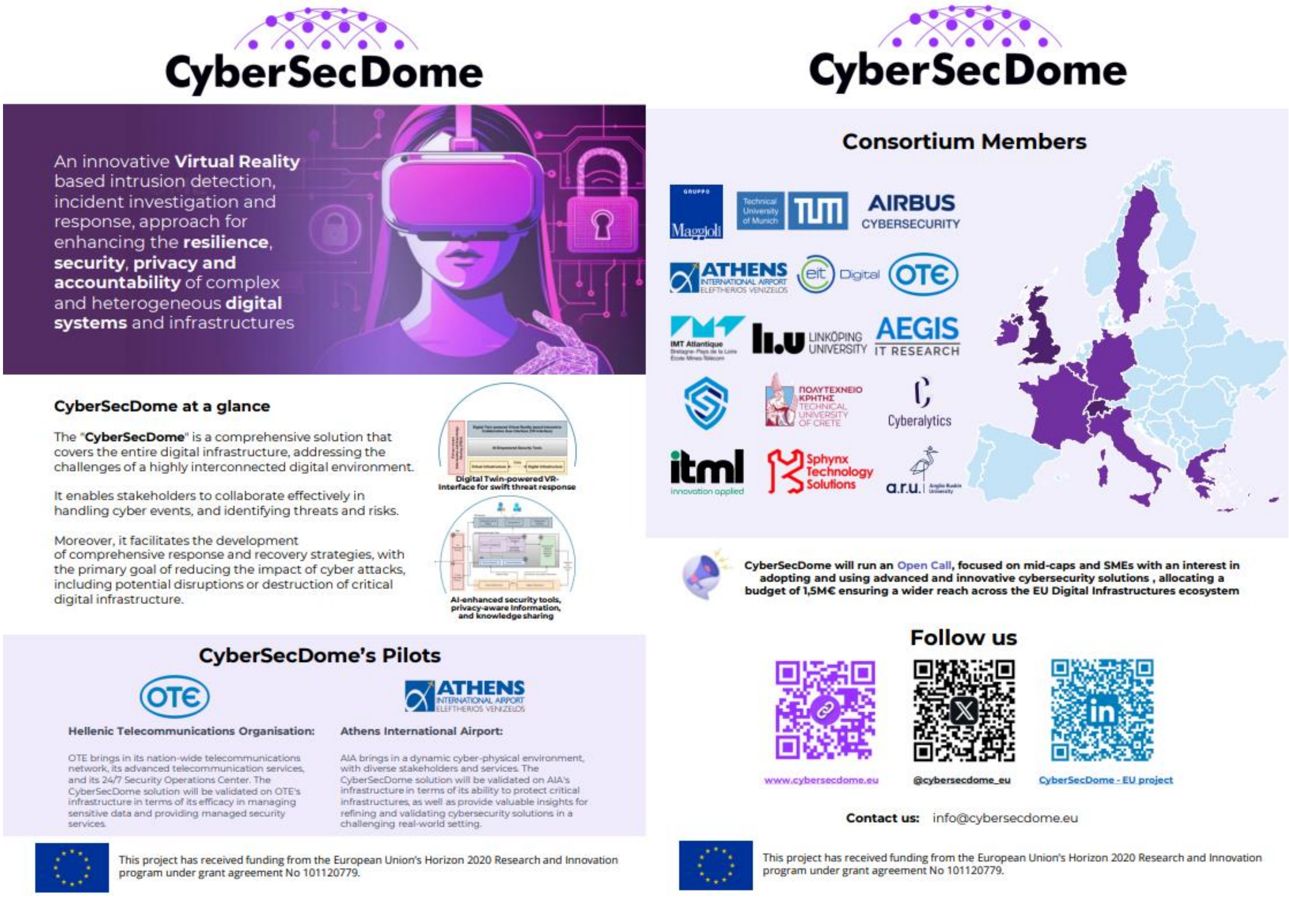
CyberSecDome partners:

Stay tuned with the CyberSecDome project!
More updates to come.

@cybersecdome_eu

@CyberSecDome – EU project

Figure 4 - CyberSecDome Press Release (link)



CyberSecDome

An innovative **Virtual Reality** based intrusion detection, incident investigation and response, approach for enhancing the **resilience**, **security**, **privacy and accountability** of complex and heterogeneous **digital systems** and infrastructures

CyberSecDome at a glance

The "**CyberSecDome**" is a comprehensive solution that covers the entire digital infrastructure, addressing the challenges of a highly interconnected digital environment.

It enables stakeholders to collaborate effectively in handling cyber events, and identifying threats and risks.

Moreover, it facilitates the development of comprehensive response and recovery strategies, with the primary goal of reducing the impact of cyber attacks, including potential disruptions or destruction of critical digital infrastructure.

Digital Twin-powered VR-Interface for swift threat response
AI-enhanced security tools, privacy-aware information, and knowledge sharing

CyberSecDome's Pilots

Hellenic Telecommunications Organisation:

OTE brings in its nation-wide telecommunications network, its advanced telecommunication services, and its 24/7 Security Operations Center. The CyberSecDome solution will be validated on OTE's infrastructure in terms of its efficacy in managing sensitive data and providing managed security services.

Athens International Airport:

AIA brings in a dynamic cyber-physical environment, with diverse stakeholders and services. The CyberSecDome solution will be validated on AIA's infrastructure in terms of its ability to protect critical infrastructures, as well as provide valuable insights for refining and validating cybersecurity solutions in a challenging real-world setting.

This project has received funding from the European Union's Horizon 2020 Research and Innovation program under grant agreement No 101120779.

CyberSecDome

Consortium Members

Maggioli
Technical University of Munich TUM
AIRBUS CYBERSECURITY
ATHENS INTERNATIONAL AIRPORT ELEFTHERIOS VENIZELOS
eit Digital
OTE
IMT Atlantique
LiU LINKÖPING UNIVERSITY
AEGIS IT RESEARCH
ΠΟΛΥΤΕΧΝΕΙΟ ΚΡΗΤΗΣ TECHNICAL UNIVERSITY OF CRETE
Cyberalytics
itml innovation applied
Sphynx Technology Solutions
a.r.u. Anglia Ruskin University

CyberSecDome will run an Open Call, focused on mid-caps and SMEs with an interest in adopting and using advanced and innovative cybersecurity solutions , allocating a budget of 1,5M€ ensuring a wider reach across the EU Digital Infrastructures ecosystem

Follow us

www.cybersecdome.eu

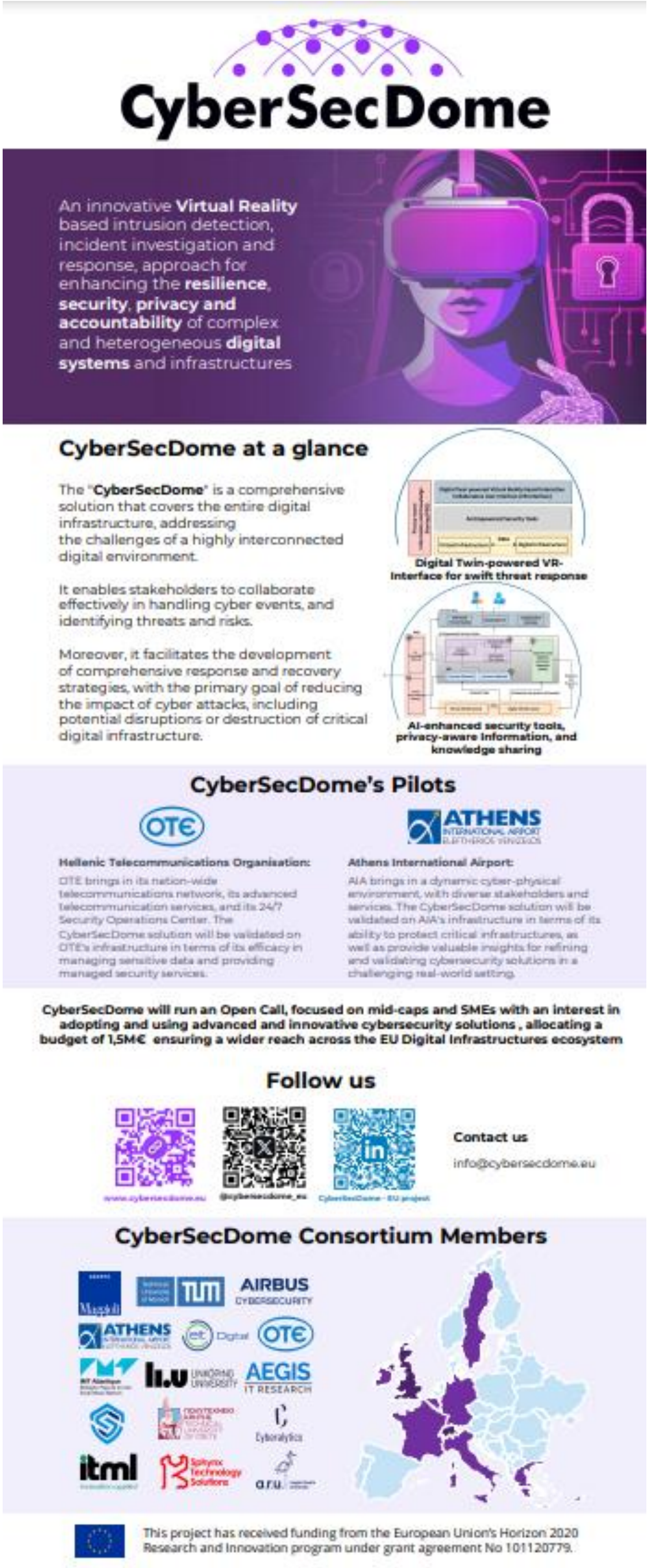
@cybersecdome_eu

CyberSecDome - EU project

Contact us: info@cybersecdome.eu

This project has received funding from the European Union's Horizon 2020 Research and Innovation program under grant agreement No 101120779.

Figure 5 - CyberSecDome flyer (link)



CyberSecDome

An innovative **Virtual Reality** based intrusion detection, incident investigation and response, approach for enhancing the **resilience**, **security, privacy and accountability** of complex and heterogeneous **digital systems** and infrastructures

CyberSecDome at a glance

The "**CyberSecDome**" is a comprehensive solution that covers the entire digital infrastructure, addressing the challenges of a highly interconnected digital environment.

It enables stakeholders to collaborate effectively in handling cyber events, and identifying threats and risks.

Moreover, it facilitates the development of comprehensive response and recovery strategies, with the primary goal of reducing the impact of cyber attacks, including potential disruptions or destruction of critical digital infrastructure.

Digital Twin-powered VR-Interface for swift threat response

AI-enhanced security tools, privacy-aware Information, and knowledge sharing

CyberSecDome's Pilots

Hellenic Telecommunications Organisation:

OTE brings in its nation-wide telecommunications network, its advanced telecommunication services, and its 24/7 Security Operations Center. The CyberSecDome solution will be validated on OTE's infrastructure in terms of its efficacy in managing sensitive data and providing managed security services.

Athens International Airport:

AIA brings in a dynamic cyber-physical environment, with diverse stakeholders and services. The CyberSecDome solution will be validated on AIA's infrastructure in terms of its ability to protect critical infrastructures, as well as provide valuable insights for refining and validating cybersecurity solutions in a challenging real-world setting.

CyberSecDome will run an Open Call, focused on mid-caps and SMEs with an interest in adopting and using advanced and innovative cybersecurity solutions , allocating a budget of 1,5M€ ensuring a wider reach across the EU Digital Infrastructures ecosystem

Follow us

www.cybersecdome.eu

@cybersecdome_eu

CyberSecDome - EU project

Contact us

info@cybersecdome.eu

CyberSecDome Consortium Members

This project has received funding from the European Union's Horizon 2020 Research and Innovation program under grant agreement No 101120779.

Figure 6 - CyberSecDome Roll-up (link)

3.6 Communication Tools

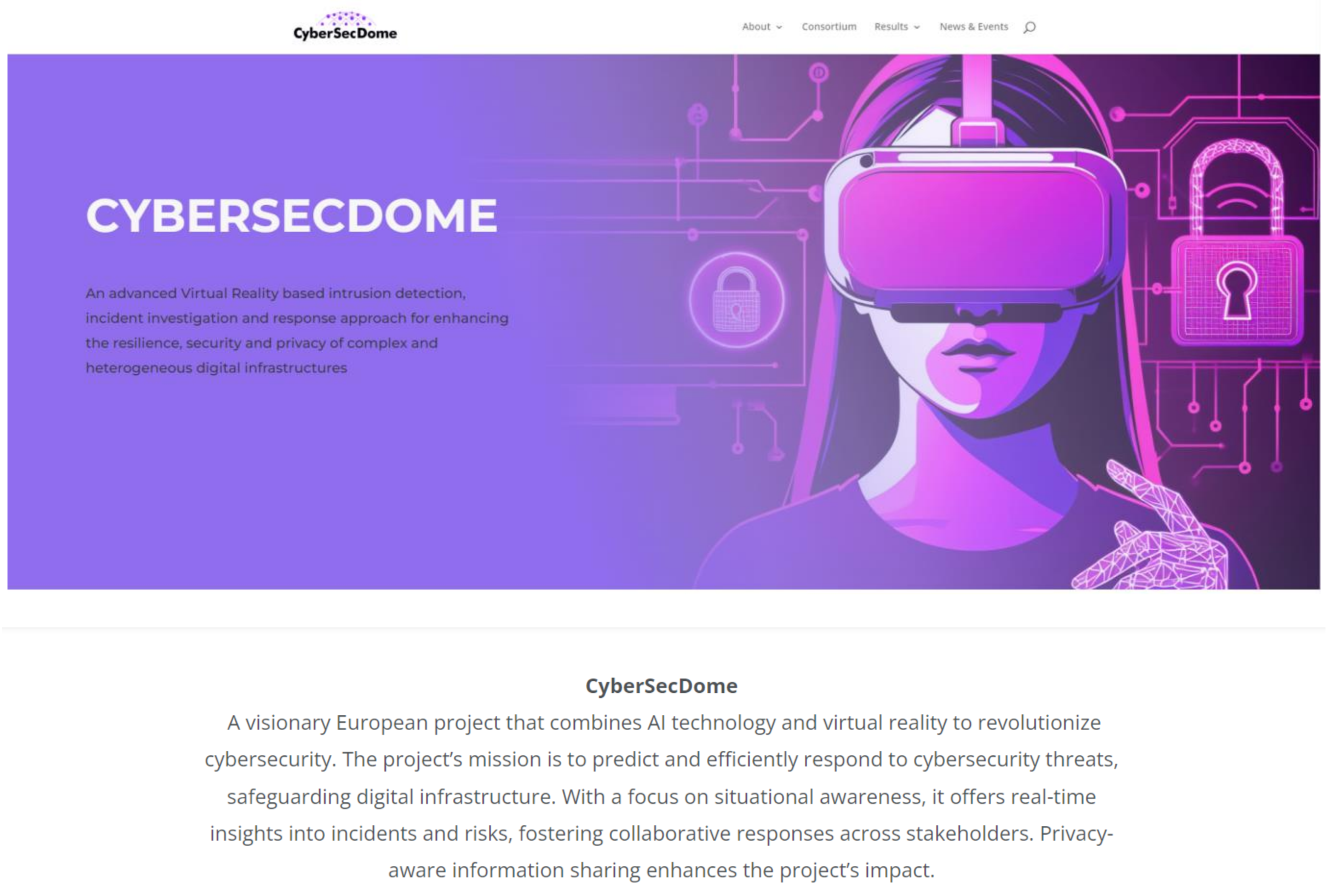
3.6.1 Project Webpage

Digital communication is one of the most effective ways to strengthen the project's engagement with key audiences and stakeholders. The CyberSecDome website has been designed and developed by ITML and is accessible at http://www.cybersecdome.eu/.

The website has been designed and structured with the intent to be one of the main channels for the communication and the dissemination of the project objectives and achievements not only to European and global industry, academia, and scientific communities but also to stakeholders and the interested audience.
It was also designed to offer a user-friendly environment with easy navigation, placing a main menu panel on the top of the main page, as a central interaction point for the webpage visitors.

The project webpage serves as a central hub for accessing project information, updates, resources, and contact details. The website's contents also include an overview of the project description, concept, objectives, mission, pilots, and application areas along with a consortium members' description and their visual identity.

It also hosts a range of dynamic features, including updates on upcoming events, meetings, workshops, news, and a repository of related audio-visual materials. These sections will be continuously updated to ensure visitors have access to the latest information and materials pertaining to the project's scientific publications, webinars, and blog articles. This commitment to regular updates enhances the website's role as a key virtual engagement platform, providing visitors with a rich and informative experience.

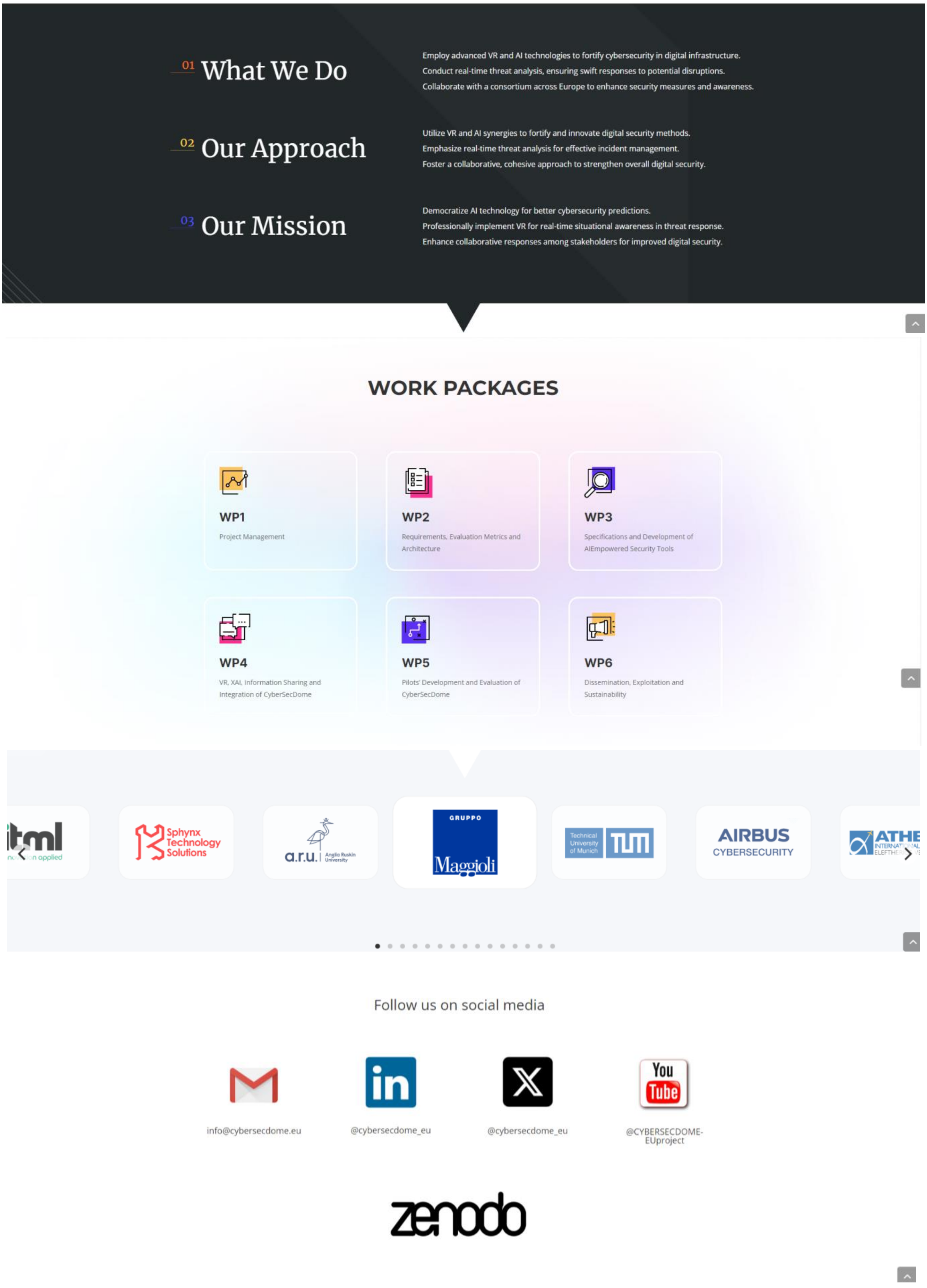


CYBERSECDOME

An advanced Virtual Reality based intrusion detection, incident investigation and response approach for enhancing the resilience, security and privacy of complex and heterogeneous digital infrastructures

CyberSecDome

A visionary European project that combines AI technology and virtual reality to revolutionize cybersecurity. The project's mission is to predict and efficiently respond to cybersecurity threats, safeguarding digital infrastructure. With a focus on situational awareness, it offers real-time insights into incidents and risks, fostering collaborative responses across stakeholders. Privacy-aware information sharing enhances the project's impact.



01 What We Do

Employ advanced VR and AI technologies to fortify cybersecurity in digital infrastructure.
Conduct real-time threat analysis, ensuring swift responses to potential disruptions.
Collaborate with a consortium across Europe to enhance security measures and awareness.

02 Our Approach

Utilize VR and AI synergies to fortify and innovate digital security methods.
Emphasize real-time threat analysis for effective incident management.
Foster a collaborative, cohesive approach to strengthen overall digital security.

03 Our Mission

Democratize AI technology for better cybersecurity predictions.
Professionally implement VR for real-time situational awareness in threat response.
Enhance collaborative responses among stakeholders for improved digital security.

WORK PACKAGES

WP1
Project Management

WP2
Requirements, Evaluation Metrics and Architecture

WP3
Specifications and Development of AIEmpowered Security Tools

WP4
VR, XAI, Information Sharing and Integration of CyberSecDome

WP5
Pilots' Development and Evaluation of CyberSecDome

WP6
Dissemination, Exploitation and Sustainability

tml
Sphynx Technology Solutions
a.r.u. Anglia Ruskin University
GRUPPO Maggioli
Technical University of Munich
AIRBUS CYBERSECURITY
ATHE

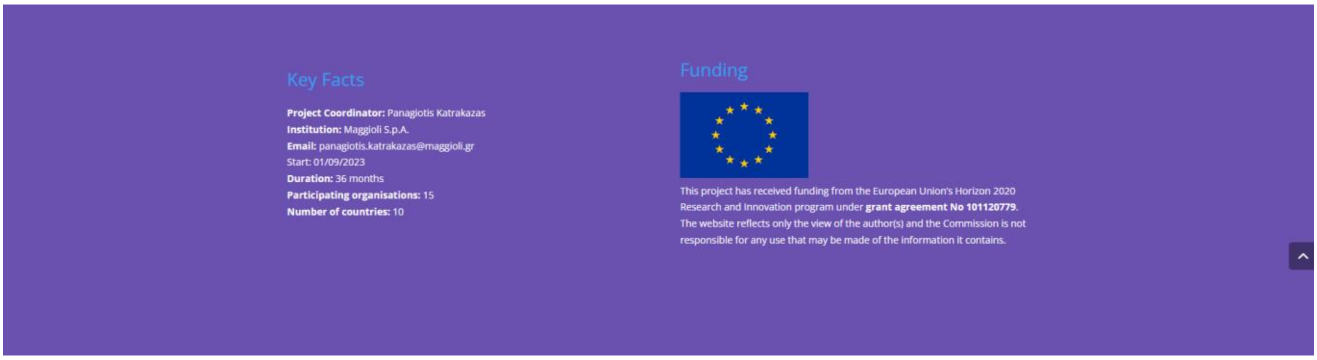
Follow us on social media

info@cybersecdome.eu

@cybersecdome_eu

@cybersecdome_eu

@CYBERSECDOME-EUproject



Key Facts

Project Coordinator: Panagiotis Katrakazas
Institution: Maggioli S.p.A.
Email: panagiotis.katrakazas@maggioli.gr
Start: 01/09/2023
Duration: 36 months
Participating organisations: 15
Number of countries: 10

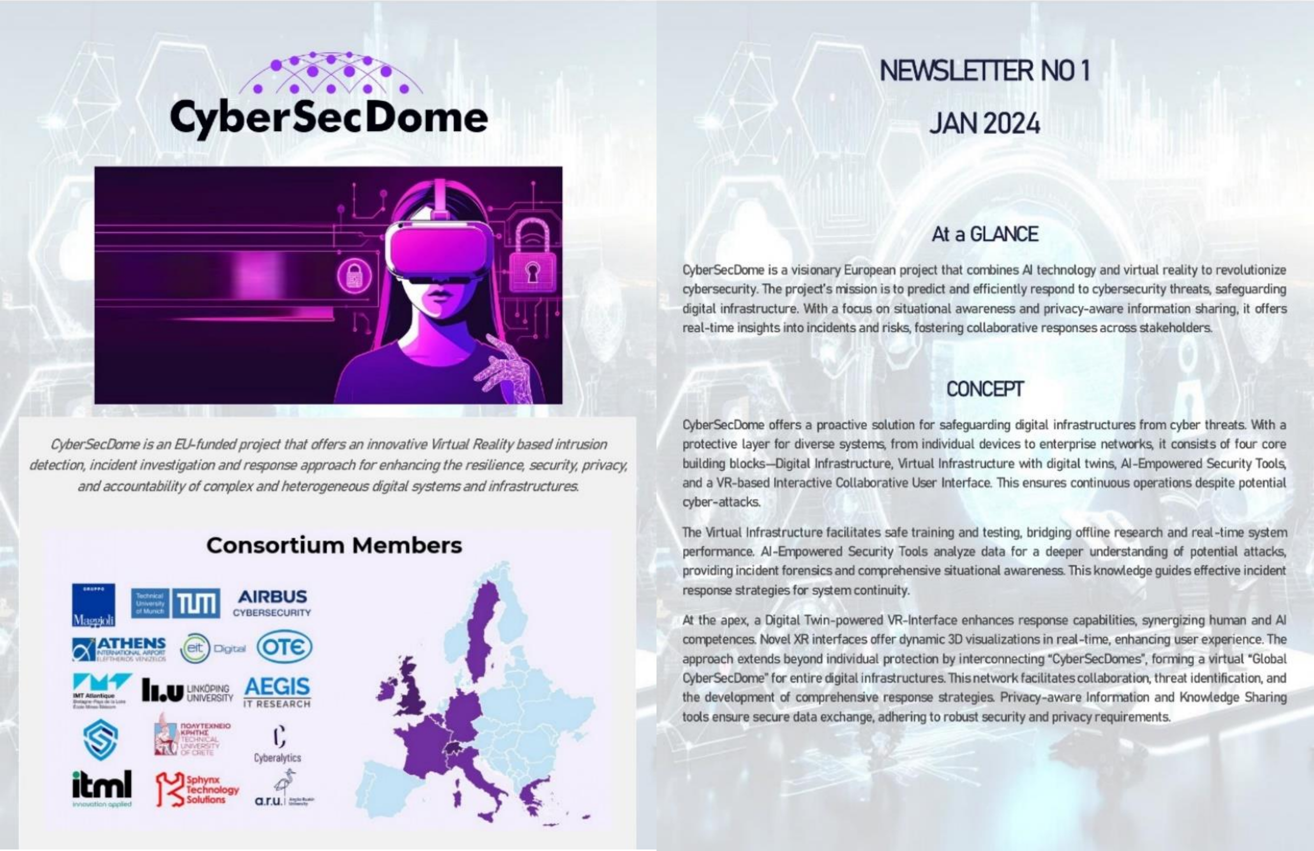
Funding

This project has received funding from the European Union's Horizon 2020 Research and Innovation program under **grant agreement No 101120779**. The website reflects only the view of the author(s) and the Commission is not responsible for any use that may be made of the information it contains.

Figure 7 - CyberSecDome main webpage

3.6.2 Project Newsletters

The CyberSecDome project will periodically issue a digital newsletter to keep the audience informed about upcoming events, project milestones, and relevant news stories within the cybersecurity domain. To meet the project's KPIs, the plan is to publish more than 8 newsletters featuring technical activities by the end of the project. The 1st newsletter (see Figure 8) serving as an introduction, was published in month M5.



CyberSecDome is an EU-funded project that offers an innovative Virtual Reality based intrusion detection, incident investigation and response approach for enhancing the resilience, security, privacy, and accountability of complex and heterogeneous digital systems and infrastructures.

Consortium Members

NEWSLETTER NO 1
JAN 2024

At a GLANCE

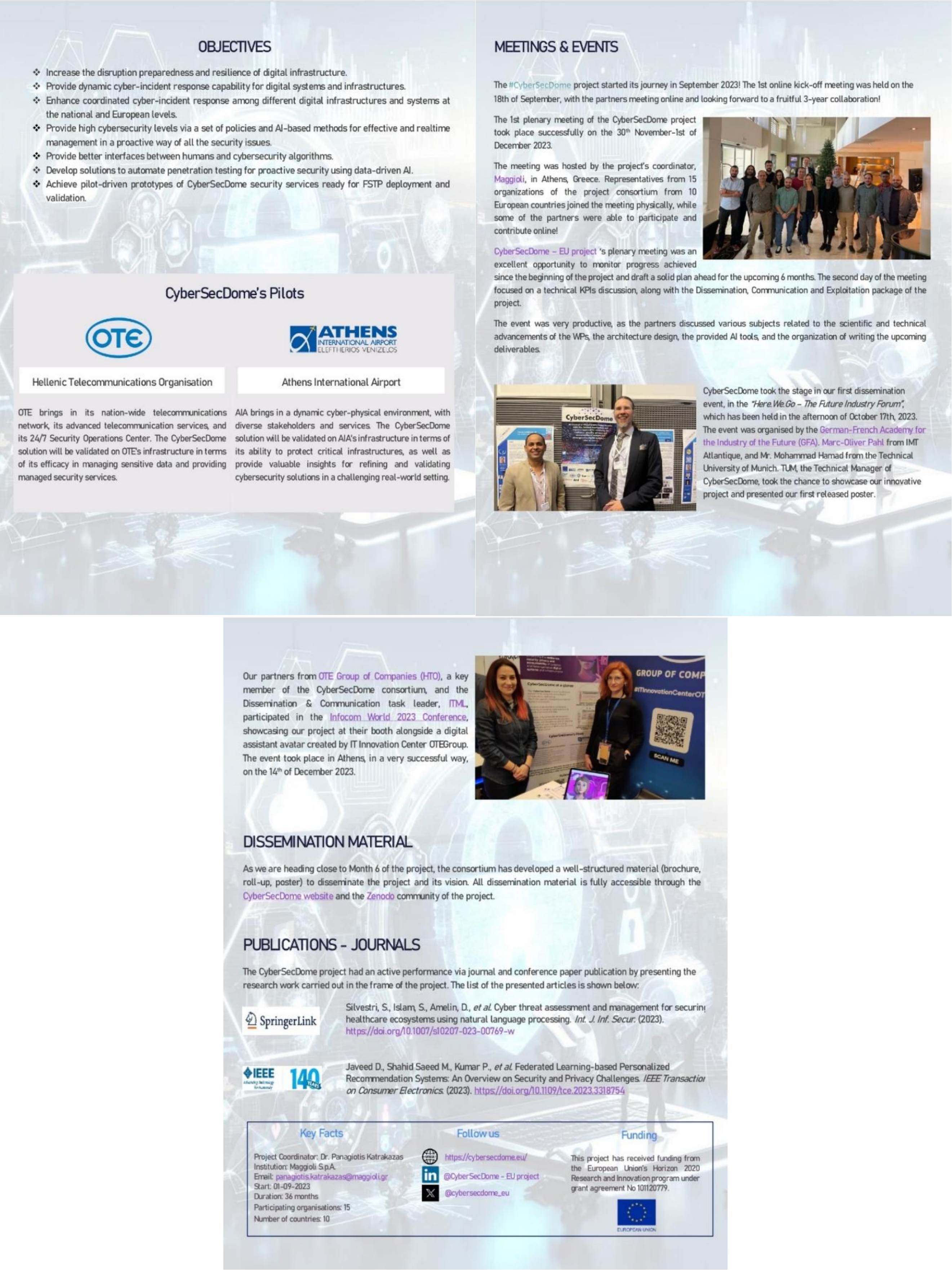
CyberSecDome is a visionary European project that combines AI technology and virtual reality to revolutionize cybersecurity. The project's mission is to predict and efficiently respond to cybersecurity threats, safeguarding digital infrastructure. With a focus on situational awareness and privacy-aware information sharing, it offers real-time insights into incidents and risks, fostering collaborative responses across stakeholders.

CONCEPT

CyberSecDome offers a proactive solution for safeguarding digital infrastructures from cyber threats. With a protective layer for diverse systems, from individual devices to enterprise networks, it consists of four core building blocks—Digital Infrastructure, Virtual Infrastructure with digital twins, AI-Empowered Security Tools, and a VR-based Interactive Collaborative User Interface. This ensures continuous operations despite potential cyber-attacks.

The Virtual Infrastructure facilitates safe training and testing, bridging offline research and real-time system performance. AI-Empowered Security Tools analyze data for a deeper understanding of potential attacks, providing incident forensics and comprehensive situational awareness. This knowledge guides effective incident response strategies for system continuity.

At the apex, a Digital Twin-powered VR-Interface enhances response capabilities, synergizing human and AI competences. Novel XR interfaces offer dynamic 3D visualizations in real-time, enhancing user experience. The approach extends beyond individual protection by interconnecting "CyberSecDomes", forming a virtual "Global CyberSecDome" for entire digital infrastructures. This network facilitates collaboration, threat identification, and the development of comprehensive response strategies. Privacy-aware Information and Knowledge Sharing tools ensure secure data exchange, adhering to robust security and privacy requirements.



OBJECTIVES

- Increase the disruption preparedness and resilience of digital infrastructure.
- Provide dynamic cyber-incident response capability for digital systems and infrastructures.
- Enhance coordinated cyber-incident response among different digital infrastructures and systems at the national and European levels.
- Provide high cybersecurity levels via a set of policies and AI-based methods for effective and realtime management in a proactive way of all the security issues.
- Provide better interfaces between humans and cybersecurity algorithms.
- Develop solutions to automate penetration testing for proactive security using data-driven AI.
- Achieve pilot-driven prototypes of CyberSecDome security services ready for FSTP deployment and validation.

CyberSecDome's Pilots

Hellenic Telecommunications Organisation	Athens International Airport
OTE brings in its nation-wide telecommunications network, its advanced telecommunication services, and its 24/7 Security Operations Center. The CyberSecDome solution will be validated on OTE's infrastructure in terms of its efficacy in managing sensitive data and providing managed security services.	AIA brings in a dynamic cyber-physical environment, with diverse stakeholders and services. The CyberSecDome solution will be validated on AIA's infrastructure in terms of its ability to protect critical infrastructures, as well as provide valuable insights for refining and validating cybersecurity solutions in a challenging real-world setting.

MEETINGS & EVENTS

The #CyberSecDome project started its journey in September 2023! The 1st online kick-off meeting was held on the 18th of September, with the partners meeting online and looking forward to a fruitful 3-year collaboration!

The 1st plenary meeting of the CyberSecDome project took place successfully on the 30th November-1st of December 2023.

The meeting was hosted by the project's coordinator, Maggioli, in Athens, Greece. Representatives from 15 organizations of the project consortium from 10 European countries joined the meeting physically, while some of the partners were able to participate and contribute online!

CyberSecDome – EU project 's plenary meeting was an excellent opportunity to monitor progress achieved since the beginning of the project and draft a solid plan ahead for the upcoming 6 months. The second day of the meeting focused on a technical KPIs discussion, along with the Dissemination, Communication and Exploitation package of the project.

The event was very productive, as the partners discussed various subjects related to the scientific and technical advancements of the WPs, the architecture design, the provided AI tools, and the organization of writing the upcoming deliverables.

CyberSecDome took the stage in our first dissemination event, in the *"Here We Go – The Future Industry Forum"*, which has been held in the afternoon of October 17th, 2023. The event was organised by the German-French Academy for the Industry of the Future (GFA). Marc-Oliver Pahl from IMT Atlantique, and Mr. Mohammad Hamad from the Technical University of Munich. TUM, the Technical Manager of CyberSecDome, took the chance to showcase our innovative project and presented our first released poster.

Our partners from OTE Group of Companies (HTO), a key member of the CyberSecDome consortium, and the Dissemination & Communication task leader, ITML, participated in the Infocom World 2023 Conference, showcasing our project at their booth alongside a digital assistant avatar created by IT Innovation Center OTEGroup. The event took place in Athens, in a very successful way, on the 14th of December 2023.

DISSEMINATION MATERIAL

As we are heading close to Month 6 of the project, the consortium has developed a well-structured material (brochure, roll-up, poster) to disseminate the project and its vision. All dissemination material is fully accessible through the CyberSecDome website and the Zenodo community of the project.

PUBLICATIONS - JOURNALS

The CyberSecDome project had an active performance via journal and conference paper publication by presenting the research work carried out in the frame of the project. The list of the presented articles is shown below:

SpringerLink — Silvestri, S., Islam, S., Amelin, D., *et al.* Cyber threat assessment and management for securin healthcare ecosystems using natural language processing. *Int. J. Inf. Secur.* (2023). https://doi.org/10.1007/s10207-023-00769-w

IEEE 140 — Javeed D., Shahid Saeed M., Kumar P., *et al.* Federated Learning-based Personalized Recommendation Systems: An Overview on Security and Privacy Challenges. *IEEE Transactio on Consumer Electronics.* (2023). https://doi.org/10.1109/tce.2023.3318754

Key Facts

Project Coordinator: Dr. Panagiotis Katrakazas
Institution: Maggioli S.p.A.
Email: panagiotis.katrakazas@maggioli.gr
Start: 01-09-2023
Duration: 36 months
Participating organisations: 15
Number of countries: 10

Follow us

https://cybersecdome.eu/
@CyberSecDome - EU project
@cybersecdome_eu

Funding

This project has received funding from the European Union's Horizon 2020 Research and Innovation program under grant agreement No 101120779.

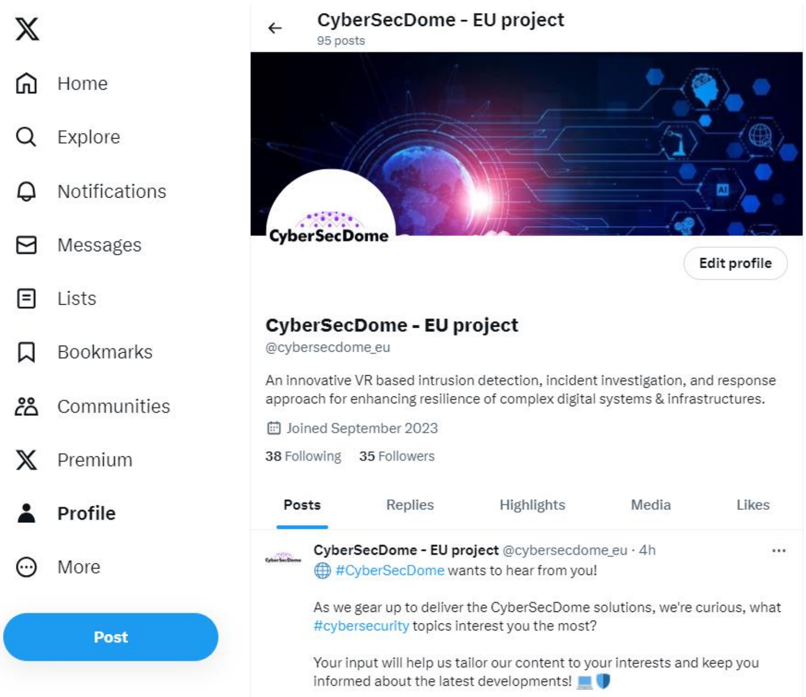
EUROPEAN UNION

Figure 8 - CyberSecDome 1st Newsletter (link)

3.6.3 Social Media presence

In addition to the CyberSecDome website, dedicated social media platforms (Twitter, LinkedIn and YouTube) enhance the dissemination of the project's progress, reaching a global audience of professionals and the public. These active platforms will provide timely updates, achievements, and results delivered by the CyberSecDome consortium to project audiences.

Twitter



CyberSecDome - EU project
95 posts

CyberSecDome - EU project
@cybersecdome_eu

An innovative VR based intrusion detection, incident investigation, and response approach for enhancing resilience of complex digital systems & infrastructures.

Joined September 2023

38 Following 35 Followers

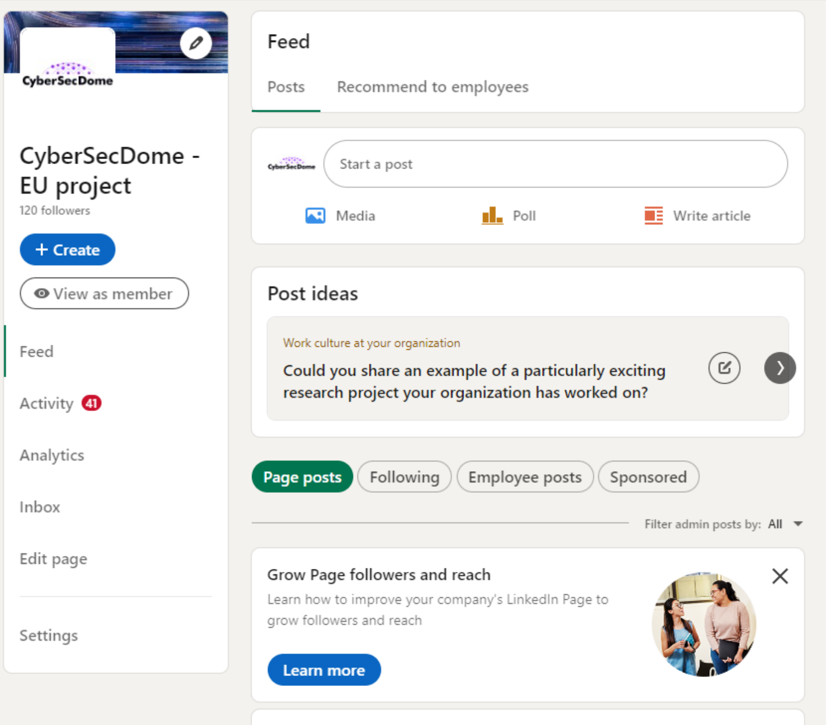
CyberSecDome - EU project @cybersecdome_eu · 4h
#CyberSecDome wants to hear from you!

As we gear up to deliver the CyberSecDome solutions, we're curious, what #cybersecurity topics interest you the most?

Your input will help us tailor our content to your interests and keep you informed about the latest developments! 💻🛡

Figure 9 - CyberSecDome Twitter profile (link)

LinkedIn



CyberSecDome - EU project
120 followers

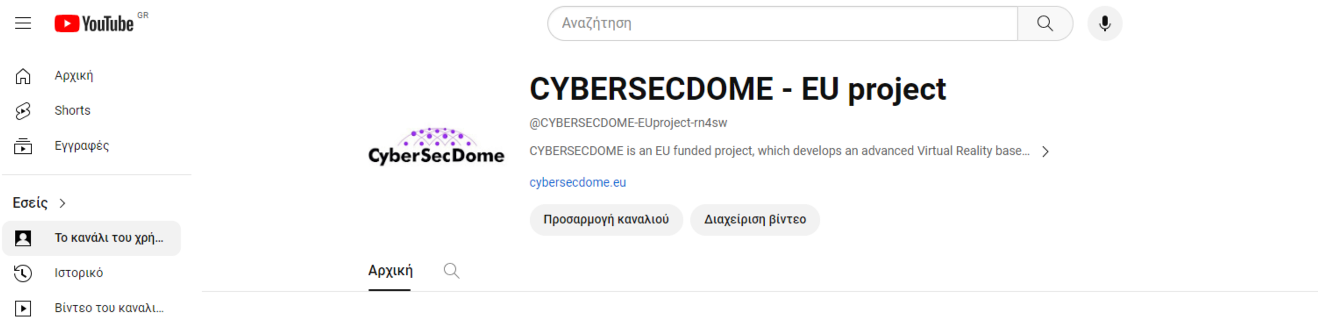
Post ideas

Work culture at your organization
Could you share an example of a particularly exciting research project your organization has worked on?

Grow Page followers and reach
Learn how to improve your company's LinkedIn Page to grow followers and reach

Figure 10 - CyberSecDome LinkedIn profile (link)

YouTube



CYBERSECDOME - EU project

@CYBERSECDOME-EUproject-rn4sw

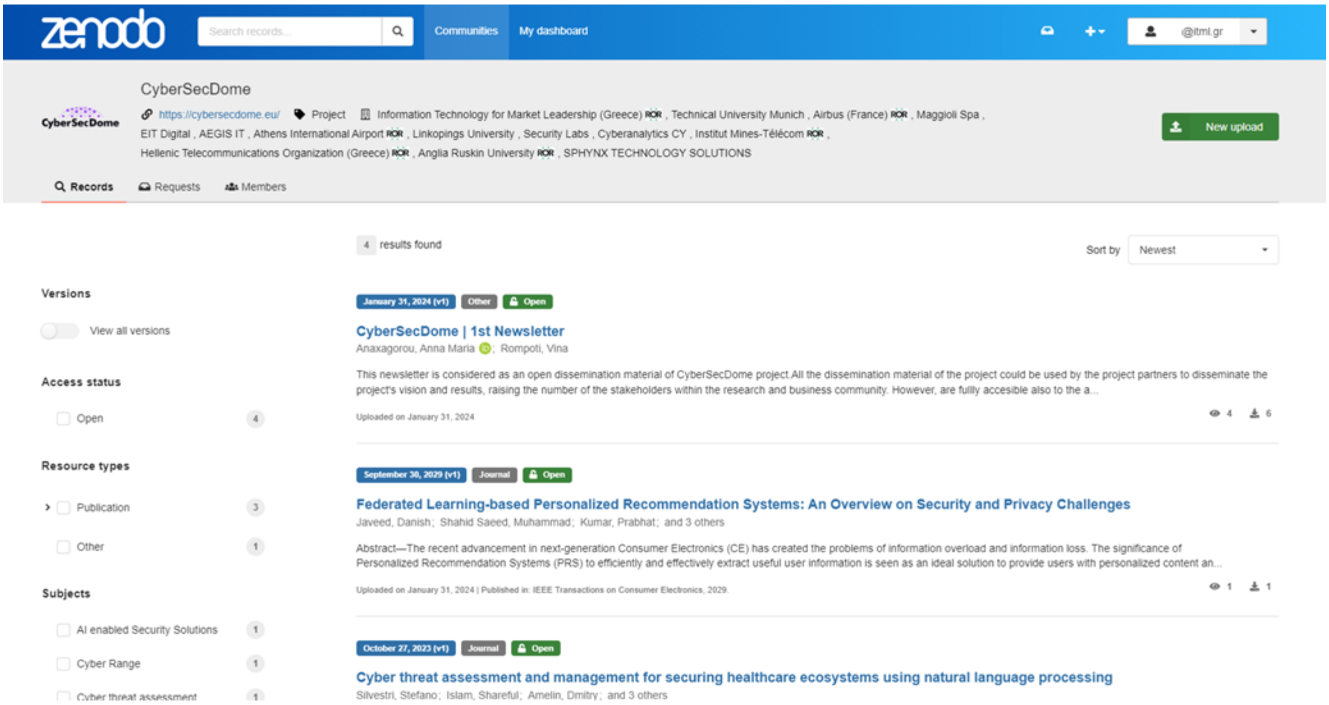
CYBERSECDOME is an EU funded project, which develops an advanced Virtual Reality base... >

cybersecdome.eu

Figure 11 - CyberSecDome YouTube channel (link)

Zenodo

CyberSecDome maintains an account on Zenodo, a digital repository for research outputs. This account serves as a platform for depositing, sharing, and preserving various research outputs related to the project, including datasets, software, presentations, and publications. By leveraging Zenodo, CyberSecDome contributes to open science initiatives, making its research outputs openly accessible and discoverable to the wider research community.



CyberSecDome

https://cybersecdome.eu/ Project Information Technology for Market Leadership (Greece) ROR , Technical University Munich , Airbus (France) ROR , Maggioli Spa , EIT Digital , AEGIS IT , Athens International Airport ROR , Linkopings University , Security Labs , Cyberanalytics CY , Institut Mines-Télécom ROR , Hellenic Telecommunications Organization (Greece) ROR , Anglia Ruskin University ROR , SPHYNX TECHNOLOGY SOLUTIONS

4 results found

January 31, 2024 (v1) Other Open

CyberSecDome | 1st Newsletter

Anaxagorou, Anna Maria; Rompoti, Vina

This newsletter is considered as an open dissemination material of CyberSecDome project.All the dissemination material of the project could be used by the project partners to disseminate the project's vision and results, raising the number of the stakeholders within the research and business community. However, are fullly accesible also to the a...

Uploaded on January 31, 2024 👁 4 ⬇ 6

September 30, 2029 (v1) Journal Open

Federated Learning-based Personalized Recommendation Systems: An Overview on Security and Privacy Challenges

Javeed, Danish; Shahid Saeed, Muhammad; Kumar, Prabhat; and 3 others

Abstract—The recent advancement in next-generation Consumer Electronics (CE) has created the problems of information overload and information loss. The significance of Personalized Recommendation Systems (PRS) to efficiently and effectively extract useful user information is seen as an ideal solution to provide users with personalized content an...

Uploaded on January 31, 2024 | Published in: IEEE Transactions on Consumer Electronics, 2029. 👁 1 ⬇ 1

October 27, 2023 (v1) Journal Open

Cyber threat assessment and management for securing healthcare ecosystems using natural language processing

Silvestri, Stefano; Islam, Shareful; Amelin, Dmitry; and 3 others

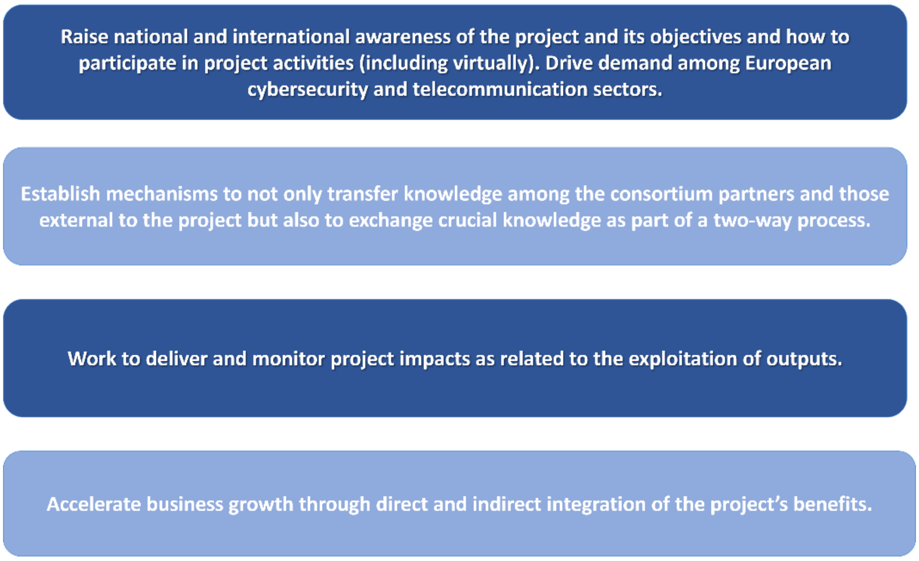
Figure 12 - CyberSecDome Zenodo community (link)

4 Dissemination Strategy

The CyberSecDome consortium has developed a roadmap toward impact maximisation based on six distinct steps: **(i)** development of a Communication, Dissemination, Exploitation and Business Growth (CDEB) strategy, **(ii)** monitoring and measuring progress, **(iii)** incorporating results into all tools and processes, **(iv)** integrating learnings to deepen impact, **(v)** engaging key stakeholders, and **(vi)** building staff and partner capacity.

CyberSecDome aims to optimise the collaborative response among the stakeholders within the Digital Infrastructure ecosystem by developing privacy-aware information and knowledge-sharing mechanisms.

One of the project's cross-cutting objectives is to develop a central reference point around the project and sustain it throughout its duration and beyond. Our CDEB plan has four objectives, as detailed below:



Raise national and international awareness of the project and its objectives and how to participate in project activities (including virtually). Drive demand among European cybersecurity and telecommunication sectors.

Establish mechanisms to not only transfer knowledge among the consortium partners and those external to the project but also to exchange crucial knowledge as part of a two-way process.

Work to deliver and monitor project impacts as related to the exploitation of outputs.

Accelerate business growth through direct and indirect integration of the project's benefits.

Figure 13 - CDEB Objectives

All the objectives require to be accompanied with communication measures and KPIs to monitor success, while all the partners are trying to follow them.

The strategy is structured based on the following steps: 1) Set the objectives, 2) Identify the target groups, 3) Engage channels, 4) Set communication roles and responsibilities within the consortium, 5) Monitor impacts, 6) Link to the external EU agenda and 7) Define market penetration/development strategy. The goal of the peer-based dissemination of results consists in providing an understandable outreach to all main outcomes from various viewpoints, technical or business-related or relevant from a learning or teaching perspective.

4.1 Dissemination Target Groups

Several complementary target groups (TGs) have been identified as potential stakeholders of interest for CyberSecDome. When we disseminate a project, we seek to make our results public. Within Dissemination, we are focusing mostly on scientists but also on other audiences which can learn from CyberSecDome results. The below target groups for dissemination have been identified to maximise the results 'impact, contribute to the improvement of the state of art and certainly to allow other researchers to go a step further.

The profiles of CyberSecDome's target groups are presented in detail below:

- Telecommunication Industry
- Tech Providers
- Social Innovation Sector
- Partnerships & Networks
- Policymakers
- Society

Table 1 - CyberSecDome Target Groups

Telecommunication Industry: ***Telecom operators/providers, OTE operators, ICT service providers, Cloud service providers, Aviation operators (HIGH Importance)***	
In light of the changes in the threat landscape, the telecommunication networks and digital infrastructures utilized in multiple critical sectors like (transport/aviation sector and business domain etc.) are increasingly targeted by cyber-attacks and need adequate security precautions. This segment comprises Telecom operators, and ICT service providers responsible for a) provision of ICT business and societal services b) managing vast amounts of data and complex systems/equipment c) monitoring digital networks and providing advanced data communications services thus requiring possessing robust cybersecurity response capabilities and improved incident detection and handling processes.	HIGH
Tech Providers: ***Digital Twins (DT), Cyber Range (CR), Virtual Reality (VR), AI/ML Engineers, Data Scientists, Academic Researchers, Cybersecurity service providers, Standardisation Committees***	
The members who develop research outputs, innovation findings, business activities and standardisation efforts around the technologies transforming the sector –i.e., the technology-push perspective. The objective for these profiles is to investigate, advance and demonstrate the benefits offered by CyberSecDome-related technologies (i.e., AI/ML, VR, Data Analytics, etc.) to the real world. This category includes research-driven institutions (technical universities, RTOs, spin-offs) and private-sector organisations (from highly risk-taking start-ups and SMEs to innovation units in the large-scale industry). Bodies and communities driving standards and data interoperability will be considered as well.	HIGH
Social Innovation Sector: ***Ethical Researchers, Privacy, Security, Legal Agencies, Digital Education Providers, Civil Society Organizations***	
The implementation of heterogeneous digital systems with dynamic recovery and response capabilities is not just a mere technical question. Human and ethical factors are compulsory to facilitate a transformation compliant with human needs. Social innovators identify the challenges, strengthen the opportunities for user-friendliness, and empower a smooth transition to the Future of Work, preventing the continuous adapting to ever-evolving technology.	MEDIUM
Partnerships & Networks: ***ECCC, EIT Digital, NCC, Relevant projects, EU Digital Europe, EU Cybersecurity Associations***	
One of the main intentions of CyberSecDome is to quickly harness the knowledge and capacity of initiatives providing key cybersecurity services and advocating the secure digital transformation of connected networks and information systems. To develop the essential capacities to secure the EU's digital economy, the project will leverage the consortium's leadership and participation in active ecosystems to create synergies, bridging the collaboration between the 'Cybersecurity Ecosystem' and 'Tech Providers'. Segments will include (1) the	MEDIUM

European Cybersecurity Competence Network and Centre (ECCC), which aims to increase Europe's cybersecurity capacities and competitiveness (2) the project will seek interactions with the primary EU communities/centres such as EIT Digital or the NCC. CyberSecDome will (3) build on research results conducted under H2020 SU-DS01-2018, SU-DS04-2018- 2020, SU-DS05-2018-2019 and SU-DS-02-2018 calls (such as AI4HEALTHSEC, Cyber-MAR, FeatureCloud projects); while will interact with (4) associations that concentrate large communities of private-public organisations, generating value and upscaling the cybersecurity competitiveness of SMEs start-ups, research centres, universities e.g. ESCO (5) the flagship initiatives for the emerging European data spaces, e.g. the Data Spaces Support Centre under the Digital Europe Programme, and the brand-new Data Spaces Business Alliance.	
Policymakers: ***EU directives and agencies (ENISA, EU Cybersecurity Act, NIS Directive***	
The members of public bodies and task forces immerse in policy-oriented activities, funding programmes and regulatory laws. They are responsible for setting the rules and public incentives for private and public sectors' safety and security. The primary representative of this category will be the EU Regulators or agencies such as the European Union Agency for Cybersecurity (ENISA), EU Cybersecurity Act, and NIS Directive.	MEDIUM
Society: ***General public, Non-specialised media***	
CyberSecDome will encourage a common understanding and trust of the positive impact of cybersecurity that shifts the focus from technology-driven progress to a thoroughly human-centric and sustainable approach. Highly accessible content will be produced to engage citizens, reinforcing the role that the EU public funding entails to make it happen.	MEDIUM

The aforementioned target groups have been categorised as per their significance (high/medium). The consortium will seek to contribute to those, with the boost productivity, accomplish efficient resource management and improve safety conditions; While they will focus to contribute to initiatives such as policy makers of EU agencies by supporting in enhancing the trustworthiness of connected services, processes, and digital infrastructure. All the partners will support the appropriate communication efforts to allow a wider community to benefit from our experience and results, to broaden project's visibility and to widely share research results with all the relevant external target groups.

4.2 Stakeholders Engagement

CyberSecDome will introduce a holistic system incorporated with AI-empowered cybersecurity tools that will increase the level of knowledge and expertise of key stakeholders in detecting and predicting incidents, diagnosing risks, responding to attacks of interconnected and heterogeneous systems.

The consortium aims to optimise the collaborative response among the stakeholders within the Digital Infrastructure ecosystem by developing privacy-aware information and knowledge-sharing mechanisms.

The targets of dissemination and exploitation strategy are to include the potential users of the CyberSecDome stratification concept, within the Telecommunication industry such as Telecom operators/providers, ICT service providers, Cloud service providers, and Aviation operators. Moreover, as already mentioned above, technology providers are also key stakeholders of CyberSecDome; such as providers from Digital Twins, Cyber Range and Virtual Reality, AI/ML Engineers, Data Scientists from IT sector, Academic Researchers, Cybersecurity service provider and Standardisation Committees. Bodies and communities driving standards and data interoperability will be considered as well. Furthermore, public authorities will be considered, as well as other stakeholders who are directly or indirectly related to project outcomes (e.g., digital infrastructures providers, policymakers, Computer emergency response teams, civil Society, SMEs, and other European related research projects).

WP6 in general will motivate further participation of stakeholders in the project events and promote exchange of experiences and knowledge sharing with related initiatives and take-up of the project results. Initially, these groups will be asked to offer their opinions and observations into the project's progress. Their participation will significantly improve the project's performance. Longer term, it will be crucial to the use of CyberSecDome tools and techniques once the project is completed. The dissemination method, which involves pushing information out ("push out method") to target groups and audiences, is primarily effective when response from these audiences is obtained, as communication is an active, two-way process. This feedback makes it possible to evaluate before moving on with developing the following set of dissemination actions and revising the overall plan.

However, it is worth mentioning that CyberSecDome has reserved a total budget of **1.200.000,00 €** to provide financial support to Third Parties in further extending the project developments, applicability, and integration across the ecosystem of the EU Digital, through the organization of Open Calls. Specifically, the aim is to extend the CyberSecDome use-cases and application domains, addressing sector-specific constraints, ensuring reproducibility, accelerating the CyberSecDome deployment into 3rd parties' infrastructures, and contributing to knowledge transfer to digital infrastructures.

The target beneficiaries are industry parties (including mid-caps and SMEs) that operate Digital Systems and Infrastructures with interest in adopting and using advanced and innovative cybersecurity solutions. In regard to this, a vice versa communication will be established with the possible selected profiles, with enhancing this way the dissemination project outcomes, and contributing to the project's success with the aim of foster a sense of ownership and collaboration among all the involved parties.

A comprehensive report regarding the "Open-Call" will be distributed and delivered on M12 of the project and will include all the methodologies and procedures (D5.2; EIT).

4.3 Scientific Publications

Within the CDEB objectives, and specifically the first one, to raise national and international awareness of the project and its objectives and how to participate in project activities (including virtually) we have defined measures to maximise the impact of project vision towards the external stakeholders and general public.

Therefore, CyberSecDome partners will carefully select publication venues based on their scientific excellence and impact privileged where possible open-access publishing. Indicative conferences and journals that will be targeted include IFIP SEC International Conference on Information Security and Privacy Protection [4] and the IEEE Symposium on Security and Privacy [5], the International Journal of Information Privacy, Security and Integrity [6] and IEEE Transactions on Information Forensics & Security (T-IFS)[7].

[4] IFIP Information Security Conference & Privacy Conference, https://ifipsec.org/

[5] IEEE Symposium on Security and Privacy, https://ieeexplore.ieee.org/xpl/conhome/1000646/all-proceedings

[6] The International Journal of Information Privacy, Security and Integrity, https://www.inderscienceonline.com/toc/ijipsi/current

[7] IEEE Transactions on Information Forensics & Security, https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=10206

The consortium aims to produce >12 scientific publications reflecting the results of the project's demonstrators by targeting the scientific community conducting core or application research on disruption preparedness and resilience of digital infrastructures to enable future advancements and inspire further research based on the project's concept and results.

4.4 Events and Workshops

In order to minimise the possible barriers beyond the scope of the project, CyberSecDome is investing in raising awareness through a number of initiatives. These include among others intensive training activities, organising a series of outreach events and informative sessions addressed to the general public and key stakeholders to change the present perception. CyberSecDome work packages focus on organising events to strengthen the synergies and to facilitate best practices sharing and exchanges.

CyberSecDome's **CDEB plan has four objectives** which are fully presented in the beginning of Section 4. Part of this strategy towards achieving a wider impact beyond the project itself, refers also to the aspects that deal with a broader economic impact and the landscape of cybersecurity business in Europe, leverages business growth activities, particularly building staff and partners capacity, and expanding and diversifying through disruptive products and services. Regarding this, partners will build awareness through organisation and participation in key events, conferences and exhibitions. Partners, and especially SMEs, will seek to join forces with other businesses to promote the new services to new or existing customers or launch them in new geographical areas. This will be achieved through participation in international networking events. This reflects to improving social awareness through the organisation of 5 events and participation in >12 third-party events to communicate the project outcomes. Furthermore, the consortium will organise a series of in person-events including four (4) events (M12, M18, M24, M30 of the project), and a final event (conference session or a workshop) in M36 to present the results of the project. Specific Key Performance Indicators are presented in Section 4.5. Target groups for the organised events will be cybersecurity solution providers, research and academic community and the general public.

CyberSecDome workshops and events will give an extraordinary edge to allow for not only the mere sharing of our experiences, best practices and project key results but also enable selected target audiences to learn, use, be inspired by and take them up.

4.5 Key Performance Indicators

A performance indicator or key performance indicator (KPI) is a type of performance measurement[8]. KPIs evaluate the success of an organization or of a particular activity (such as projects, programs, products and other initiatives) in which it engages. KPIs provide a focus for strategic and operational improvement, create an analytical basis for decision making and help focus attention on what matters most[9].

Our dissemination activities will target not only scientific communities with an interest in CyberSecDome outcomes, but also European user groups, professional bodies, and other types of stakeholders which have been already identified. KPIs are referred also to communication activities which are mainly meant to raise the interest of the different stakeholders and engage end users while receiving feedback for the implementation.

Communication measures and KPIs are presented in the table below, and partners will follow them accordingly during the project lifetime duration. Leveraging on the network effect activated with both dissemination and

[8] Carol Fitz-Gibbon (1990), "Performance indicators", BERA Dialogues (2), ISBN 978-1-85359-092-4.
[9] https://www.kpi.org/KPI-Basics/

communication, the exploitation activities will be specifically devoted to fostering the market potential of products and solutions to be offered to the end-users, while considering different applications for the developed technologies and services.

T6.1 "Communication and dissemination activities" focuses on planning, carrying out and monitoring the dissemination and communication activities of CyberSecDome. This task is led by ITML, and all the partners are contributing into it. The dissemination policy will be planned and monitored through periodic plans and monitoring reports. In this task, we will also actively seek to collect feedback from attendees of our dissemination activities (e.g., seminars, workshops, and conference presentations, PhD schools) and use them to assess the take of our results and the effectiveness of our dissemination strategy. To better monitor all the actions this tables have been circulated to include all the relevant key indicators.

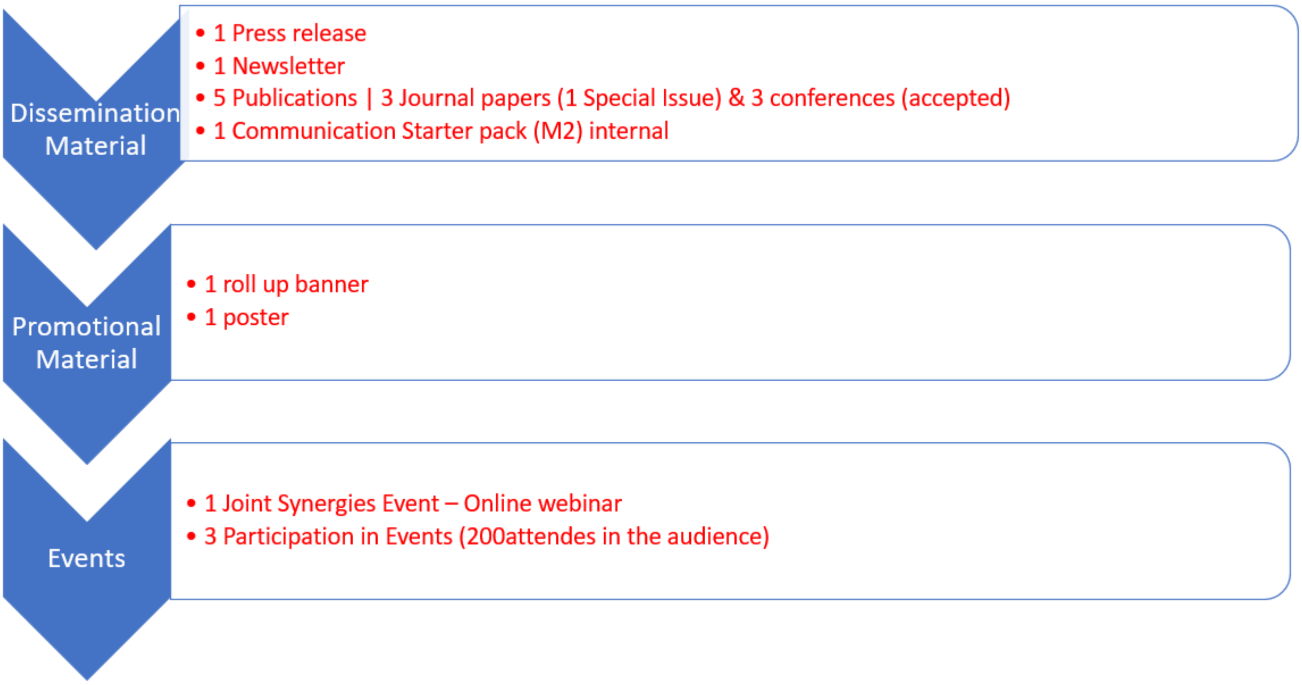
Table 2 - CyberSecDome KPIs table

Partner	Dissemination Activities	Action item	KPIs defined in DoA
ITML, ALL	Dissemination Activities	Twitter	10 push announcements (monthly) 5 new followers (monthly) 20 re-tweets (monthly)
		LinkedIn	10 push ancements (monthly) 5 new followers (monthly) 30 profile view (monthly)
		Website	>20 visitors (monthly) >1000 site access (annually) 500 downloads (by the end of the project)
ITML, ALL	Dissemination Material/ Promotional	Newsletters with technical activities (bi-monthly)	>8 Newsletters
		Electronic Brochures	>1000 downloads of high-quality electronic brochures with the technical approach and activities (by the end of the project)
		5min video	>500 views of 5-min videos on YouTube (by the end of the project)
		Supporting material	>500 downloads
ITML, ALL	Organisation of events (in-person)/material for engagement	Events	4 events (M12, M18, M24, M30), and 1 final event (conference session or a workshop) in M36 to present the results of the project.
		Hard copies in events	>50 hard copies distributed in >5 events
		Policy makers	engagement of >2 policy making bodies
ALL	Participation of events		Participation in >10 small and large-scale events
			>2 events organised (with 70 attendees)
			>20% of participants engaged for further exploitation
			>1 internal training workshop (on the project-developed technologies and CyberSecDome tools)
			≥1 partnership formed with a key business in the field (e.g., Cybersecurity)
ITML&MAG			A communications starter pack will be produced early on (M2) for partners to ensure consistency
			3 versions of the CDEB plan

Partner	Dissemination Activities Action item	KPIs defined in DoA
	CDEB Internal Reports & Communications / Internal reports (by the end of the project)	>15 internal mails with rich information on project progress and DE events & opportunities
		2 reports published with CDEB KPIs that are continuously updated
ALL	Joint cluster synergies/Established links	>3 similarly themed projects identified
		>1 jointly organised clustering workshop
ALL	Publications, Special issues, etc	>3 publications in international refereed journals
		>1 journal special issues
		>3 publications in international magazines
		>6 conference presentations
		>3 publications in international refereed journals

4.6 Summary of WP6 related metrics (M1-M6)

The CyberSecDome project passes through the month 6 now (February 2024). In the below figures we are presenting an overview of the current project's outcomes, to capture what we have achieved so far; where we stand so far in terms of KPIs metrics.



Dissemination Material
- 1 Press release
- 1 Newsletter
- 5 Publications | 3 Journal papers (1 Special Issue) & 3 conferences (accepted)
- 1 Communication Starter pack (M2) internal

Promotional Material
- 1 roll up banner
- 1 poster

Events
- 1 Joint Synergies Event – Online webinar
- 3 Participation in Events (200attendes in the audience)

Figure 14 - WP6 Related Metrics

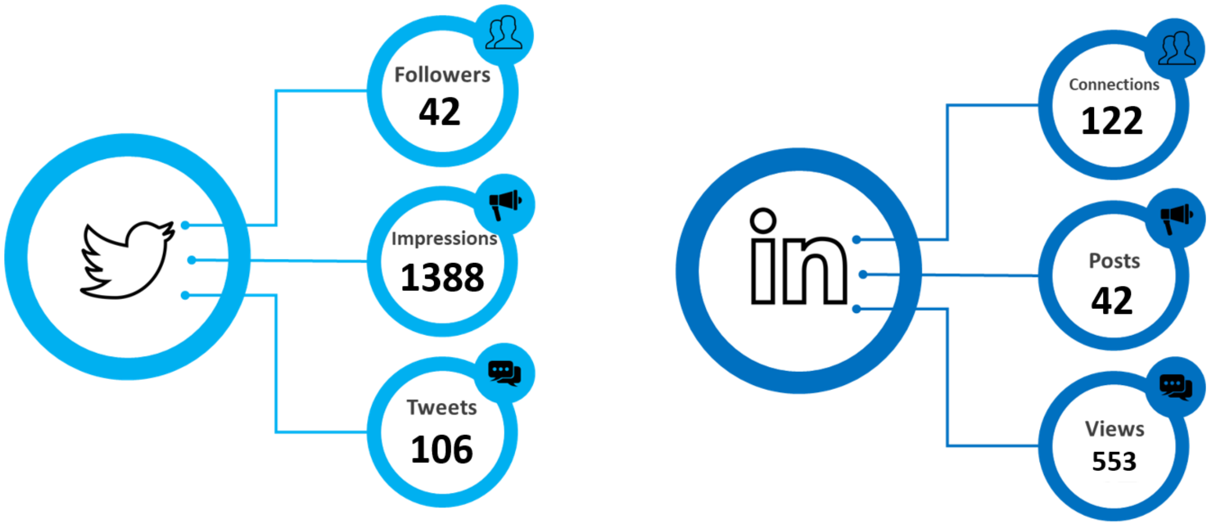


Figure 15 - CyberSecDome Social Media Metrics

4.7 Project Synergies

One of the main intentions of CyberSecDome is to quickly harness the knowledge and capacity of initiatives providing key cybersecurity services and advocating the secure digital transformation of connected networks and information systems. To develop the essential capacities to secure the EU's digital economy, the project will leverage the consortium's leadership and participation in active ecosystems to create synergies with other related projects.

Bringing CyberSecDome's outcomes to the attention of project clusters and policy makers at national and EU level is great way of keeping up the project's vision and scope. Partners of CyberSecDome will set up collaboration mechanisms, liaison, and synergies among multiple cybersecurity-relevant stakeholders to build a people-centric and sustainable digital infrastructure. As well defined in the GA, the project will build on the results gained from research and innovation projects in the area of **cybersecurity of digital infrastructures**; for example, projects funded from ***H2020 SU-DS01-2018, SU-DS04-2018-2020, SU-DS05-2018-2019 and SU-TDS-02-2018***.

The below table describes national and international research and innovation activities which are linked with CyberSecDome, focusing on differentiations and enhancements:

Table 3 – CyberSecDome National and international research and innovation activities

Project details	Project description	Conditions linking to CyberSecDome and results to be reused
AI4HEALTHSE H2020-SU-DS-2018-2019-2020, GA: 883273	A4HEALTHSEC offers an advanced solution that improves the detection and analysis of cyber-attacks and threats on Healthcare Information Infrastructures, increases knowledge of the current cyber security and privacy risks and builds risk awareness, within the digital healthcare ecosystem.	CyberSecDome will benefit from the proposed AI Dynamic Situation Awareness Framework for effective and efficient identification, evaluation, investigation and mitigation methods of realistic risks, threats and multi-dimensional attacks.

Project details	Project description	Conditions linking to CyberSecDome and results to be reused
FeatureCloud, H2020-SU-TDS-02-2018, GA: 826078	FeatureCloud project develops privacy-preserving federated ML mechanisms and advanced AI techniques to address modern cybersecurity challenges, especially for healthcare-related settings.	CyberSecDome will benefit from AI/ML anomaly detection and intrusion prediction techniques.
EnergyShield, H2020-SU-DS04- 2018-2020, GA: 832907	EnergyShield moves on integrating cybersecurity tools in a holistic solution with assessment, monitoring/protection and learning/sharing capabilities that work synergistically.	CyberSecDome will use the proposed efficient synergistic and integrated framework of the implemented systems.
CUREX, H2020-SU-TDS-02-2018, GA: 826404	CUREX focuses on enabling secure and authorized sensitive health data exchange by leveraging novel methods of ontological data modelling, vulnerability discovery, threat intelligence, cybersecurity, and privacy risk assessment methodologies.	CyberSecDome will take advantage of the secure data exchange frameworks, which will be used by the different modules to exchange efficiently and safely their data
ASCLEPIOS, H2020-SU-TDS-02-2018, GA ID: 826093	ASCLEPIOS focuses on designing cloud-based mechanisms and protocols for protecting both corporate and personal sensitive health-based data.	CyberSecDome will benefit from the secure cloud-based encrypted framework so that the different cloud-integrated components can communicate safely with each other.
CUSTODES, HORIZON-CL3-2022-CS-01, GA: 101120684	The CUSTODES system aims to enhance transparency, re-usability, and trust in the certification process of composite ICT products or services. It will achieve this by discovering and translating certification information, providing it to stakeholders, and sharing newly identified vulnerabilities related to specific Building blocks or composite products. Additionally, CUSTODES will utilize a Restricted & Trusted Execution (RTE) Environment to ensure the chain of custody of the product under assessment.	CyberSecDome will significantly benefit from the proposed cybersecurity certification framework outlined in the EU Cybersecurity Act (EUCSA), which also supports trust and security across ICT products, services, and processes.
nIoVe, H2020-SU-ICT-01-2018, GA: 833742	nIoVe aimed to deploy a novel multi-layered interoperable cybersecurity solution for the Internet of Vehicles (IoV) by employing an advanced cybersecurity system enabling stakeholders and incident response teams to share CTIs, coordinate their cyber security response and recovery activities.	CyberSecDome will benefit from the coordinated intrusion response toolkit, trust management and threat intelligence sharing platforms.
Cyber-MAR, H2020-SU-DS01- 2018, GA ID: 833389	Cyber-MAR focused on developing an innovative cybersecurity simulation environment for accommodating the peculiarities of the maritime sector while being easily applicable in other transport subsectors.	CyberSecDome will benefit from the proposed cybersecurity simulation environment for the digital twin simulation/emulation environment of the real system.

The above table indicates a list of related EU projects for possible future collaboration to establish links in cluster level. This is an initial list which will be further examined, and consortium will provide an updated list with projects that seeks to establish synergies through the project lifetime, or those which have been already established during the referenced period. Thus, the D6.2 "Intermediary Report on Dissemination and

Communication Activities", will be submitted on M18, and should refer a section with the achievements towards the collaboration in cluster level.

4.8 Communication and Dissemination Plan

By the 1st plenary meeting of CyberSecDome which has been held on November 2023 (M3), an initial Communication and Dissemination plan has been published to the consortium for better mapping all the dissemination action items.

A regular update of the communication, dissemination and exploitation plan with lessons learnt will take place every year (M12/M24/M36) and be shared to the consortium for internal use. This includes a breakdown of target stakeholder groups, a timeline of key EU/EC-related events, consultations, and policy milestones over the lifetime of the project, with a clear strategy for planned ways to engage with these. Therefore, all the activities that have been occurred will be further presented in each relevant deliverable of WP6 (D6.2, D6.3; and D6.6, D6.7 regarding Exploitation activities).

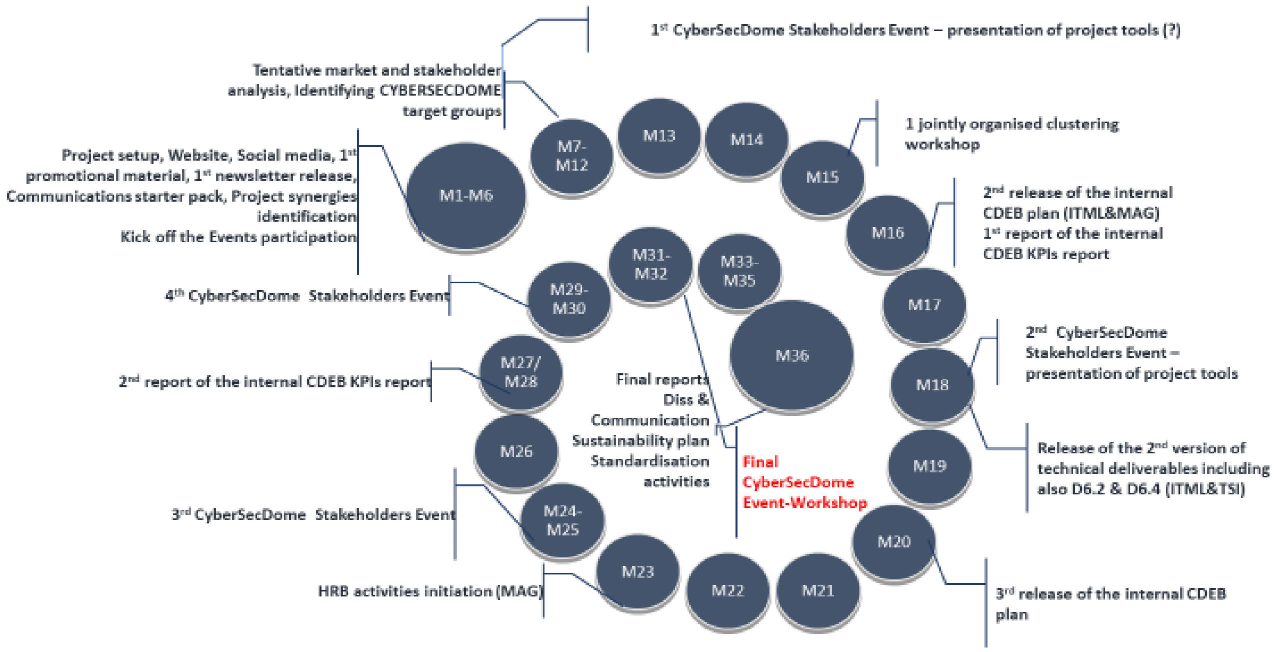

1st CyberSecDome Stakeholders Event – presentation of project tools (?)
Tentative market and stakeholder analysis, Identifying CYBERSECDOME target groups
Project setup, Website, Social media, 1st promotional material, 1st newsletter release, Communications starter pack, Project synergies identification
Kick off the Events participation
1 jointly organised clustering workshop
M1-M6
M7-M12
M13
M14
M15
M16
M17
M18
M19
M20
M21
M22
M23
M24-M25
M26
M27/M28
M29-M30
M31-M32
M33-M35
M36
2nd release of the internal CDEB plan (ITML&MAG)
1st report of the internal CDEB KPIs report
4th CyberSecDome Stakeholders Event
2nd CyberSecDome Stakeholders Event – presentation of project tools
2nd report of the internal CDEB KPIs report
Final reports Diss & Communication Sustainability plan Standardisation activities
Final CyberSecDome Event-Workshop
Release of the 2nd version of technical deliverables including also D6.2 & D6.4 (ITML&TSI)
3rd CyberSecDome Stakeholders Event
HRB activities initiation (MAG)
3rd release of the internal CDEB plan

Figure 16 - CyberSecDome Initial Communication and Dissemination Plan

Conclusions

This deliverable presents the strategy of CyberSecDome towards raising awareness and visibility for the project. It serves as a guide for the CyberSecDome consortium providing the necessary procedures and actions to follow an effective and smooth strategy in terms of collaboration between the partners. In addition, the document provides a clear understanding of the WP6 objectives, and particularly the dissemination and communication activities, that will be undertaken to achieve the objectives and responsibilities. Thus, it should be considered as an asset of internal dissemination among the project partners. In addition, this document is itself an asset of internal dissemination among members of the consortium, providing them with knowledge of each member’s contribution to dissemination assets and actions. Moreover, D6.1 addresses aspects of engaging stakeholders by providing the key audience that CyberSecDome focuses on for potential dissemination activities. For the purpose of achieving successful dissemination and communication activities, project’s performance will be measured based on several indicators, presented in this deliverable.

CyberSecDome partners will establish mechanisms to not only transfer knowledge among the consortium and those external to the project but also to exchange crucial knowledge as part of a two-way process. ITML, as a leader of T6.1, will be in close collaboration and direct communication with all project partners in order to smoothly fulfil the necessary activities. Finally, the future deliverables D6.2 (M18) and D6.3 (M36) will illustrate detailed a report on ‘Dissemination and Communication Activities’, along with an improved communication plan if updates will be occurred.

References

[1]. “Ukraine Conflict: Digital and Cyber Aspects | Digital Watch Observatory.” Link: https://dig.watch/trends/ukraine-conflict-digital-and-cyber-aspects

[2]. Andreas Streim, “German businesses under attack: losses of more than 220 billion euros per year”. Link: German businesses under attack: losses of more than 220 billion euros per year | Presseinformation | Bitkom e. V.

[3]. P. H. O’Neill, “Ransomware did not kill a German hospital patient | MIT Technology Review.”. Link: Ransomware did not kill a German hospital patient | MIT Technology Review.

[4]. Carol Fitz-Gibbon (1990), "Performance indicators", BERA Dialogues (2), ISBN 978-1-85359-092-4.

[5]. Weilkiens, Tim; Weiss, Christian; Grass, Andrea; Duggen, Kim Nena (2016). "Frameworks". *OCEB 2 Certification Guide*. Elsevier. pp. 149–169. doi:10.1016/b978-0-12-805352-2.00007-8. ISBN 9780128053522.

[6]. "What is a Key Performance Indicator (KPI)". KPI.org. Retrieved 1 January 2022. Link: https://www.kpi.org/KPI-Basics/.