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.

D6.2 – Intermediary Report on Dissemination and Communication Activities

Editor(s): Anna Maria Anaxagorou

Beneficiary: ITML

Version: 1.0

Status: Final

Delivery date: 25/02/2025

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:	D6.2 Intermediary report on Dissemination and Communication Strategy Activities
Related WP:	WP6 Dissemination, Exploitation and Sustainability
Due Date:	28/02/2025

Editor(s):	Anna Maria Anaxagorou (ITML), Vina Rompoti (ITML)
Contributor(s):	ALL partners
Reviewer(s):	Kostas Drakonakis (TUC), Spyros Fotis (AEGIS)
Approved by:	All Partners

Executive Summary

This document has been developed as part of Task 6.1 of the CyberSecDome project, which encompasses communication and dissemination activities. Specifically, it outlines the dissemination and communication efforts undertaken during the first 18 months of the project.

The purpose of the dissemination and communication strategy is to effectively organize the necessary activities to meet the project's objectives. Key objectives include:

- Creating the project's visual identity, which encompasses traditional informational materials, digital tools (including the project website and social media) and audio-visual content (such as videos and podcasts).
- Participating in and organizing outreach initiatives, international events (e.g., conferences and workshops) and information days.
- Developing and supporting activities for launching CyberSecDome Open Call.
- Establishing a robust dissemination and communication strategy that the project consortium can follow to raise awareness and connect with relevant target audiences.

To evaluate the effectiveness of the dissemination and communication activities, the dissemination KPIs have been analyzed and documented. These KPIs will be monitored regularly to ensure that the project's goals and desired impacts, as initially defined, are being achieved.

Document History

Version	Date	Author(s)	Comments
0.1	13/12/2024	Anna Maria Anaxagorou (ITML)	Table of Contents
0.2	19/01/2025	ALL partners	Contribution in Sections 2, 3 and 5
0.3	07/02/2025	Anna Maria Anaxagorou (ITML), Vina Rompoti (ITML)	Draft ready for internal review
0.4	12/02/2025	Spyros Fotis (AEGIS)	Peer review
0.5	14/02/2025	Kostas Drakonakis (TUC)	Peer review
0.6	17/02/2025	Anna Maria Anaxagorou (ITML), Vina Rompoti (ITML)	Integrating review comments
0.7	21/02/2025	Haris Mouratidis (SLC)	Quality check
1.0	24/02/2025	Anna Maria Anaxagorou (ITML), Vina Rompoti (ITML)	Final version ready for submission

Table of Contents

List of Figures

List of Tables

Acronyms and Abbreviations

AI	Artificial Intelligence
CDEB	Communication, Dissemination, Exploitation and Business Growth
KPI	Key Performance Indicator
ECCC	European Cybersecurity Competence Centre
GA	Grant Agreement
IPR	Intellectual Property Right
KER	Key Exploitable Result
ML	Machine Learning
NCC	National Coordination Centres
NLP	Natural Language Processing
OS	Open Science
SOTA	State-of-the-art
SME	Small and Medium-sized Enterprise
TG	Target Group
TL	Task Leader
VR	Virtual Reality
WP	Work Package
XAI	eXplainable AI

1 Introduction

1.1 Purpose and Scope

The primary goal of this deliverable is to provide an overview of the communication and dissemination activities carried out as part of the CyberSecDome project during its first 18 months. The report showcases the progress made in engaging stakeholders, raising awareness and sharing knowledge about the project's activities and main achievements so far. It covers targeted communication and dissemination measures designed to enhance the visibility of the developed AI-enhanced cybersecurity solutions and promote their adoption. Finally, it highlights collaboration with key stakeholders, including academia, industry, policymakers and general public through diverse channels such as workshops, webinars, publications and events.

1.2 Contribution to other Deliverables

This deliverable plays a central role in shaping and guiding the dissemination and communication activities within the CyberSecDome project. By establishing clear objectives and methods for information sharing, it enhances the effectiveness of various project deliverables and work packages, particularly those related to dissemination efforts, such as D6.1 "Dissemination and Communication Strategy". Additionally, it refers to deliverables D5.2, D5.3 and D5.4, which are identified as Open Call deliverables, focusing on how these efforts have been communicated to potential applicants. Through this process, the deliverable guarantees that essential project outcomes, research findings and achievements are efficiently conveyed to relevant stakeholders, thus aiding in the fulfilment of milestones across different deliverables.

Building on the dissemination and communication strategy detailed in D6.1, this report highlights the progress made in implementing those initial plans and shows how activities have evolved to ensure continued impact. Together, D6.1 and this report provide a unified approach to communication and dissemination, ensuring active stakeholder engagement, fostering collaboration and improving the project's visibility and overall impact.

1.3 Structure of the Document

The deliverable, is structured int the following way:

- **Section 1** provides an overview of the deliverable's purpose, scope and objectives.
- **Section 2** describes the dissemination activities carried out during the first 18 months of the project, including completed publications and event participation.
- **Section 3** focuses on the communication efforts made during the first 18 months, outlining the strategies and tools used to engage stakeholders.
- **Section 4** presents the current status and performance of all CDEB Key Performance Indicators (KPIs), reflecting the effectiveness of the dissemination and communication efforts.
- **Section 5** outlines the planned dissemination and communication activities for the remainder of the project, including upcoming events and initiatives the CyberSecDome consortium partners intend to participate in.
- **Section 6** summarises the key findings of the deliverable and provides a roadmap for future dissemination and communication efforts.

2 Dissemination activities until M18

2.1 Scientific publications

Scientific publications are important in sharing knowledge and expanding the reach of the CyberSecDome project. The academic partners in the project collaborate to enhance the impact of dissemination efforts by preparing and publishing research articles. These publications contribute to the broader scientific community while also showcasing the project's advancements.

The following tables list the publications and conference proceedings authored by CyberSecDome partners directly linked to the project. Additionally, Sections 2.1.1 through 2.1.15 provide a detailed overview of each publication and conference proceeding, including the title, abstract and a Zenodo link for easy access.

Table 1: Publications in International journals and magazines

Responsible Partner(s)	Paper Title	DOI/URL	Date	Views / Downloads
ARU	Federated Learning-based Personalised Recommendation Systems: An Overview on Security and Privacy Challenges	https://doi.org/10.1109/tce.2023.3318754	September, 2023	54 / 33
ARU & MAG	Cyber threat assessment and management for securing healthcare ecosystems using natural language processing (Special Issue)	https://doi.org/10.1007/s10207-023-00769-w	October, 2023	30 / 28
ARU	Digital twins-enabled zero touch network: A smart contract and explainable AI integrated cybersecurity framework	https://doi.org/10.1016/j.future.2024.02.015	February, 2024	82 / 42
MAG	A Stakeholder Needs Analysis in Cybersecurity: A Systemic Approach to Enhancing Digital Infrastructure Resilience	https://doi.org/10.3390/businesses4020015	June, 2024	38 / 25
ARU	Generative AI and Cognitive Computing-Driven Intrusion Detection System in Industrial CPS	https://doi.org/10.1007/s12559-024-10309-w	June, 2024	42 / 28
TUM	REACT: Autonomous Intrusion Response System for Intelligent Vehicles	https://doi.org/10.1016/j.cose.2024.104008	June, 2024	78 / 47
ARU & MAG	Adoption of Deep-Learning Models for Managing Threat in API Calls with Transparency	https://doi.org/10.3390/s24154859	June, 2024	12 / 13

Responsible Partner(s)	Paper Title	DOI/URL	Date	Views / Downloads
	Obligation Practice for Overall Resilience			
ARU	Vulnerability detection using BERT based LLM model with transparency obligation practice towards trustworthy AI	https://doi.org/10.1016/j.mlwa.2024.100598	December, 2024	13 / 13

Table 2: Conference Papers

Responsible Partner(s) & Conference Name	Paper title	DOI/URL	Status	Views / Downloads
TUM | IEEE International Conference on Computer Communications (IEEE INFOCOM 2024)	PTPsec: Securing the Precision Time Protocol Against Time Delay Attacks Using Cyclic Path Asymmetry Analysis	https://zenodo.org/records/14806692	Published	8 / 8
TUM | 2024 IEEE 27th International Symposium on Real-Time Distributed Computing (ISORC)	Securing Real-Time Systems using Schedule Reconfiguration	https://zenodo.org/records/14806788	Published	10 / 9
TUM | 35th IEEE Intelligent Vehicles Symposium (IEEE IV)	Advanced IDPS Architecture for Connected and Autonomous Vehicles	https://zenodo.org/records/14806852	Published	10 / 10
ARU, MAG | 20th AIAI (Artificial Intelligence Applications and Innovations)	Enhancing Malware Detection through Machine Learning using XAI with SHAP Framework	https://zenodo.org/records/14832484	Published	6 / 1
ARU, MAG | 20th AIAI (Artificial Intelligence Applications and Innovations)	Synthetic Data Generation and Impact Analysis of Machine Learning Models for Enhanced Credit Card Fraud Detection	https://zenodo.org/records/14832599	Published	-
IMT | (NOMS 2024-2024 IEEE Network Operations and Management Symposium)	Similarity-Based Selective Federated Learning for Distributed Device-Specific Anomaly Detection	*No open access / TBA*	Published	-
IMT, TUM | (NOMS 2024-2024 IEEE	Shells Bells: Cyber-Physical Anomaly	https://zenodo.org/records/14807181	Published	32 / 24

Responsible Partner(s) & Conference Name	Paper title	DOI/URL	Status	Views / Downloads
Network Operations and Management Symposium)	Detection in Data Centers			
AEGIS, TUM | IEEE Conference on Standards for Communications and Networking (CSCN 2023)	*Creating a Security Enforcement Environment for a Vehicular Platform*	*Not available yet*	*Accepted*	-
TUM | International Conference on Computational Technologies and Electronics (ICCTE-2023)	*Security Challenges in Autonomous Systems Design*	*Not available yet*	*Accepted*	-
TUM | 025 IEEE/ACM 19th Symposium on Software Engineering for Adaptive and Self-Managing Systems (SEAMS)	*Analysis of Autonomous Driving Software to Low-Level Sensor Cyber Attacks*	*Not available yet*	*Accepted*	-
TUM | DATE 2025	*Cybersecurity Challenges of Autonomous Systems*	*Not available yet*	*Accepted*	-
CyberSecDome consortium | DATE 2025	*CyberSecDome – Framework for Secure, Collaborative and Privacy-Aware Incident Handling for Digital Infrastructure*	*Not available yet*	*Accepted*	-

2.1.1 Publication #1

"Federated Learning-based Personalised Recommendation Systems: An Overview on Security and Privacy Challenges". Zenodo Link.

Abstract—*The recent advancement in next-generation Consumer Electronics (CE) has created the problems of information overload and information loss. The significance of Personalised Recommendation Systems (PRS) to efficiently and effectively extract useful user information is seen as an ideal solution to provide users with personalised content and services and therefore is used in different application domains including healthcare, e-commerce, social media, etc. Security and privacy are the two major challenges of the existing PRS for next-gen CE data. Federated learning (FL) has the potential to elevate the aforementioned challenges by sharing local recommender parameters while keeping all the training data on the device and therefore is seen as a promising technique to enhance security and privacy in PRS for the next-gen CE data. In this survey, we have first discussed the enhancement of the existing CE technologies, a holistic review of security and privacy challenges in current PRS and the advantage of FL-based PRS for next-gen CE. Finally, we list a few open issues and challenges that can guide researchers and practitioners to further drive research in this promising area.*

2.1.2 Publication #2

"Cyber threat assessment and management for securing healthcare ecosystems using natural language processing. International Journal of Information Security, 23, pages 31–50 (Special Issue)". Zenodo Link.

Abstract—*The healthcare sectors have constantly faced significant challenge due to the rapid rise of cyber threats. These threats can pose any potential risk within the system context and disrupt the critical healthcare service delivery. It is therefore necessary for the healthcare organisations to understand and tackle the threats to ensure overall security and resilience. However, threats are continuously evolving and there is large amount of unstructured security-related textual information is available. This makes the threat assessment and management task very challenging. There are a number of existing works that consider Machine Learning models for detection and prediction of cyber-attack but they lack of focus on the Natural Language Processing (NLP) to extract the threat information from unstructured security-related text. To this end, this work proposes a novel method to assess and manage threats by adopting natural language processing. The proposed method has been tailored for the healthcare ecosystem and allows to identify and assess the possible threats within healthcare information infrastructure so that appropriate control and mitigation actions can be taken into consideration to tackle the threat. In detail, NLP techniques are used to extract the useful threat information related to specific assets of the healthcare ecosystems from the largely available security-related information on Internet (e.g. cyber security news), to evaluate the level of the identified threats and to select the required mitigation actions. We have performed experiments on real healthcare ecosystems in Fraunhofer Institute for Biomedical Engineering, considering in particular three different healthcare scenarios, namely implantable medical devices, wearables and biobank, with the purpose of demonstrating the feasibility of our approach, which is able to provide a realistic manner to identify and assess the threats, evaluate the threat level and suggest the required mitigation actions.*

2.1.3 Publication #3

"Digital twins-enabled zero-touch network: A smart contract and explainable AI integrated cybersecurity framework. Future Generation Computer Systems (T. 156, July 2024, pp. 191–205)". Zenodo Link.

Abstract—*Data-driven modeling using Artificial Intelligence (AI) is envisioned as a key enabling technology for Zero Touch Network (ZTN) management. Specifically, AI has shown huge potential for automating and modeling the threat detection mechanism of complicated wireless systems. The current data-driven AI systems, however, lack transparency and accountability in their decisions and assuring the reliability and trustworthiness of the data collected from participating entities is an important obstacle to threat detection and decision-making. To this end, we integrate smart contracts with eXplainable AI (XAI) to design a robust cybersecurity framework for ZTN. The proposed framework uses a blockchain and smart contract-enabled access control and authentication mechanism to ensure trust among the participating entities.*

2.1.4 Publication #4

"A Stakeholder Needs Analysis in Cybersecurity: A Systemic Approach to Enhancing Digital Infrastructure Resilience". Zenodo Link.

Abstract—*The escalating complexity and sophistication of cyber threats necessitate advanced solutions that not only counteract these threats but also proactively adapt to the evolving needs of diverse stakeholders involved in digital infrastructures, such as telecom operators, cloud service providers and end-users in sectors like healthcare and finance. This research addresses a crucial gap by focusing on a systemic, AI-powered approach to stakeholder needs analysis in cybersecurity. By aligning closely with stakeholder requirements, the proposed framework aims to offer dynamic, responsive cybersecurity solutions that enhance the resilience of digital infrastructures against evolving cyber threats. This research systematically maps the landscape of stakeholder needs in cybersecurity across different sectors through qualitative methods like interviews and focus groups, supplemented by data from the CyberSecDome project's pilot cases and open calls. Requirements for an AI-driven framework are then formulated based on these data to identify patterns and predict stakeholder needs. The*

analysis reveals critical challenges faced by stakeholders, including limited threat intelligence sharing, insufficient automation in incident response and regulatory hurdles related to data protection laws and evolving cybersecurity legislation. There is a strong interest in leveraging AI for enhanced intrusion detection, real-time threat intelligence sharing and privacy-preserving information exchange.

2.1.5 Publication #5

"Generative AI and Cognitive Computing-Driven Intrusion Detection System in Industrial CPS". Zenodo Link.

Abstract—*Industrial Cyber-Physical Systems (ICPSs) are becoming more and more networked and essential to modern infrastructure. This has led to an increase in the complexity of their dynamics and the challenges of protecting them from advanced cyber threats have escalated. Conventional intrusion detection systems (IDS) often struggle to interpret high-dimensional, sequential data efficiently and extract meaningful features. They are characterised by low accuracy and a high rate of false positives. In this article, we adopt the computational design science approach to design an IDS for ICPS, driven by Generative AI and cognitive computing. Initially, we designed a Long Short-Term Memory-based Sparse Variational Autoencoder (LSTM-SVAE) technique to extract relevant features from complex data patterns efficiently. Following this, a Bidirectional Recurrent Neural Network with Hierarchical Attention (BiRNN-HAID) is constructed. This stage focuses on proficiently identifying potential intrusions by processing data with enhanced focus and memory capabilities. Next, a Cognitive Enhancement for Contextual Intrusion Awareness (CE-CIA) is designed to refine the initial predictions by applying cognitive principles. This enhances the system's reliability by effectively balancing sensitivity and specificity, thereby reducing false positives. The final stage, Interpretive Assurance through Activation Insights in Detection Models (IAA-IDM), involves the visualisations of mean activations of LSTM and GRU layers for providing in-depth insights into the decision-making process for cybersecurity analysts. Our framework undergoes rigorous testing on two publicly accessible industrial datasets, ToN-IoT and Edge-IIoTset, demonstrating its superiority over both baseline methods and recent state-of-the-art approaches.*

2.1.6 Publication #6

"REACT: Autonomous Intrusion Response System for Intelligent Vehicles". Zenodo Link.

Abstract—*Autonomous and connected vehicles are rapidly evolving, integrating numerous technologies and software. This progress, however, has made them appealing targets for cybersecurity attacks. As the risk of cyber threats escalates with this advancement, the focus is shifting from solely preventing these attacks to also mitigating their impact. Current solutions rely on vehicle security operation centers, where attack information is analysed before deciding on a response strategy. However, this process can be time-consuming and faces scalability challenges, along with other issues stemming from vehicle connectivity. This paper proposes a dynamic intrusion response system integrated within the vehicle. This system enables the vehicle to respond to a variety of incidents almost instantly, thereby reducing the need for interaction with the vehicle security operation center. The system offers a comprehensive list of potential responses, a methodology for response evaluation and various response selection methods. The proposed solution was implemented on an embedded platform. Two distinct cyberattack use cases served as the basis for evaluating the system. The evaluation highlights the system's adaptability, its ability to respond swiftly, its minimal memory footprint and its capacity for dynamic system parameter adjustments. The proposed solution underscores the necessity and feasibility of incorporating dynamic response mechanisms in smart vehicles. This is a crucial factor in ensuring the safety and resilience of future smart mobility.*

2.1.7 Publication #7

"Adoption of Deep-Learning Models for Managing Threat in API Calls with Transparency Obligation Practice for Overall Resilience". Zenodo Link.

Abstract—System-to-system communication via Application Programming Interfaces (APIs) plays a pivotal role in the seamless interaction among software applications and systems for efficient and automated service delivery. APIs facilitate the exchange of data and functionalities across diverse platforms, enhancing operational efficiency and user experience. However, this also introduces potential vulnerabilities that attackers can exploit to compromise system security, highlighting the importance of identifying and mitigating associated security risks. By examining the weaknesses inherent in these APIs using security open-intelligence catalogues like CWE and CAPEC and implementing controls from NIST SP 800-53, organisations can significantly enhance their security posture, safeguarding their data and systems against potential threats. However, this task is challenging due to evolving threats and vulnerabilities. Additionally, it is challenging to analyse threats given the large volume of traffic generated from API calls. This work contributes to tackling this challenge and makes a novel contribution to managing threats within system-to-system communication through API calls. It introduces an integrated architecture that combines deep-learning models, i.e., ANN and MLP, for effective threat detection from large API call datasets. The identified threats are analysed to determine suitable mitigations for improving overall resilience. Furthermore, this work introduces transparency obligation practices for the entire AI life cycle, from dataset preprocessing to model performance evaluation, including data and methodological transparency and SHapley Additive exPlanations (SHAP) analysis, so that AI models are understandable by all user groups. The proposed methodology was validated through an experiment using the Windows PE Malware API dataset, achieving an average detection accuracy of 88%. The outcomes from the experiments are summarised to provide a list of key features, such as FindResourceExA and NtClose, which are linked with potential weaknesses and related threats, in order to identify accurate control actions to manage the threats.

2.1.8 Publication #8

"Vulnerability detection using BERT based LLM model with transparency obligation practice towards trustworthy AI". Zenodo Link.

Abstract—*Vulnerabilities in the source code are one of the main causes of potential threats in software-intensive systems. There are a large number of vulnerabilities published each day and effective vulnerability detection is critical to identifying and mitigating these vulnerabilities. AI has emerged as a promising solution to enhance vulnerability detection, offering the ability to analyse vast amounts of data and identify patterns indicative of potential threats. However, AI-based methods often face several challenges, specifically when dealing with large datasets and understanding the specific context of the problem. Large Language Model (LLM) is now widely considered to tackle more complex tasks and handle large datasets, which also exhibits limitations in terms of explaining the model outcome and existing works focus on providing overview of explainability and transparency. This research introduces a novel transparency obligation practice for vulnerability detection using BERT based LLMs. We address the black-box nature of LLMs by employing XAI techniques, unique combination of SHAP, LIME, heat map. We propose an architecture that combines the BERT model with transparency obligation practices, which ensures the assurance of transparency throughout the entire LLM life cycle. An experiment is performed with a large source code dataset to demonstrate the applicability of the proposed approach. The result shows higher accuracy of 91.8 % for the vulnerability detection and model explainability outcome is highly influenced by "vulnerable", "function", "mysql_tmpdir_list", "strmov" tokens using both SHAP and LIME framework. Heatmap of attention weights, highlights the local token interactions that aid in understanding the model's decision points.*

2.1.9 Conference paper #1

"PTPsec: Securing the Precision Time Protocol Against Time Delay Attacks Using Cyclic Path Asymmetry Analysis". Zenodo Link.

Abstract—*High-precision time synchronisation is a vital prerequisite for many modern applications and technologies, including Smart Grids, Time-Sensitive Networking (TSN) and 5G networks. Although the Precision Time Protocol (PTP) can accomplish this requirement in trusted environments, it becomes unreliable in the presence of specific cyber-attacks. Mainly, time delay attacks pose the highest threat to the protocol, enabling attackers to diverge targeted clocks undetected. With the increasing danger of cyber-attacks, especially against critical infrastructure, there is a great demand for effective countermeasures to secure both time synchronisation and the applications that depend on it. However, current solutions are not sufficiently capable of mitigating sophisticated delay attacks. For that, we provide a method to find redundant paths in arbitrary networks and show how this redundancy can be exploited to reveal and mitigate undesirable asymmetries on the synchronisation path that cause the malicious clock divergence. Furthermore, we propose PTPsec, a secure PTP protocol and its implementation based on the latest IEEE 1588-2019 standard.*

2.1.10 Conference paper #2

"Securing Real-Time Systems using Schedule Reconfiguration". Zenodo Link.

Abstract—*Modern real-time systems are susceptible to cyberattacks. The growing adoption of multi-core platforms, where safety and non-safety critical tasks coexist, further introduces new security challenges. Existing solutions suffer from either a lack of determinism or excessive cost. This paper addresses these shortcomings and proposes an offline analysis to compute all feasible schedules for real-time tasks running on a multi-core platform, isolating compromised tasks while guaranteeing a failure operational system and low-cost reconfigurable scheduling. Our experimental results using a UAV autopilot system on a quad-core platform (Raspberry Pi) demonstrate that the proposed scheme incurs run-time recovery overhead at the level of microseconds. Also, the reconfiguration process covers up to 100% of all possible responses for compromised tasks in the synthetic test cases.*

2.1.11 Conference paper #3

"Advanced IDPS Architecture for Connected and Autonomous Vehicles". Zenodo Link.

Abstract—*Highly connected and automated driving technologies have ushered digital transformation and flexibility to modern cars. However, the vehicle's attack surface has significantly expanded due to increased connectivity. To address this problem, automotive manufacturers are adopting more secure practices driven by standards and regulations. In addition to the deployed cryptographically strong security measures in automotive, we need an Intrusion Detection and Prevention System (IDPS) that actively monitors the vehicle for intrusions, prevents them and provides notification, as required by UN Regulation No. 155. In this work, we aim to identify the current limitations of the existing automotive approaches and contribute to an advanced IDPS solution. We propose architectural changes that improve reliability and form a framework to propose reactions in a safety-related automotive context. We evaluate our proposed architecture with regard to performance and security design. With the proposed changes to the IDPS architecture, our aim is to integrate a dynamic and adaptive strategy for IDPS, enhancing resilience against emerging threats and vulnerabilities.*

2.1.12 Conference paper #4

"Enhancing Malware Detection through Machine Learning using XAI with SHAP Framework". Zenodo Link.

Abstract—*Malware represents a significant cyber threat that can potentially disrupt any activities within an organisation. There is a need to devise effective proactive methods for malware detection, thereby minimising the associated risks. However, this task is challenging due to the ever-growing volume of malware data and the continuously evolving techniques employed by malicious actors. In this context, machine learning models offer a promising approach to identify key malware features and facilitate accurate detection. Machine learning has proven to be effective in detecting malware and has recently gained widespread attention from both the academic and research sectors. Despite their effectiveness, current research on machine learning (ML) models for malware detection often lacks necessary explanations for the selection of key features. This opacity of ML models can complicate the understanding of the outputs, errors and decision-making processes. To address this challenge, this research uses Explainable AI (XAI), particularly the SHAP framework, to enhance transparency and interpretability. By providing extensive insights into how each feature contributes to the model's conclusions, the approach further improves the model's accountability. An experiment was conducted to demonstrate the applicability of the proposed method, beginning with the training of the chosen machine learning models, including Random Forest, Adaboost, Support Vector Machine and Artificial Neural Network, for detecting malware and concluding with the explanation of the decision-making process using XAI techniques.*

2.1.13 Conference paper #5

"Synthetic Data Generation and Impact Analysis of Machine Learning Models for Enhanced Credit Card Fraud Detection". Zenodo Link.

Abstract—*The financial industry is currently experiencing a substantial shift in its operating landscape as a result of the swift integration of technology. This transformation brings with it potential risks and challenges. Heightened occurrence of online fraud is one the key concerns for this sector, which has been exacerbated by the growing prevalence of online payment methods on e-commerce platforms and other websites. The identification of credit card fraud is a challenging task due to nature of imbalanced transactional data to detect and predict any fraudulent activities. In this context, this paper provides a unique approach to create synthetic dataset to tackle imbalanced issue for credit card fraud detection. The approach adopts Synthetic Minority Over-sampling Technique (SMOTE) technique for data generation. An experiment is performed using a number of ML models including SVM, KNN and Random Forest to demonstrate the feasibility of using synthetic data. In this study, we have combined resampling techniques like SMOTE for oversampling the minority class with ensemble methods and appropriate evaluation metrics like the F1-score to improve the imbalanced data. The result from the experiment compared with widely used public datasets to evaluate the model performance. The analysis reveals a significant imbalance in the real ULB dataset, with the positive class (frauds) comprising a mere 0.172% of all transactions. The findings clearly show that the Random Forest model performs better than other modes with outstanding precision, recall, accuracy and F1 score values to detect fraudulent transactions and reduce false positives.*

2.1.14 Conference paper #6

"Similarity-Based Selective Federated Learning for Distributed Device-Specific Anomaly Detection". Zenodo published link will be announced.

Abstract—*Resource constraints and heterogeneity make securing the IoT a challenge. Device-specific AD can address these challenges. Depending on the algorithm used, training device-specific models takes time. This makes it difficult to bootstrap new devices. Transfer learning via federated learning and model aggregation can speed up the creation of AD models. The novel approach implements an automatic selection of similar devices and creates an aggregated model for new devices. The evaluation uses the UNSW NB 15 dataset. The results*

show good performance and >90% reduction in bootstrapping time. The approach also satisfies security concerns as it mitigates injection attacks by not using too different models for aggregation.

2.1.15 Conference paper #7

"Shells Bells: Cyber-Physical Anomaly Detection in Data Centers". Zenodo Link.

Abstract—*Monitoring the side-channel sound can improve anomaly detection (AD) in data centers (DCs). However, a DC's dense setup results in a composite soundscape which makes it difficult to attribute sounds to individual devices. We propose a novel cyber-physical AD approach that validates device activity in realistic composite audio signals. By leveraging information from management network traffic, we predict changes in the DC soundscape. We use a convolutional neural network to compare our predictions with real observations to validate correct device activity and identify anomalies. Our evaluation using data from a real DC environment identifies spoofed and masqueraded activity with an accuracy of 98.62%.*

2.2 Events organised by CyberSecDome

Aiming at sharing knowledge and engaging key stakeholders, multiple dissemination events have been organised by the **CyberSecDome** partners, which are listed in the table below.

Table 3: Events organised by the CyberSecDome partners

Event	Date	Month	Location	Partner(s)
"Cybersecurity Matters" by CyberSecDome & Custodes EU projects	February 2024	M6	Online	EIT & ITML
CyberSecDome (Internal) Workshop | The EU Artificial Intelligence Act (AI Act)	April 2024	M8	Online	AEGIS (& all partners)
1st Open Call Info Day	July 2024	M11	EIT Digital, Brussels	EIT (& all partners)
6th edition of the Future IoT PhD School | Hackathon workshops by CyberSecDome partners	October 2024	M14	IMT, Paris, France	IMT & TUM (& ITML)
2nd Info Day & Open Call Launch event	December 2024	M16	ITML	ITML (& all partners)
1st Open Call Webinar	January 2025	M17	Online	AEGIS (& all partners)
2nd Open Call Webinar (Q&A Submission)	February 2025	M18	Online	AEGIS (& all partners)

2.3 Participation in Third-Party events

During the referenced period (M1-M18), partners have also participated in third-party events. CyberSecDome's members seized the opportunity to spread information about our project and develop a network among interested stakeholders in several dissemination events. These activities are listed in the table below:

Table 4: Third-party events attended

Event	Partner	Date	No. of participants	Location	Link
Here. We. Go – The Future Industry Forum	IMT, TUM	17 October 2023	≈50	Munich, Germany	https://www.future-industry.org/herewego23/
GFA Flag Attack 2023 The French-German Capture the Flag (CTF)	IMT, Airbus	5-6 December 2023	≈50	Paris, France	https://www.future-industry.org/ctf23-recap/
Infocom World 2023	OTE, ITML	14 December 2023	>500	Athens, Greece	https://infocomworld.gr/en/
Cybersecurity Meetup	OTE, TUC, AEGIS, STS	14 February 2024	>300	Athens Greece	https://cybersecdome.eu/cybersecdome-cybersecurity-meetup-at-ote-innovation-center/
14th InfoCom Security 2024 Conference	OTE, ITML, AEGIS	10-11 April 2024	>1000	Athens, Greece	https://www.infocomsecurity.gr/
"Cybersecurity First" Event	EIT	23 April 2024	≈500	Budapest, Hungary	https://cybersecdome.eu/cybersecdome-at-eit-digitals-cybersecurity-first-event/
South Summit 2024	EIT	5-7 June 2024	>2000	Madrid, Spain	https://www.southsummit.io/madrid/
CyberSecDome in "Talk.Cybercni.fr" – Your monthly Cybersecurity Speaker Series	IMT, LiU	28 June 2024	≈80	Online	https://cybersecdome.eu/2024/07/15/cybersecdome-in-talk-cybercni-fr/
20th International Conference on Artificial Intelligence Applications	OTE, ARU, SLC	27-30 June 2024	≈50	Corfu, Greece	https://ifipaiai.org/2024/

Event	Partner	Date	No. of participants	Location	Link
and Innovations (AIAI)					
First Workshop on Real-Time Autonomous Systems Security	TUM	09 July 2024	≈50	Lille, France	https://www.ecrts.org/rtautosec-2024/
2nd CyberSecDome in "Talk.Cybercni.fr" – Your monthly Cybersecurity Speaker Series	IMT, ARU	26 July 2024	≈100	Online	https://cybersecdome.eu/talk-cybercni-fr-2nd-session/
CyberHOT Summer School	ITML	9-10 September 2024	≈100	Piraeus, Athens	https://www.cyberhot.eu/
European Big Data Value Forum 2024	OTE	2-4 October 2024	>2000	Budapest, Hungary	https://european-big-data-value-forum.eu/2024-edition/
26th InfoCom World Conference Digital Greece: Time for a Leap!	OTE, ITML, AEGIS	12 November 2024	>1000	Athens Greece	https://infocomworld.gr/en/
European Cyber Week 2024	MAG, TUC, ITML	18-20 November 2024	>1000	Rennes, France	https://www.european-cyber-week.eu/en
DATAMITE Meet Up	OTE, ITML, MAG	06 February 2025	≈400	Athens, Greece	https://datamite-horizon.eu/2025/01/27/save-the-date-datamite-meet-up-event/

Below, we present the CyberSecDome events in which partners organized or participated **in person**. These events included presentations, either at booths or as keynote speakers.

2.3.1 Event #1 – CyberSecDome at "Here. We. Go – The Future Industry Forum"

CyberSecDome made its debut at the "Here. We. Go – The Future Industry Forum", held on October 17th, 2023. The event was organised by the German - French Academy for the Industry of the Future (GFA) and provided a platform to showcase cutting-edge advancements in industrial innovation. During the event, Marc-Oliver Pahl

from IMT Atlantique and Mr. Mohammad Hamad from the Technical University of Munich (TUM), the Technical Manager of CyberSecDome, introduced the project to the audience. They presented CyberSecDome's first official poster, highlighting the project's objectives and innovative approach to cybersecurity.

Figure 1: CyberSecDome at "Here. We. Go – The Future Industry Forum"

2.3.2 Event #2 - CyberSecDome at the GFA Flag Attack 2023 – A French-German Event

CyberSecDome participated in the GFA Flag Attack 2023, a Capture the Flag (CTF) event held on December 5-6, 2023, at Campus Cyber in La Défense, Paris. Organised by the German - French Academy for the Industry of the Future (GFA), Airbus Defense & Space, Programme de Transfert au Campus Cyber and Inria, the event brought together students from the Institut Mines-Télécom (IMT) Schools in France and the Technical University of Munich (TUM) in Germany. Airbus provided the CTF challenges and infrastructure, enhancing the event's success. During a keynote session, Marc-Oliver Pahl (IMT Atlantique) and Sébastien Peynet (Airbus) presented CyberSecDome, emphasising its role in cybersecurity innovation.

Figure 2: CyberSecDome at GFA Flag Attack 2023

2.3.3 Event #3 - CyberSecDome at the Infocom World 2023 Conference

CyberSecDome was represented at the Infocom World 2023 Conference on December 14, 2023, in Athens. OTE, a key partner in the CyberSecDome consortium, along with ITML, the Dissemination & Communication task leader, showcased the project at their booth. A digital assistant avatar, developed by the IT Innovation Center of OTE Group, also accompanied them at the booth, further highlighting the project's innovative approach.

Figure 3: CyberSecDome at Infocom World 2023

2.3.4 Event #4 - CyberSecDome at the Cybersecurity Meetup

On February 14, 2024, a pivotal Cybersecurity Meetup was hosted by our partner OTE, at their IT Innovation Center. This event brought together experts from academia, research, public authorities and the legal fields, offering a valuable platform for networking and knowledge exchange. CyberSecDome partners, including Technical University of Crete, AEGIS and Sphynx, collaborated to explore innovative solutions and foster collaborative opportunities in the field of cybersecurity. CyberSecDome was also prominently featured with its banner and avatar, providing attendees with detailed information about the project’s objectives and impact.

Figure 4: CyberSecDome at the Cybersecurity Meetup

2.3.5 Event #5 - CyberSecDome at the 14th Infocom Cybersecurity 2024 Conference

On April 10-11, 2024, CyberSecDome participated in the 14th InfoCom Security 2024 Conference at the Athens Conservatory. Partners OTE, ITML and AEGIS joined the event to boost the project's visibility. During the conference, Mr. Nikos Kogios from OTE delivered a presentation titled "CyberSecDome: Use of AI & VR in Offensive & Defensive Cybersecurity", highlighting the integration of AI and VR in OTE pilot scenarios. The presentation demonstrated how these technologies enhance cybersecurity. As the project progresses, more updates will follow, ensuring CyberSecDome stays at the forefront of cybersecurity innovation.

Figure 5: CyberSecDome at the 14th Infocom Cybersecurity 2024 Conference

2.3.6 Event #6 - CyberSecDome at EIT Digital's 'Cybersecurity First' Event

On April 23, 2024, CyberSecDome participated in the EIT Digital "Cybersecurity First" event, held at EIT Digital's offices in Budapest. The event gathered stakeholders from academia, research and industry to discuss upcoming cybersecurity challenges and explore collaboration opportunities. A key takeaway from the discussions was: "There is no technology without cybersecurity; tech must always be secure." During the event, Mrs. Annalisa Andaloro shared insights into CyberSecDome's vision, architecture and the upcoming Open Call.

Figure 6: CyberSecDome at EIT Digital's 'Cybersecurity First' Event

2.3.7 Event #7 - CyberSecDome at South Summit 2024

From June 5 to 7, 2024, CyberSecDome partner EIT Digital had a booth at South Summit 2024 in Madrid. During the summit, EIT Digital engaged with numerous visitors, sharing exciting opportunities related to the upcoming Open Call for validating CyberSecDome technology. The discussions were productive, fostering new connections and potential collaborations. EIT Digital was inviting further discussions at the EIT House in Brussels on July 3rd for the first Info Day on the CyberSecDome Open Call.

Figure 7: CyberSecDome at South Summit 2024

2.3.8 Event #8 - CyberSecDome at the 20th International Federation for Information Processing (IFIP)

CyberSecDome recently participated in the 20th IFIP AIAI – International Conference on Artificial Intelligence Applications and Innovations, held at Ionian University in Corfu, from June 27 to 30, 2024. The event, organised under the umbrella of IFIP WG12.5, is a prestigious platform for global researchers. OTE, Anglia Ruskin University and Security Labs representatives showcased the CyberSecDome project at the conference with the latter delivering the keynote talk 'AI and Cybersecurity: Friend or Foe?' highlighting the evolving relationship between artificial intelligence and cybersecurity. Additionally, our partners presented two research papers: 'Enhancing Malware Detection through Machine Learning using XAI with SHAP Framework' and 'Synthetic Data Generation

and Impact Analysis of Machine Learning Models for Enhanced Credit Card Fraud Detection'. CyberSecDome also participated in a panel discussion organised by the EU-project DATAMITE on June 28th, 2024, alongside experts from various European projects discussing the impact of data and its monetisation across industries.

Figure 8: CyberSecDome at the 20th IFIP AIAI Conference

2.3.9 Event #9 – First Workshop on Real-Time Autonomous Systems Security

On July 9, 2024, CyberSecDome participated in the First Workshop on Real-Time Autonomous Systems Security (RTAutoSec 2024), held in Lille, France, in conjunction with ECRTS 2024. The workshop focused on the security, resilience and privacy challenges of modern autonomous systems, covering topics such as real-time constraints, adversarial threats and AI-driven security solutions. As a supporting EU project, CyberSecDome contributed to discussions on enhancing cybersecurity for real-time autonomous systems, emphasizing the importance of secure architectures and proactive defense mechanisms. The event gathered leading researchers and industry experts, fostering collaboration on innovative security approaches.

Figure 9: CyberSecDome in the First Workshop on Real-Time Autonomous Systems Security

2.3.10 Event #10 – CyberSecDome at CyberHOT Summer School 2024

CyberSecDome participated in the CyberHOT Summer School at the University of Piraeus to promote cybersecurity awareness and engage with future cybersecurity professionals. Our team showcased the project through roll-ups and flyers while attending insightful presentations on pen-testing, incident response and OSINT weaponisation. The event included hands-on training sessions where participants explored cybersecurity communication strategies, securing critical software and defending against evolving threats. It was a great opportunity to share CyberSecDome's vision and collaborate with experts in the field.

Figure 10: CyberSecDome at CyberHOT Summer School 2024

2.3.11 Event #11 - CyberSecDome at the 6th Future IoT PhD School 2024 in Paris

CyberSecDome participated in the 6th Future IoT PhD School held at Campus Cyber in Paris from September 30th to October 4th, 2024. Organised by IMT Atlantique and Technical University of Munich, the event brought together PhD students and researchers to explore cutting-edge IoT developments and foster collaboration between academia and industry. CyberSecDome was featured prominently with a keynote by our Technical Coordinator from Technical University of Munich, who showcased the project's AI-based security tools and integrated architecture. ITML partners engaged students in an exciting Hackathon and delivered a keynote on secure IoT supply chains, highlighting the role of Federated Learning in cybersecurity.

Figure 11: CyberSecDome at the 6th Future IoT PhD School 2024

2.3.12 Event #12 - CyberSecDome at the European Big Data Value Forum 2024

CyberSecDome participated in the European Big Data Value Forum 2024, held from October 2 to 4, 2024 in Budapest, Hungary. As BDVA's flagship event, EBDVF brought together the European data-driven AI research and innovation community. At the event, CyberSecDome was proudly showcased at our partner OTE's booth, featuring our CyberSecDome avatar and a project video. This provided attendees with a chance to explore our cutting-edge cybersecurity solutions. Additionally, OTE delivered an insightful talk on AI in Telecoms: The Data Challenge, emphasising emerging technologies and innovative solutions.

Figure 12: CyberSecDome at EBDVF 2024

2.3.13 Event #13 - CyberSecDome at the 26th InfoCom World Conference

CyberSecDome was featured at the OTE booth during the 26th InfoCom World Conference on November 12, 2024. The event provided an excellent opportunity to highlight our collaboration with OTE and showcase the innovative cybersecurity solutions driving the project. Mr. Fotis Stathopoulos from OTE presented

"CyberSecDome - Added Values from a Pilot", discussing OTE's cybersecurity scenarios and ITML's Federated Learning approach for secure AI model training. The session also introduced the CyberSecDome Open Call, led by AEGIS IT RESEARCH and encouraged stakeholders to join the upcoming Open Call Info Day on December 4, 2024, to explore opportunities in cybersecurity innovation.

Figure 13: CyberSecDome at the 26th InfoCom World Conference

2.3.14 Event #14 - CyberSecDome at European Cyber Week 2024 in Rennes

CyberSecDome participated in the European Cyber Week 2024, held in Rennes from November 18 to 20. At the booth we showcased the project's latest advancements in cybersecurity, including the upcoming Open Call and Info Day. Attendees had the opportunity to engage with our team, learn about CyberSecDome's mission to enhance digital security across Europe and discover how they can collaborate on cutting-edge initiatives. The event served as a platform to share insights, distribute our new Open Call flyer and invite stakeholders to join the CyberSecDome Info Day on December 4, 2024, in Athens and online, to explore funding opportunities and further strengthen the European cybersecurity ecosystem.

Figure 14: CyberSecDome at European Cyber Week 2024

2.3.15 Event #15 - CyberSecDome at DATAMITE Meet Up Event

CyberSecDome participated in the DATAMITE Meetup 2025, hosted by the OTE Group's IT Innovation Center, an exceptional networking event that brought together Europe's leading researchers, industry professionals and policymakers under the theme 'Bridging Research and Industry in EU-funded Innovation.' Held on February 6, 2025, at OTE's headquarters in Athens, Greece, the meetup facilitated five insightful panel discussions addressing critical areas such as data ethics, privacy, cybersecurity, AI, IoT and sustainable innovation.

Participants explored the opportunities and challenges of data marketplaces, innovative monetisation strategies within the health sector and the data-driven transformation across various industries. The CyberSecDome partners had the opportunity to engage with attendees at our booth, where we shared our vision, project objectives and discussed the exciting opportunities available through the CyberSecDome Open Call.

Figure 15: CyberSecDome at DATAMITE Meet Up Event

2.4 Clustering activities

The goal of this strategy was to plan and execute collaborative activities with relevant projects, initiatives and networks. These efforts utilised multiple channels, including the project website, as well as the extensive connections and networking profiles of the CyberSecDome partners, who are actively engaged in various consortia and networks. To kick off the initiative, an online search was conducted to identify similar projects within CyberSecDome's thematic area, followed by initial contact with several project representatives.

To ensure meaningful synergies, it was crucial to identify areas of complementarity between CyberSecDome and these projects, as well as shared objectives. Establishing common ground not only enhances the project's visibility but also strengthens stakeholder engagement. A list of projects with which connections have been established so far is provided below.

During the reporting period, significant efforts were made to identify shared interests and foster collaboration with related projects. Early in the project, CyberSecDome initiated this process with the CUSTODES project by co-organising the webinar "Cybersecurity Matters." In subsequent months, CyberSecDome collaborated with SecAwarenessTruss to share a booth at conferences and expos, jointly presenting their vision and methodologies on cybersecurity (related post). Additionally, consortium partners participated in an international conference, sharing a booth with the DATAMITE project (related post) and contributing to a panel discussion that brought together experts from multiple European projects, including EloquenceAI, 6G-PATH, AMBITIOUS Project, Smart5Grid Project. This panel highlighted the importance and monetisation of data across industries.

As CyberSecDome approaches the halfway point of its duration, efforts have been expanded to establish communication with additional projects to co-organise a joint clustering webinar. This initiative, involving projects funded under Horizon Europe, the Research and Innovation Programme and the European Union's Digital Europe Programme, will feature collaborations with SYNAPSE, CUSTODES, PHOENI2X, SecAwarenessTruss, CONSOLE and CRACoWi. Details of future clustering activities are outlined in Section 0. Additionally, the outcomes of these activities will be elaborated upon in the final project report, the deliverable D6.3, titled "Final Report on Dissemination and Communication Activities", within the WP6.

3 Communication activities until M18

The communication strategy of CyberSecDome encompasses a range of planned activities aimed at effectively promoting project results to diverse audiences, including stakeholders, media and public. These activities foster awareness and engagement while facilitating a two-way exchange of information to ensure that key stakeholders remain well-informed about the project's objectives and developments.

During this reporting period, various communication and promotional materials have been produced and made available on the project's website, including:

- CyberSecDome branding materials (roll-ups, leaflets, posters, press releases)
- Videos and podcasts highlighting key project insights
- Project newsletters providing updates on progress and achievements

3.1 Branding material

The CyberSecDome branding material developed within the first 18 months is presented in the table below and also in **APPENDIX I - Branding material,** .

Table 5: CyberSecDome branding materials

Type of Material	Date	Month	Link
1st Poster	November 2023	M3	https://cybersecdome.eu/wp-content/uploads/2023/11/CYBERSECDOME_1stPoster_Nov2023.pdf
CyberSecDome Roll-up	December 2023	M4	https://cybersecdome.eu/wp-content/uploads/2023/12/CyberSecDome-Roll-up.pdf
CyberSecDome Flyer A5	December 2023	M4	https://cybersecdome.eu/wp-content/uploads/2024/01/CyberSecDome-Flyer.pdf
Tri-fold Brochure	April 2024	M8	https://cybersecdome.eu/wp-content/uploads/2024/12/CyberSecDome-2nd-Press-Release-Dec2024.pdf
Open Call 2nd Info Day Flyer	November 2024	M15	https://cybersecdome.eu/wp-content/uploads/2024/11/CyberSecDome-Open-Call-flyer.pdf

The poster and roll-up were updated to include information about the project's YouTube channel and the latest partner logos during the project's duration.

3.2 Video/Podcasts

During the M1-M18 period of the project, CyberSecDome produced a promotional video to introduce the project's goals, vision and expected impact. This video has been shared on the project's website and YouTube channel to enhance visibility and outreach. In regard to Open Call needs, CyberSecDome is preparing targeted promotional material, including an Open Call podcast, to effectively communicate funding opportunities to

potential applicants. Throughout the Open Call period, the CyberSecDome consortium will provide supplementary videos and podcasts for participants as necessary.

Table 6: CyberSecDome videos/podcasts

Type of Material	Date	Month	Link
CyberSecDome Promotional Video 	July 2024	M11	https://www.youtube.com/watch?v=B9sFGX31slQ
CyberSecDome Info Day Highlights & Open Call Launch Recap 	Dec 2024	M16	https://www.youtube.com/shorts/CJOJFYGTME8
CyberSecDome Open Call Podcast 	February 2025	M18	https://www.youtube.com/watch?v=ysnOpKvRA9Y&t=142s&ab_channel=CYBERSECDOME-EUproject

3.3 Social Media channels

We actively engage with our audience through various social media platforms, including LinkedIn, X, YouTube and Zenodo. These channels allow us to share updates, promote our initiatives and foster discussions with our community.

3.3.1 CyberSecDome X

CyberSecDome's X account (@cybersecdome_eu) actively shares project updates, event highlights and cybersecurity insights. With 80 followers as of M18, the account fosters engagement and visibility within the cybersecurity and AI research community.

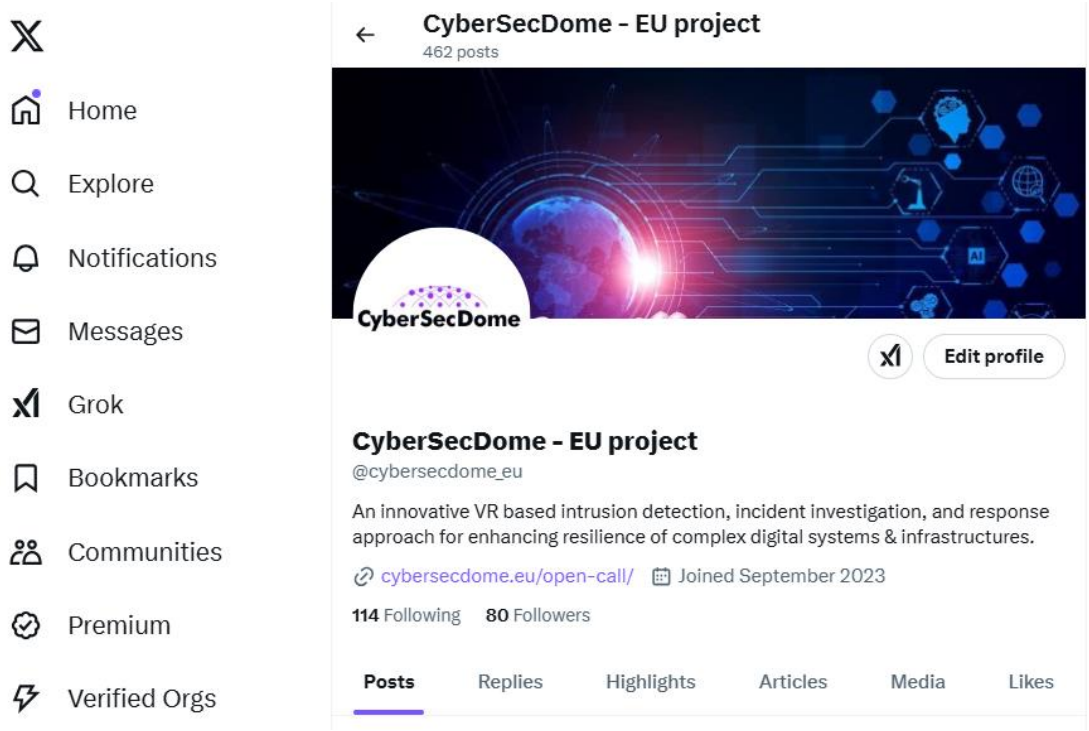


Figure 16: CyberSecDome X profile (link)

3.3.2 CyberSecDome LinkedIn

CyberSecDome's LinkedIn page (@CyberSecDome - EU project) connects with industry professionals, researchers, and policymakers, sharing key developments, open calls, and collaboration opportunities. Additionally, the page serves as a platform for discussions among members of the CyberSecDome LinkedIn group, fostering dialogue on important topics in cybersecurity. As of M18, the page has 609 followers, reflecting strong interest in the project's impact on European cybersecurity.

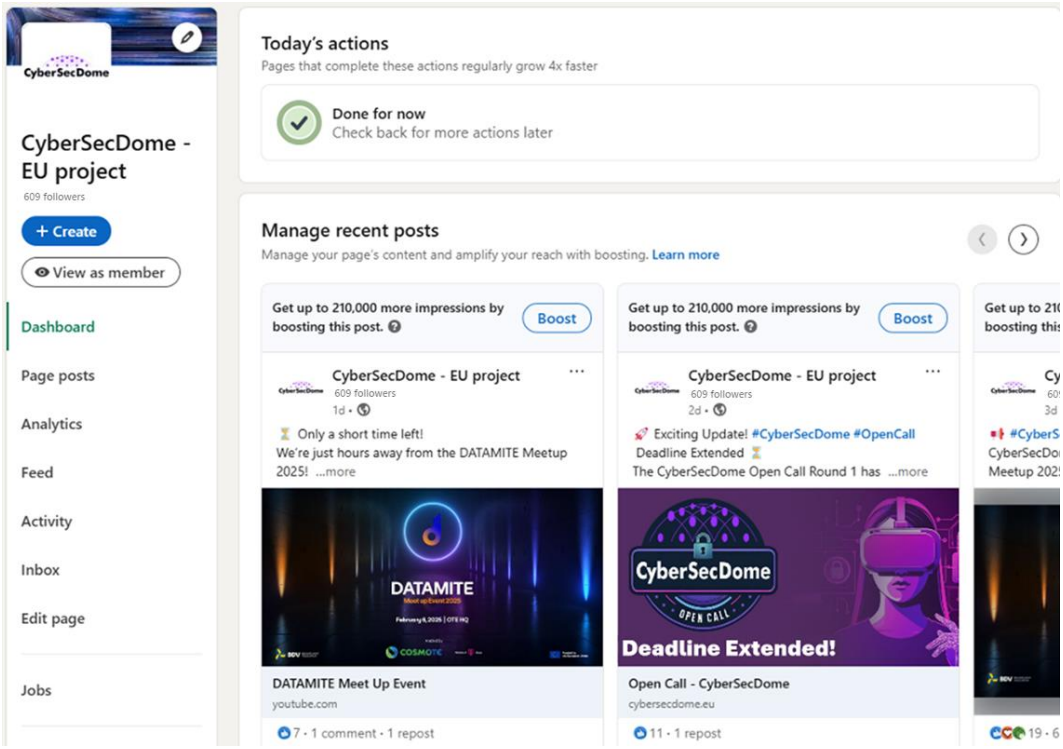


Figure 17: CyberSecDome LinkedIn profile (link)

3.3.3 CyberSecDome YouTube

The CyberSecDome YouTube channel (@CyberSecDome-EUproject-2023) hosts promotional videos, webinars and technical insights related to the project. This video-based content helps communicate complex cybersecurity concepts in an accessible way, reaching a broader audience.

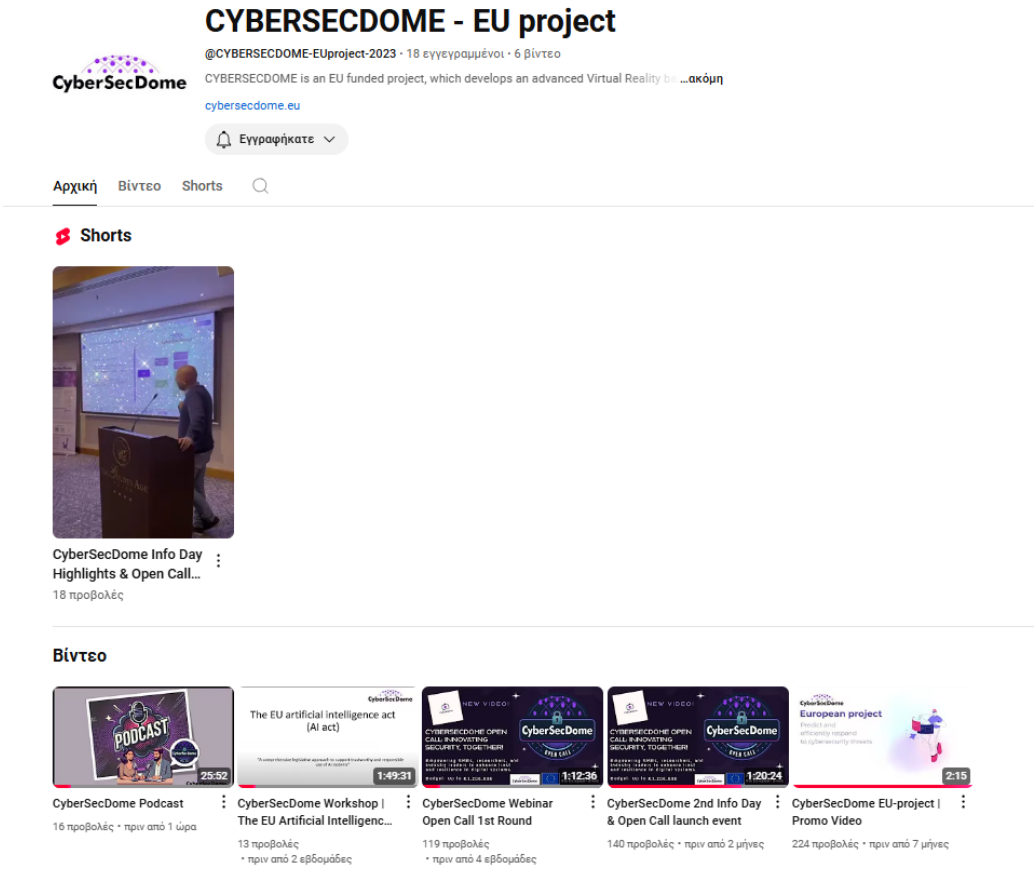


Figure 18: CyberSecDome YouTube channel (link)

3.3.4 CyberSecDome Zenodo

CyberSecDome maintains a presence on Zenodo, where we upload project deliverables, publications and other research outputs. This platform allows us to share our work with the broader academic and research community, ensuring that our contributions are easily accessible and open for collaboration. As of M18, our content has received 415 views and 281 downloads, demonstrating the reach and impact of our shared materials.

Figure 19: CyberSecDome Zenodo Community

3.4 Newsletters/Press Releases

Another key dissemination tool is the CyberSecDome newsletter, along with press releases. The purpose of the newsletter is to provide concise updates on the project's progress, covering technical developments, publications and other dissemination and communication activities. The newsletters are prepared by ITML with

input and contributions from all project partners. With 64 subscribers so far, the plan is to release at least one edition every three to four months, while continuously expanding our content database.

Table 7: CyberSecDome newsletters

Type of Material	Date	Month	Link
1st Press Release	November 2023	M3	https://cybersecdome.eu/wp-content/uploads/2023/11/CyberSecDome-Press-Release-Nov2023.pdf
Newsletter #1	January 2024	M5	https://cybersecdome.eu/wp-content/uploads/2024/01/1st-Newsletter-ITML-Final.pdf
Newsletter #2	May 2024	M9	https://cybersecdome.eu/wp-content/uploads/2024/05/2nd-Newsletter.pdf
Newsletter #3	September 2024	M13	https://cybersecdome.eu/wp-content/uploads/2024/09/3rd-Newsletter.pdf
Newsletter #4	December 2024	M16	https://cybersecdome.eu/wp-content/uploads/2024/12/4th-Newsletter.pdf
2nd Press Release	December 2024	M16	https://cybersecdome.eu/wp-content/uploads/2024/12/CyberSecDome-2nd-Press-Release-Dec2024.pdf

3.5 Open Call Communication Activities

3.5.1 Open Call Webpage

The CyberSecDome project website (https://cybersecdome.eu/) is the major channel for dissemination and communication, providing easy access to project-related information and resources. Launched in M2, the website is managed and hosted by ITML and plays a key role in making project outputs publicly available.

The website is regularly updated to reflect project news, upcoming events, scientific publications, submitted and accepted deliverables and various promotional materials. These updates help maintain engagement and ensure that stakeholders stay informed about the project's progress.

CyberSecDome created a dedicated webpage (https://cybersecdome.eu/open-call/) to support the Open Call process, providing an overview of the call, including its objectives, eligibility criteria and key deadlines. A button on this page directs visitors to the CyberSecDome Open Call Application Page (https://cybersecdome.eu/open-call-application-page/), where applicants can explore the available topics, find the templates and submit their proposals.

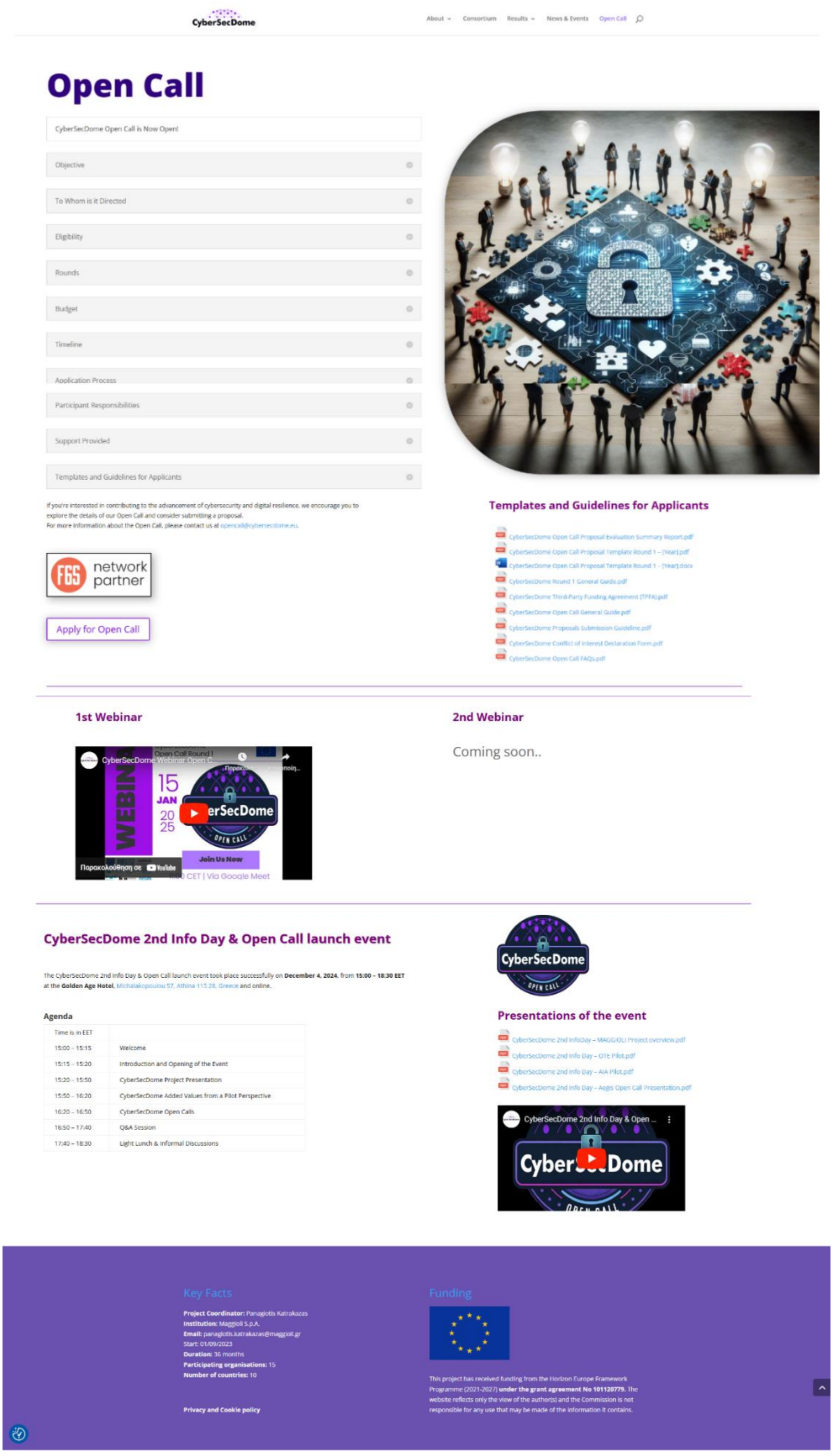


Figure 20: CyberSecDome Open Call Website

Figure 21: CyberSecDome Open Call Application Webpage

3.5.2 LinkedIn Open Call Group

CyberSecDome established a dedicated LinkedIn Group to foster engagement with potential applicants, stakeholders and cybersecurity professionals. The group serves as a platform for discussions, sharing updates about the Open Call, exploring relevant topics and addressing inquiries from interested participants.

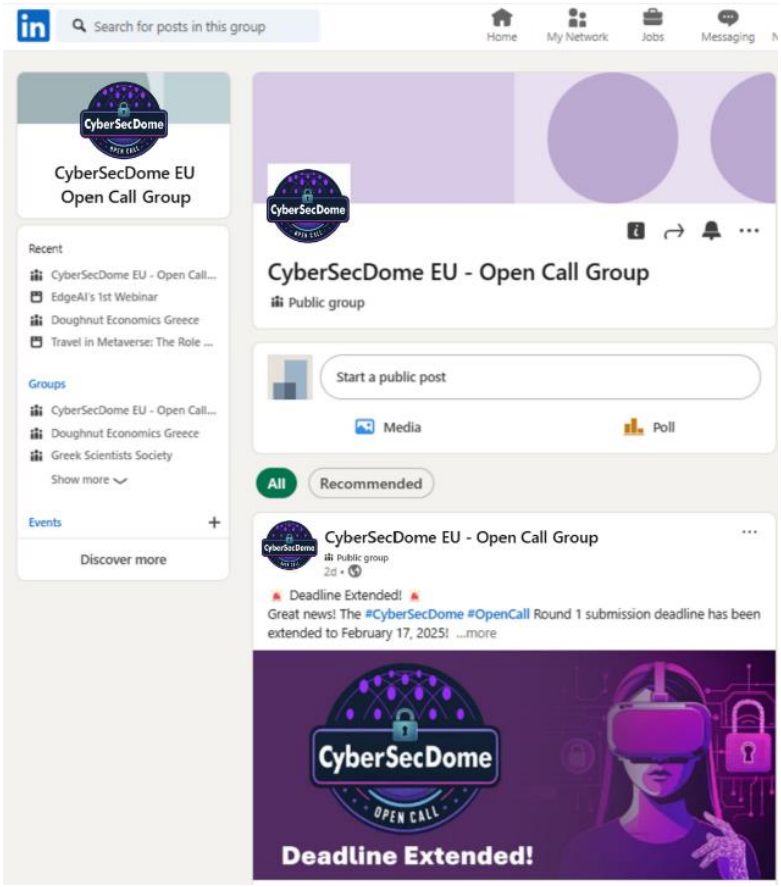


Figure 22: CyberSecDome LinkedIn Open Call Group

3.5.3 Mailchimp Campaigns

Mailchimp campaigns play a crucial role in our communication strategy. We have used Mailchimp to send targeted emails for various purposes, including promoting events such as the Info Days and Open Call webinars. The recipients of these emails are subscribers to our newsletter, ensuring that our messages reach an engaged audience. These campaigns help ensure wide dissemination of project updates and facilitate engagement with our stakeholders. The emails are carefully crafted to provide clear, relevant information and encourage participation in project-related activities.

Table 8: Mailchimp campaigns launched by CyberSecDome

Type of Material	Date	Month	Link
CyberSecDome Info Day	June 2024	M9	https://mailchi.mp/1b4d21b83d1b/cybersecdome-info-day
CyberSecDome 2nd Info Day & Open Call Launch Event	November 2024	M15	https://mailchi.mp/831083e3f915/cybersecdome-2nd-info-day

Type of Material	Date	Month	Link
Invitation to CyberSecDome Open Call Webinar	January 2025	M17	https://mailchi.mp/f0a77a135c84/cybersecdome-open-call-1st-webinar
CyberSecDome Open Call Deadline Extended!	February 2025	M18	https://mailchi.mp/dcddf7277dc9/cybersecdome-open-call-deadline-extended

3.5.4 Open Call Dissemination events organised by CyberSecDome

Aiming at sharing knowledge about CyberSecDome Open Call and engaging key stakeholders, multiple dissemination events have been organised by the CyberSecDome partners, which are listed in the table below.

Table 9: Events organised by the CyberSecDome partners

Event	Date	Month	Location	Partner
1st Open Call Info Day	July 2024	M11	EIT Digital, Brussels	EIT Digital (& all partners)
2nd Info Day & Open Call Launch event	December 2024	M16	ITML, Athens, Greece & Online	ITML (& all partners)
1st Open Call Webinar	January 2025	M17	Online	AEGIS (& all partners)
2nd Open Call Webinar (Q&A Submission)	February 2025	M18	Online	AEGIS (& all partners)

3.5.4.1 CyberSecDome 1st Open Call Info Day

On July 3, 2024, CyberSecDome held its 1st Info Day at the EIT Digital House in Brussels. The event featured presentations from pilot entities OTE Group and Athens International Airport (AIA). OTE partner discussed telecom sector attack scenarios, while partners from AIA shared the challenges faced within their dynamic digital ecosystem. The event welcomed nearly 20 participants. EIT Digital and AEGIS IT Research introduced the upcoming Open Call, explaining participation details. The session included a Q&A, fostering engagement. The Open Call launched in December 2024, inviting third parties to test and validate CyberSecDome's solutions.

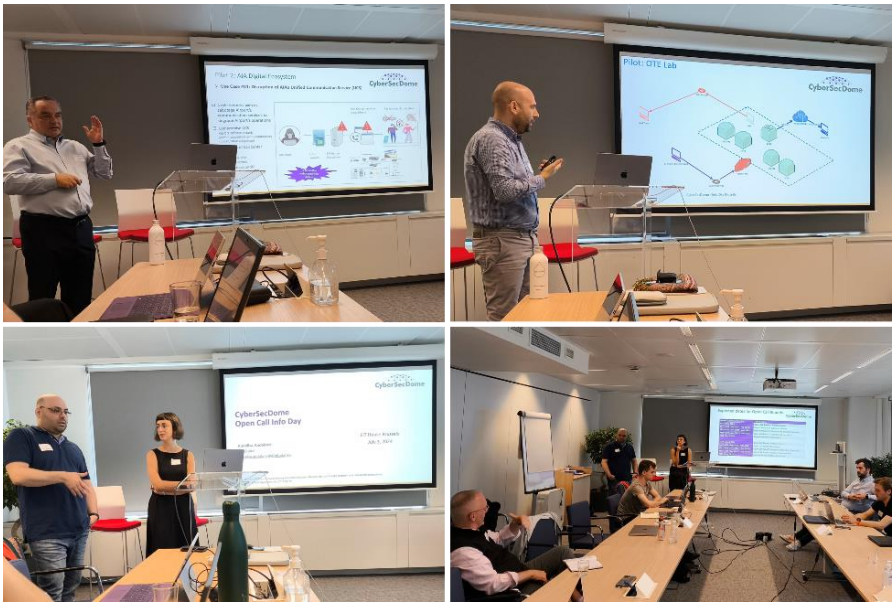


Figure 23: CyberSecDome 1st Info Day

3.5.4.2 CyberSecDome 2nd Info Day & Open Call Launch event

On December 4, 2024, CyberSecDome hosted its 2nd Info Day & Open Call Launch in Athens, Greece. The event introduced the project's objectives, innovation capacities and attack scenarios within digital ecosystems. A dedicated session detailed the Open Call, offering funding of up to €120K per proposal to support SMEs and industry stakeholders. Attendees engaged in meaningful discussions on cybersecurity challenges, application processes and funding opportunities. The Open Call Info Day concluded with a dynamic networking session, fostering collaboration and the exchange of ideas. With nearly 30 participants attending in person and over 50 joining online, the event created a vibrant, interactive atmosphere, further strengthening the cybersecurity community. It is worth to mentioning that 70% of the participants expressed interest in submitting proposals.

Figure 24: CyberSecDome 2nd Info Day & Open Call Launch event

3.5.4.3 CyberSecDome 1st Open Call Webinar

On January 15, 2025, CyberSecDome successfully hosted its 1st webinar, attracting 50 registrants eager to explore the Open Call. The session highlighted how CyberSecDome solutions can be integrated into various digital infrastructures and guided participants through the application process, evaluation criteria and project expectations. The event attracted SMEs, startups and industry experts interested in advanced cybersecurity solutions. Participants engaged in a Q&A session with the project's technical partners to address key inquiries. The webinar recording and presentation slides are available on our website.

Figure 25: CyberSecDome 1st Open Call Webinar

3.5.4.4 CyberSecDome 2nd Open Call Webinar (Q&A Submission)

On February 12, 2025, CyberSecDome hosted its 2nd Open Call Webinar, offering a live Q&A session for applicants. The event provided valuable insights into the Open Call's objectives, CyberSecDome tools and proposal guidelines. Participants had the opportunity to ask administrative, technical and strategic questions directly to the core technical team. SMEs, research organisations and technology providers were encouraged to refine their proposals before the final submission deadline.

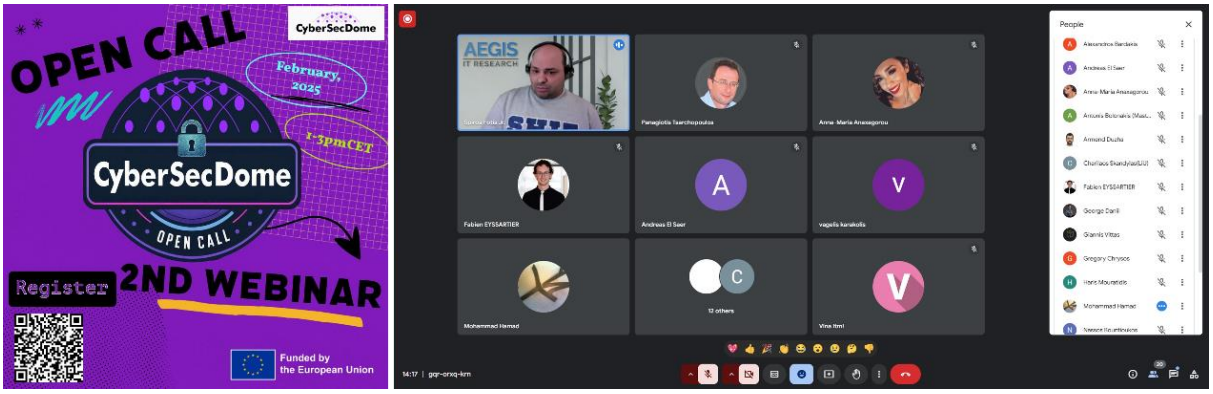


Figure 26: CyberSecDome 2nd Open Call Webinar

3.5.5 Open Call Flyer

A flyer was created to promote the CyberSecDome Open Call. This flyer was dedicated to the Open Call launch and the 2nd Info Day, serving as a key dissemination tool. It provided essential information about the call, including participation guidelines, deadlines and eligibility criteria. The flyer was distributed through various channels and events to ensure broad visibility and engagement.

Figure 27: CyberSecDome Open Call and 2nd Info Day Flyer

4 Monitoring and reporting

Monitoring and reporting dissemination and communication activities are key to the effective execution of WP6 - Dissemination, Exploitation and Sustainability and require the involvement of all partners. Each partner plays a role in carrying out their dissemination efforts, keeping ITML informed about their progress and tracking their dissemination activities. ITML regularly reviews and analyses the reported activities, integrating them into periodic project reports. This ongoing review helps improve the overall dissemination strategy. Additionally, to measure the impact of CyberSecDome's outreach efforts, we rely on specific key performance indicators (KPIs) set out in the Grant Agreement, which are detailed in Table 10. We track these KPIs using tools such as Google Analytics, Matomo, Hootsuite, LinkedIn and X.

Table 10. CyberSecDome KPIs metrics (M1-M18)

CDEB Objective 1 | 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.					
Channels	**KPI**	**Method of measurements**	**Frequency**	**Target**	**Results**
CyberSecDome website	>20 visitors (monthly)	Google Analytics	Monthly	20	**IN PROGRESS** ≈190/month (3074 in total)
	>1000 site access (annually)	Google Analytics	Annually	1000	**IN PROGRESS** 11k in total
	500 downloads	Google Analytics	End of the project	500	**IN PROGRESS** 1219 in total
Social Media (X)	10 push announcements (monthly)	Hootsuite	Monthly	10	**IN PROGRESS** ≈13/month (211 in total)
	5 new followers (monthly)	Hootsuite	Monthly	5	**IN PROGRESS** ≈5/month (80 in total)
	20 re-tweets (monthly)	Hootsuite	Monthly	20	**IN PROGRESS** ≈25/month (404 in total)
Social Media (LinkedIn)	10 push announcements (monthly)	Hootsuite	Monthly	30	**IN PROGRESS** ≈12/month (188 in total)
	5 new followers (monthly)	Hootsuite	Monthly	5	**IN PROGRESS** ≈37/month (596 in total)
	30 profile view (monthly)	LinkedIn	Monthly	30	**IN PROGRESS** ≈94/month (1510 in total)
Newsletter	>8 newsletters with technical activities (bi-monthly)	Mailchimp	End of the project	8	**IN PROGRESS** (4 in total)

Channels	KPI	Method of measurements	Frequency	Target	Results
Joint cluster synergies/ Established links	>3 similarly themed projects identified	Internal records/ Communication	End of project	3	**ACHIEVED** (5 in total)
	>1 jointly organised clustering workshop	Internal records/ Communication	End of project	1	**IN PROGRESS** (A workshop is planned to take place in May-June 2025)
Publications, Special issues, etc.	>3 publications in international refereed journals	Zenodo/Project website	End of project	3	**ACHEIVED** (7 in total)
	>1 journal special issues	Zenodo/Project website	End of project	1	**ACHEIVED** (1 in total)
	>3 publications in international magazines	Zenodo/Project website	End of project	3	**IN PROGRESS** (1 in Magazine)
	>6 conference presentations	Zenodo/Project website	End of project	6	**ACHIEVED** (7 published & 5 accepted)
CDEB Objective 2 | 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.					
Channels	**KPI**	**Method of measurements**	**Frequency**	**target**	**Results**
CyberSecDome supporting material /downloads	>1000 downloads of high-quality electronic brochures with the technical approach and activities	Zenodo records/statistics	End of project	1000	**IN PROGRESS** (319 in total)
	>100 new discussions per year on LinkedIn	LinkedIn Analytics/ Hootsuite	Annually	100	**IN PROGRESS**
	>500 downloads	Google Analytics	End of project	500	**ACHIEVED**

					(1219 in total)
	>500 views of 5-min videos on YouTube by the end of the project	YouTube	End of project	500	**IN PROGRESS** (522 views in total)
CyberSecDome Organisation of events (in-person)/material for engagement	>3 events (up to 25 participants) and >2 events (25-100 participants) organised by the end of the project; >40% of the participants in each event attracted and registered as contacts	Internal report/records	End of project	5	**IN PROGRESS** (1 event up to 25 participants & 2 events up to 25-100 participants; ***3 organised Open Call webinars**)
	>50 hard copies distributed in >5 events	Internal report/records	End of project	50	**IN PROGRESS** (in 8 events)
	Engagement of >2 policy making bodies	-	End of project	2	**IN PROGRESS**
CDEB Objective 3 | Work to deliver and monitor project impacts as related to the exploitation of outputs.					
Channels	**KPI**	**Method of measurements**	**Frequency**	**Thres**	**Results**
CyberSecDome Events (participation in events, brokerage, workshops, webinars, etc.)	Participation in >10 small and large-scale events	Internal records	End of project	10	**ACHIEVED** (16 until M18)
	>2 events organised (with 70 attendees)	Internal records	End of project	70	**ACHEIVED**
	>20% of participants engaged for further exploitation	Internal records	End of project	20%	**IN PROGRESS** (70% of the Open Call participants events expressed interest in submitting proposals)
CDEB Internal Reports & Communications	>15 internal mails with rich information on project progress and DE events & opportunities	Internal records	End of project	100%	**IN PROGRESS** (14 until M18)

	2 reports published with CDEB KPIs that are continuously updated	Internal reports	End of project	2	**IN PROGRESS** (1 until M18)
CDEB Objective 4 | Accelerate business growth through direct and indirect integration of the project's benefits					
Channels	**KPI**	**Method of measurements**	**Frequency**	**Thres**	**Results**
CyberSecDome Business growth	>1 internal training workshop (on the project-developed technologies and CyberSecDome tools)	Internal records	End of project	1	**ACHEIVED**
	≥1 partnership formed with a key business in the field (e.g., Cybersecurity)	Internal records	End of project	1	**ACHIEVED** (ECSCI Community)

5 Future Dissemination & Communication Activities

The consortium has made impressive progress in disseminating and communicating the project's objectives and achievements to relevant communities, and we are excited to continue building on this momentum with additional planning for the final year of the project. The following subsections outline the tasks and activities planned for the upcoming project year, with a particular emphasis on participation in conferences and expos, which remain a key focus. However, it is important to note that these plans may evolve as circumstances develop, ensuring the consortium remains flexible and responsive to emerging opportunities.

5.1 Future Planned dissemination activities

This section outlines a list of potential dissemination activities, including some that have already been confirmed, which the consortium members plan to consider for the upcoming year.

Table 11: Tentative list of future dissemination and communication activities

Future events (Exhibitions, fairs, Info Days, Webinars, Workshop/Seminars, Conferences, Brokerages, Networking events etc.)	Date	Location	Link Information
EU HSBooster Workshop: Insights & lessons learned in standardisation of incident response by PHOENI2X, CYBERSECDOME and SYNAPSE	20 March, 2025	Online	https://www.hsbooster.eu/
15th InfoCom Security 2025 Conference & Expo	2-3 April, 2025	Athens, Greece	https://www.infocomsecurity.gr/
3rd ECSCI Workshop on Futurizing Critical Infrastructure Resilience	29-30 April, 2025	TBD	https://www.finsec-project.eu/ecsci
DATE 2025	31-02 April, 2025	Lyon France	https://www.date-conference.com/
20th Symposium on Software Engineering for Adaptive and Self-Managing Systems (SEAMS)	28-30 April, 2025	Ottawa, Ontario, Canada	https://conf.researchr.org/home/seams-2025
5th CyberHOT hands-on CyberSecurity Summer School	29-30th May 2025	Chania, Crete, Greece	https://www.cyberhot.eu/
Clustering Webinar on Cybersecurity (already confirmed event)	TBD (May / June 2025)	Online	-
26th Infocom World 2025 Conference	TBD	Athens, Greece	https://infocomworld.gr/
7th FUTURE IOT SCHOOL	TBD	Paris, France	https://school.future-iot.org/
EFECS 2025	TBD	TBD	https://efecs.eu/

5.2 Future communication activities

As the project reaches its 19th month, marking the halfway point of its 36-month duration, WP6 will continue to plan and implement various communication activities for the upcoming project year.

5.2.1 Future Dissemination and Communication Material

In the next project period (up to Month 24), the consortium plans to release two additional newsletter issues (for a total of four by the end of the project), two dedicated newsletters or press releases focused on the Open Call, a podcast series featuring consortium partners and, if necessary due to the submission rounds and project implementation, a collection of Open Call videos.

- Newsletter #5 (March-April 2025)
- 1st Podcast series with Coordinator, MAG (March-April 2025)
- Open Call Newsletter – Press Release (May 2025)
- Newsletter #6 (August-September 2025)
- 2nd Podcast series with Technical Coordinator, TUM (May 2025)
- 3rd Podcast series with #1 Pilot partner, AIA (July 2025)
- 4th Podcast series with #2 Pilot partner, OTE (September 2025)
- 5th Podcast series with Integration leader, AIRBUS (November 2025)
- Open Call Newsletter – Press Release/Announcement (September – October 2025)

5.2.2 CyberSecDome Website

The website will be consistently updated with the following content:

- Updates on the project's progress, workshops, meetings, conference participation and other related events.
- Reports, publications, papers and promotional materials.
- New dissemination efforts and collaborations with similar projects.
- Open Call dedicated section with all necessary information for the participants.

To ensure effective monitoring of our KPI metrics, website analytics will be regularly reviewed to track and assess the website's visibility throughout the project's duration.

5.2.3 CyberSecDome Social Media

The project’s social media profiles will be regularly updated with:

- Project branding materials (e.g., new newsletter issues, podcasts, videos, etc.)
- News and developments related to the project
- Deliverables and new publications
- Insightful quotes from partners about the project
- Relevant articles from the web related to the project’s topic
- Updates and developments from similar projects

5.2.4 Collaboration with other similar projects

The CyberSecDome project will continue to expand its efforts in engaging with similar initiatives and collaborating with other EU-funded projects. The project will ensure the regular updating of its established cross-dissemination synergies. As part of its active involvement in the ECSCI cluster, CyberSecDome contributes to a strengthened collaborative network, offering its innovative Virtual Reality-based approach to improving cybersecurity resilience. Research within this cluster focuses on safeguarding critical infrastructures and services, exploring diverse solutions from various projects and fostering strong connections with complementary EU-funded initiatives.

Through its participation in the ECSCI cluster, CyberSecDome will engage in relevant events and contribute to the activities organised within this network. We aim to continue developing synergies with the projects outlined in Section 2.4, including possible joint publications, shared conference booths and broader participation in international events. Additionally, we are committed to supporting opportunities for collaborative scientific papers and contributing to standardisation efforts within the cluster.

6 Conclusion

This deliverable presents the interim version of the CyberSecDome dissemination and communication strategy, alongside the activities undertaken during the first 18 months of the project. The primary objective of these efforts is to align the dissemination of CyberSecDome information with the needs of various stakeholders, utilising a range of communication channels. These activities include developing and distributing the project's visual identity, such as Branded Dissemination and Communication material, newsletters, videos, podcasts and other promotional content.

In addition, the consortium has been actively involved in various outreach initiatives, including workshops, conferences and information sessions. These initiatives aim to encourage greater participation from stakeholders in the project's core activities, particularly in the CyberSecDome Open Call. The Open Call seeks to engage third parties from diverse sectors and regions to accelerate the integration of advanced security solutions into digital systems and infrastructures, ultimately enhancing trust, security and resilience within the digital ecosystem.

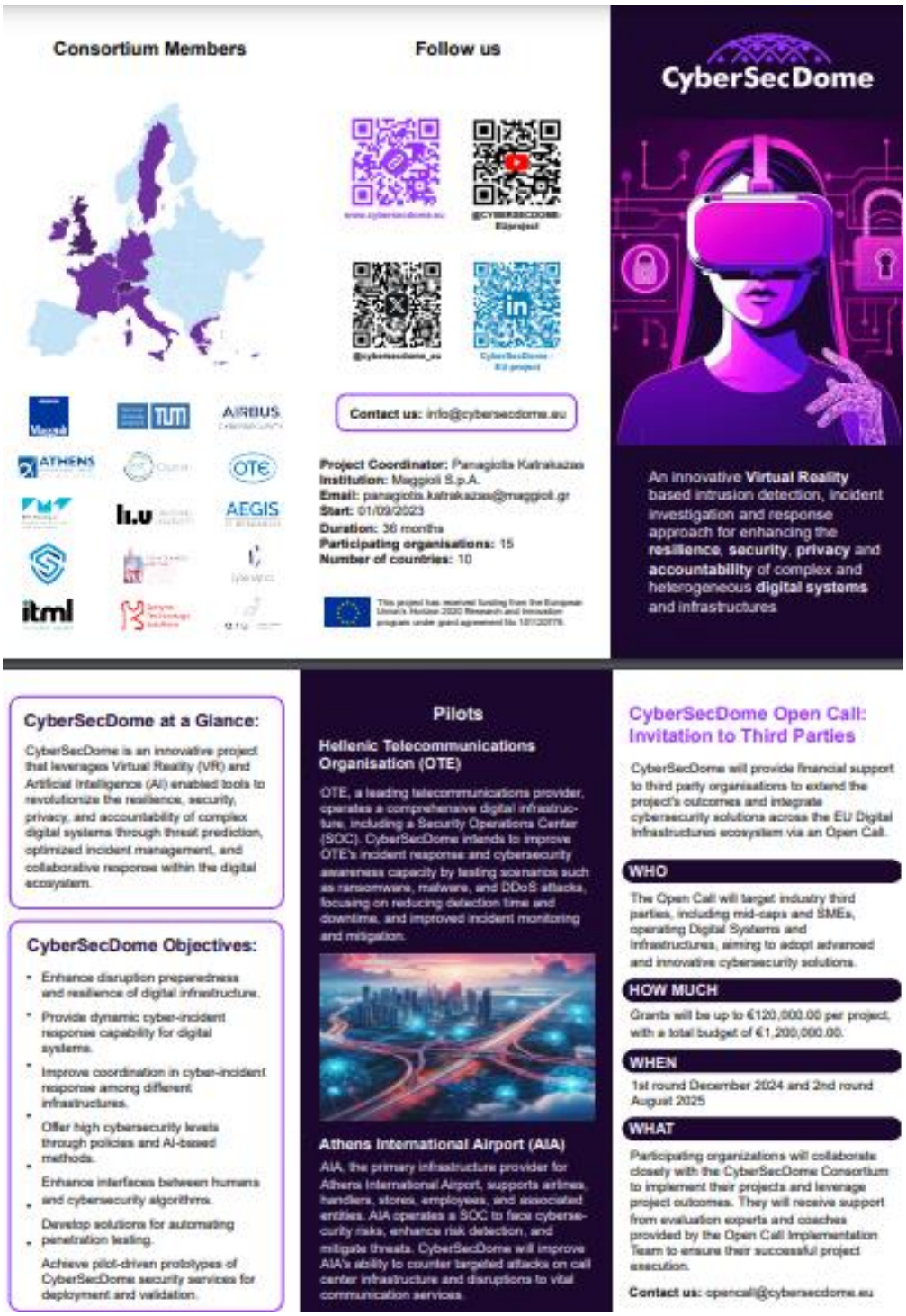
Over the course of the project's first half, the consortium has focused on increasing CyberSecDome's visibility, ensuring that information about the project's objectives, progress and outcomes is widely disseminated. This has been achieved through the creation and distribution of various communication materials, including newsletters, posters and videos, across the project's digital platforms. Additionally, partners have participated in numerous events—both online and in person—engaging with the scientific community, industry professionals and other relevant EU initiatives.

As the project enters its second phase, the CyberSecDome consortium will work to further enhance its physical presence, with a focus on more tangible technical results and outcomes. Communication efforts will be intensified, particularly through the production of scientific publications and technical reports. Moreover, the consortium will continue to strengthen collaborations with other EU-funded projects and relevant initiatives to maximise the impact and visibility of CyberSecDome's outcomes. Moreover, consortium partners, particularly the dedicated teams, will continue to provide ongoing support to all Open Call candidates, offering relevant materials to help them better understand the eligibility criteria, submission process and general updates. This will include press releases on social media, dedicated newsletters and informative videos.

Appendices

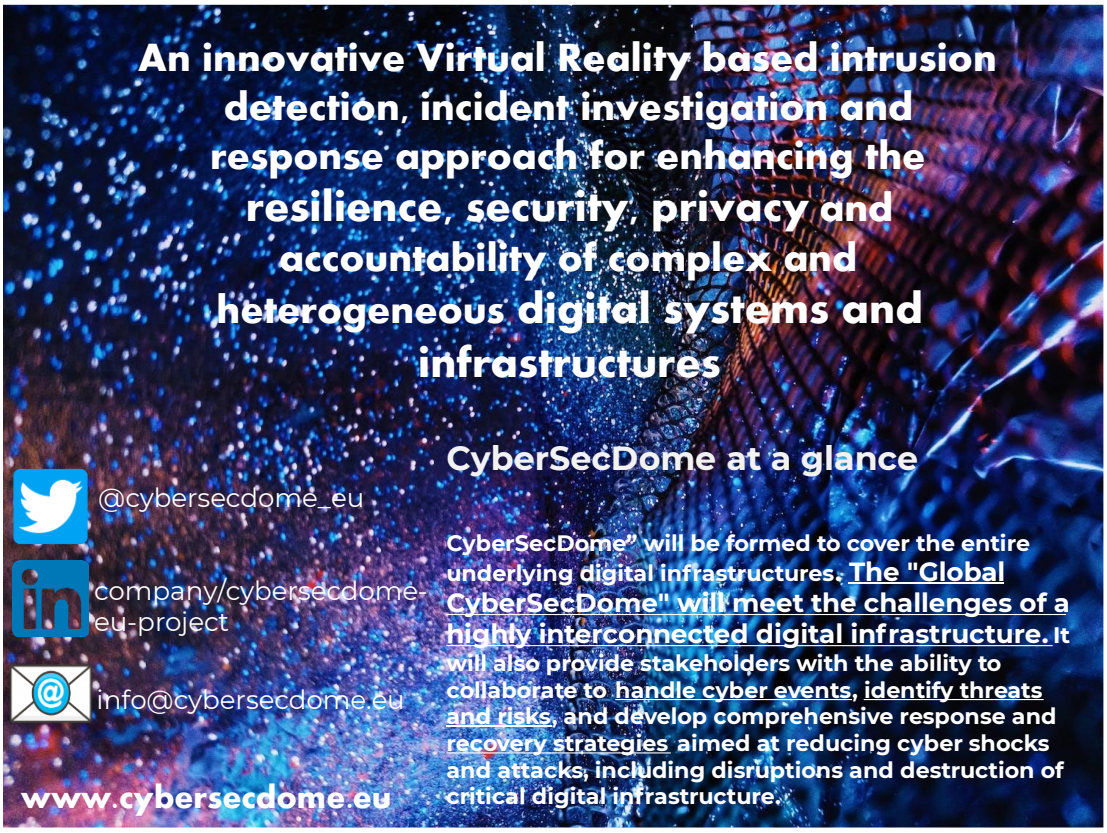
APPENDIX I - Branding material, logos, newsletters

CyberSecDome Brochure (screenshot)



CyberSecDome Poster - Version 2

CyberSecDome



CyberSecDome Consortium Members

GRUPPO Maggioli · Technical University of Munich · AIRBUS CYBERSECURITY · ATHENS INTERNATIONAL AIRPORT ELEFTHERIOS VENIZELOS · eit Digital · IMT Atlantique Bretagne-Pays de la Loire École Mines-Télécom · OTE GROUP OF COMPANIES · Security Labs Consulting · LINKÖPING UNIVERSITY · AEGIS IT RESEARCH · ΠΟΛΥΤΕΧΝΕΙΟ ΚΡΗΤΗΣ TECHNICAL UNIVERSITY OF CRETE · Cyberalytics Secure analytics for the interconnected world · itml innovation applied · Sphynx Technology Solutions · a.r.u. Anglia Ruskin University

Project Leader
Mr. Panagiotis Katrakazas
Maggioli S.p.A.
panagiotis.katrakazas@maggioli.gr

This project has received funding from the Horizon Europe Framework Programme (20212027) under the grant agreement No 101120779.

CyberSecDome Roll up banner – Version 2

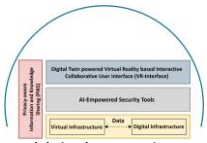
CyberSecDome

CyberSecDome at a glance

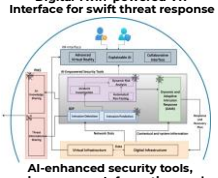
The "**CyberSecDome**" is a comprehensive solution that covers the entire digital infrastructure, addressing the challenges of a highly interconnected digital environment.

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

Project Leader

Mr. Panagiotis Katrakazas
Maggioli S.p.A.
panagiotis.katrakazas@maggioli.gr

Contact us
info@cybersecdome.eu

Consortium Members

This project has received funding from the Horizon Europe Framework Programme (2021 - 2027) under the grant agreement **No 101120779**.

CyberSecDome YouTube Thumbnail (for Open Call material)

CyberSecDome Open Call Logo (for dissemination purposes)

CyberSecDome Open Call invitations (for dissemination purposes)

CyberSecDome 4th Newsletter Edition (December 2024)