CyberSecDome

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

GRUPPO Maggioli

Technical University of Munich TUM

AIRBUS CYBERSECURITY

ATHENS INTERNATIONAL AIRPORT ELEFTHERIOS VENIZELOS

eit Digital

OTE GROUP OF COMPANIES

IMT Atlantique Bretagne-Pays de la Loire École Mines-Télécom

LiU LINKÖPING UNIVERSITY

AEGIS IT RESEARCH

Security Labs Consulting

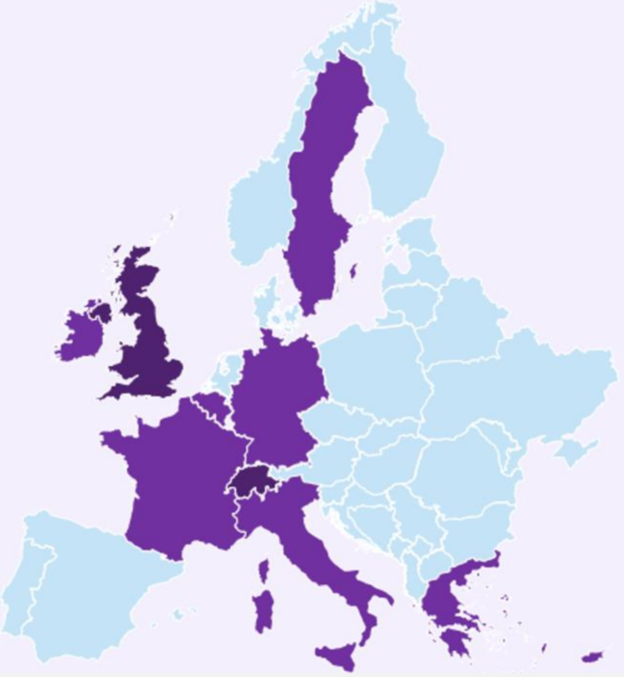
ΠΟΛΥΤΕΧΝΕΙΟ ΚΡΗΤΗΣ TECHNICAL UNIVERSITY OF CRETE

Cyberalytics Secure analytics for the interconnected world

itml innovation applied

Sphynx

a.r.u. Anglia Ruskin University



NEWSLETTER NO 5

Jan (M17) – May (M21)

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 collaboration among 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 the development of effective incident response strategies to ensure 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 levels of cybersecurity through policies and AI-based methods for proactive and real-time management of all 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.

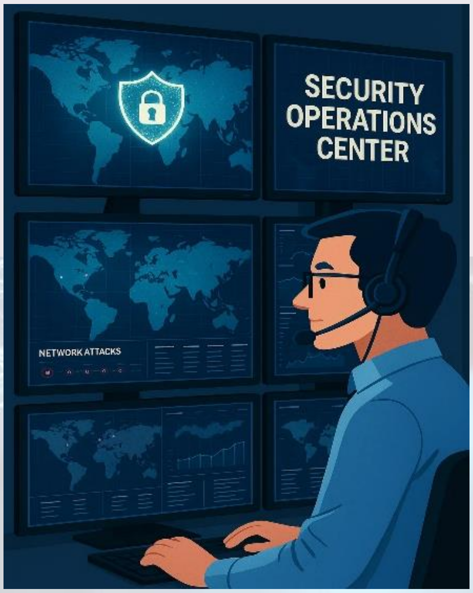
CyberSecDome's Pilots

Hellenic Telecommunications Organisation

OTE, a leading telecommunications provider, operates a comprehensive digital infrastructure, including a Security Operations Center (SOC). CyberSecDome intends to improve OTE's incident response and cybersecurity awareness capacity by testing scenarios such as ransomware, malware, and DDoS attacks, focusing on reducing detection time and downtime, and improving incident monitoring and mitigation.

Athens International Airport

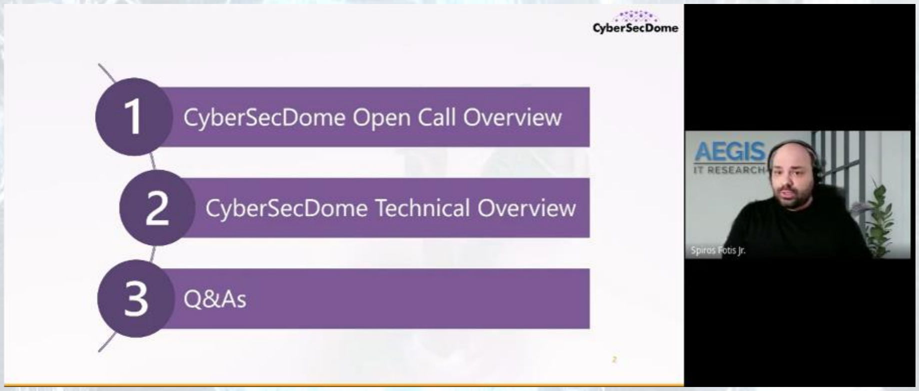
AIA, the primary infrastructure provider for Athens International Airport, supports airlines, handlers, stores, employees, and associated entities. AIA operates a Security Operations Center (SOC) to face cybersecurity risks, enhance risk detection, and mitigate threats. CyberSecDome will improve AIA's ability to counter targeted attacks on call center infrastructure and disruptions vital communication services.



MEETINGS & EVENTS

CyberSecDome 1st Open Call Webinar event, January 2025

On January 15, 2025, the first Open Call Webinar took place online, attracting approximately 50 registrants. The agenda included an in-depth exploration of the proposal structure, evaluation criteria, and scoring methodology, providing valuable insights for applicants. Participants were also presented with examples of best practices to help them prepare strong applications. Additionally, the webinar featured a live Q&A session with technical partners and members of the OCMT, allowing attendees to ask their questions directly. The session's outcome aimed to assist applicants in aligning their proposals with evaluation expectations. Following the event, the recording and slides were made available on the CyberSecDome website and shared across various social media channels.


CyberSecDome

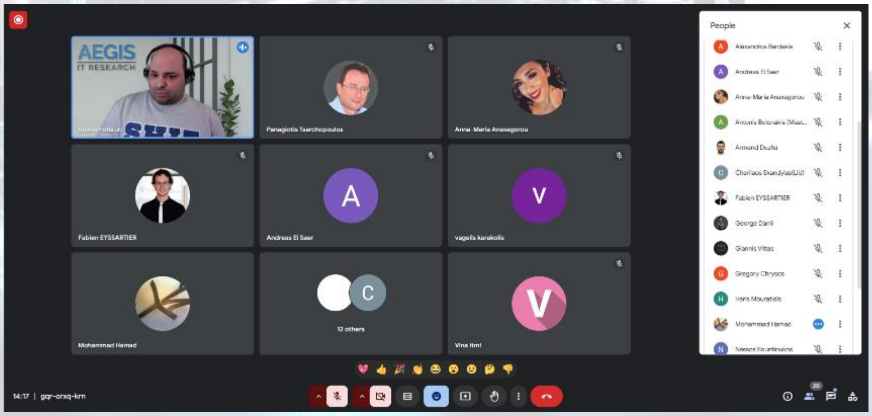
1 CyberSecDome Open Call Overview

2 CyberSecDome Technical Overview

3 Q&As

CyberSecDome 2nd Open Call Webinar (Q&A), February 2025

On February 12, 2025, a second online webinar dedicated to the first round of the open call was held to provide final guidance before the upcoming submission deadline on February 19, 2025. The session aimed to address technical, administrative, and strategic questions from applicants, specifically targeting small and medium-sized enterprises (SMEs), research organisations, and security solution providers. The outcome of this webinar was significant, as it helped clarify last-minute doubts and successfully supported a final wave of applications, including a peak of 27 proposals submitted on February 17 alone.



CyberSecDome at DATAMITE Meet Up in Athens, February 2025

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.

CyberSecDome Mid-term Review Meeting, April 2025

CyberSecDome held its Mid-term Review meeting online, marking an important milestone in the project's progress. During the meeting, CyberSecDome's progress was showcased, highlighting key achievements and ongoing developments as the project made significant advancements in delivering innovative cybersecurity solutions. Grateful to all partners for their dedication and hard work, as well as to the EU representatives for their valuable feedback and support. This constructive review motivates us to continue driving impactful cybersecurity innovation across Europe.

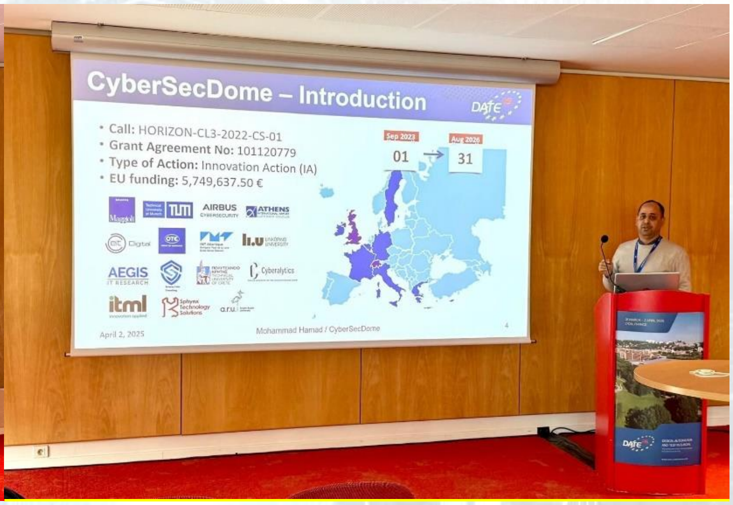
CyberSecDome at DATE2025 in Lyon, France, April 2025

CyberSecDome was proudly presented at the DATE 2025 Conference, showcasing the project's innovative efforts to enhance cybersecurity for digital infrastructures across Europe. Mohammad Hamad from the Technical University of Munich represented the consortium, sharing insights into the project's vision, progress, and its contribution to securing critical digital environments.

DESIGN, AUTOMATION AND TEST IN EUROPE
THE EUROPEAN EVENT FOR ELECTRONIC SYSTEM DESIGN & TEST
31 MARCH - 2 APRIL 2025
LYON, FRANCE
CENTRE DE CONGRÈS DE LYON

Multi-Partner Project: CyberSecDome – Framework for Secure, Collaborative, and Privacy-Aware Incident Handling for Digital Infrastructure

Mohammad Hamad, Michael Kühr, Haralambos Mouratidis, Eleni-Maria Kalogeraki, Christos Gizelis, Dimitris Papanikas, Athanasios Bountioukos-Spinaris, Charilaos Skandylas, Evangelos Raptis, Andreas Alexopoulos, Grigorios Chrysos, Mina Marmpena, Sevasti Politi, Konstantinos Lieros, Papagiannopoulos Nikolaos, Iordanis Xanthopoulos, Spyros Papastergiou, Sotiris Ioannidis, Mikael Asplund, Marc-Oliver Pahl, Sebastian Steinhorst



CyberSecDome – Introduction

- Call: HORIZON-CL3-2022-CS-01
- Grant Agreement No: 101120779
- Type of Action: Innovation Action (IA)
- EU funding: 5,749,637.50 €

April 2, 2025
Mohammad Hamad / CyberSecDome
4

CyberSecDome at SEAMS 2025 in Ottawa, Canada, April 2025

The SEAMS 2025 Conference, held in April 2025 in Ottawa, Canada included a presentation that acknowledged the CyberSecDome project. The paper titled "Analysis of Autonomous Driving Software to Low-Level Sensor Cyber Attacks" was presented by Andrew Roberts, Mohsen Malayjerdi, Mauro Bellone, Raivo Sell, Olaf Maennel, Mohammad Hamad, and Sebastian Steinhorst.

SEAMS 2025
OTTAWA, CANADA
The 20th International Conference on Software Engineering for Adaptive and Self-Managing Systems

CyberSecDome Open Call Round 1 – Catalysing EU Cybersecurity Innovation

CyberSecDome's Open Call Round 1 has been a cornerstone in the project's strategy to boost cybersecurity innovation and adoption through external collaboration. Officially launched in December 2024, the Open Call aimed to attract third-party innovators, especially SMEs and research teams, offering them a unique opportunity to integrate and test their cybersecurity solutions within the CyberSecDome platform. As the leader of the Open Call Management Team, AEGIS played a central role in designing and coordinating the full lifecycle of the call, from structuring its architecture and evaluation framework to managing applicant support, evaluator coordination, and reporting. The Open Call was executed in close collaboration with MAG (Project Coordinator), EIT Digital (Financial Support to Third Parties Manager), and with valuable contributions from TUM (Technical Coordinator) and ITML (Dissemination and Communication Leader).

Strong Dissemination & Industry Engagement

Thanks to an active and well-coordinated dissemination campaign led by ITML and supported by AEGIS, the Open Call Round 1 achieved significant reach and visibility:

- Two dedicated Info Days were organised in Brussels (June 2024) and Athens (December 2024), attracting cybersecurity stakeholders from across Europe.
- Promotional activities spanned EU networks, national clusters, LinkedIn, and targeted mailing lists.
- The F6S platform facilitated proposal submissions and outreach, resulting in over 100 applications from more than 20 countries worldwide.

This strong response demonstrated the Open Call's resonance with the European cybersecurity ecosystem and the broad interest in testing solutions against real-world use cases.

Topics & Evaluation Process

The call invited proposals across five key topics:

1. Penetration Testing & Vulnerability Detection
2. Visual Analytics & Cyber Threat Intelligence
3. Incident Investigation & Evidence Handling
4. AI for Secure IoT/OT Environments
5. Immersive Cybersecurity Training

The Technical University of Munich (TUM) defined the technical scope, led webinars for applicants and evaluators, and ensured alignment with the project's architecture. The evaluation process followed a double-blind expert review model, supported by Heads of Topics (HoTs), with oversight from the Open Call Management Team (OCMT). Evaluation criteria included excellence, impact, implementation feasibility, alignment, and value for money.

Results & Next Steps

Following a competitive evaluation process, a list of top-ranked and eligible proposals was approved for funding. With all Sub-Grant Agreements now signed, the implementation phase of the funded projects has officially begun, marking a key milestone in the CyberSecDome Open Call. To support this process, the Open Call Implementation Team (OCIT) has been fully mobilised, providing technical guidance, continuous monitoring, and tailored mentoring to each funded project. A designated OCIT contact point has been assigned to each project to ensure smooth coordination and effective communication throughout the implementation period.

As part of the onboarding process, an online Kick-Off Meeting was successfully held in early June 2025. The meeting brought together representatives from the selected projects and the CyberSecDome consortium, offering an opportunity to align objectives, clarify roles and responsibilities, and officially launch the collaborative effort. Below is the list of the funded projects along with their respective coordinators:

#	Acronym	Lead
1	CASeR-Safe	Smartotum srl
2	DomeSentinel	Focal Point sprl
3	ACRYS	CYBERFLIP S.A. WOLI SERVICES LTD
4	ATTENTO	Buontech Solutions srl
5	SCAF-DOME	ATC
6	ELEVATE	PRAGMA -IOT AE, Greece
7	ADAPT	CYBERFLIP S.A. WOLI SERVICES LTD
8	CATT-46	i46 s.r.o
9	SHIELD	i46 s.r.o

Round 2 Now Open for Applications!

The CyberSecDome Open Call Round 2 is now officially open. This round focuses on testing and validating the fully integrated CyberSecDome platform in real-world environments. Building on Round 1, which focused on aviation and telecom, Round 2 aims to broaden its impact across underrepresented sectors, including healthcare, finance, energy, industrial IoT, public services, smart cities, and more.

CyberSecDome's Open Call mechanism reflects the project's broader commitment to open innovation, stakeholder empowerment, and practical cybersecurity advancements. Through this initiative, the project is helping to shape a stronger, more resilient European cybersecurity landscape—fueled by collaboration, excellence, and impact. Applicants can learn more about the call scope, requirements, and submission process on the CyberSecDome website (Open Call Round 2 - CyberSecDome).

DISSEMINATION MATERIAL

As we celebrate the completion of the first half of the project, the consortium has created a comprehensive set of materials, including brochures, roll-up banners, and posters, to promote the project and its vision. The latest brochures for the CyberSecDome project have just been released! All dissemination material are fully accessible through the CyberSecDome website and the project's Zenodo community.

Under our dissemination efforts, we created a podcast featuring a brief discussion about the CyberSecDome project, where the presenters offer an overview of the project while also sharing critical information regarding our Open Call status and the main points from each round. The podcast can be found on our YouTube channel.

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. **CyberSecDome's** scientific papers are fully accessible through the CyberSecDome website and the project's Zenodo community.

DELIVERABLES SUBMISSION

By the M20 of the project (April 2025), the CyberSecDome consortium have successfully submitted the below deliverables:

- ✓ D1.1 Project Management, Risk Identification, and Quality Assurance Handbook (Lead: MAG); M3.
- ✓ D1.2 Privacy Protection and Data Management Plan (Lead: AEGIS); M6.
- ✓ D6.1 Dissemination and Communication Strategy (Lead: ITML); Public; M6.
- ✓ D2.1 State of the art, Reference Pilot Scenarios, Requirements, and Analysis (Lead: AIA); M8.
- ✓ D2.2 Architecture and Technical Specification of CyberSecDome (Lead: TUM); M8.
- ✓ D1.3 Annual Management Report (Lead: MAG); M12.
- ✓ D5.2 Open call methodology and procedures (Lead: EIT); M12.
- ✓ D3.1 Specifications of the AI-empowered Security Tools (Lead: AEGIS); M13.
- ✓ D4.1 Specification of the collaborative interfaces and information sharing (Lead: IMT); M13.
- ✓ D3.2 Implementation of AI-empowered security tools (Lead: ACS); M18.
- ✓ D4.2 Implementation of collaborative interfaces and information sharing (Lead: IMT); M18.
- ✓ D4.3 First Integrated CyberSecDome (Lead: ACS); M18.
- ✓ D5.1 Implementation Strategy and Evaluation plan and Benchmarks (Lead: OTE); M18.
- ✓ D6.2 Intermediary Report on Dissemination and Communication Activities (Lead: ITML); M18.
- ✓ D6.4 Intermediary Report on Contribution to Certification Standardisation (Lead: TUC); M18.
- ✓ D6.6 Intermediary Exploitation, Sustainability, and Business Plans (Lead: MAG); M18.
- ✓ D5.3 Open call documentation, reports and analytics (Lead: AEGIS); M20.

Key Facts

Project Coordinator: Dr. Armend Duzha
Institution: Maggioli S.p.A.
Email: armend.duzha@maggioli.it
Start: 01-09-2023
Duration: 36 months
Participating organisations: 15
Number of countries: 10

Follow us

https://cybersecdome.eu/

@CyberSecDome - EU project

@cybersecdome_eu

@CYBERSECDOME-EUproject

Fundings

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

European Commission | HORIZON EUROPE 2021-2027