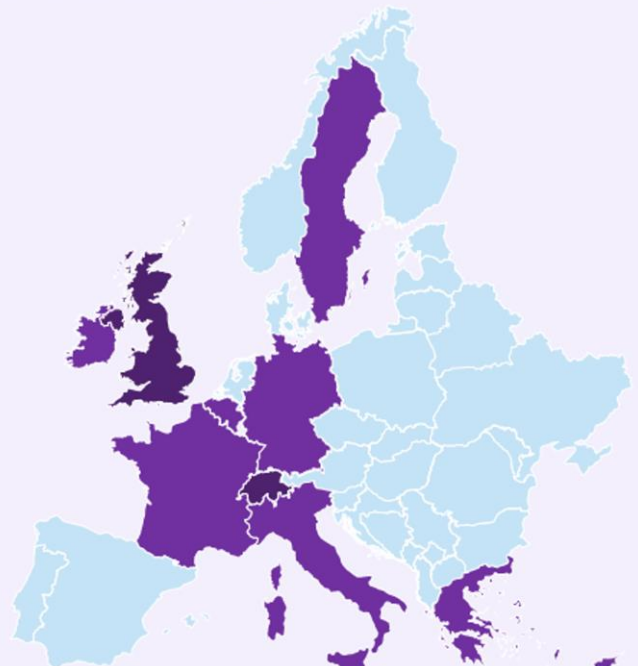


# CyberSecDome



*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



# NEWSLETTER NO 4

## Sep (M13) – Dec (M16)

### 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 to vital communication services.



# MEETINGS & EVENTS

## CyberSecDome 4th Plenary Meeting, September 2024

The CyberSecDome consortium gathered for its 4th plenary meeting on September 26-27, 2024, in Paris, France, hosted by IMT. The meeting was held in a hybrid format, allowing remote participation for partners unable to attend in person. The partners came together to review the project's progress across all work packages since M12 and held extensive technical workshops to address action points related to technical developments and upcoming deliverables. Additionally, they focused on defining the technical specifications for the upcoming [CyberSecDome Open Call](#), which will launch in December.

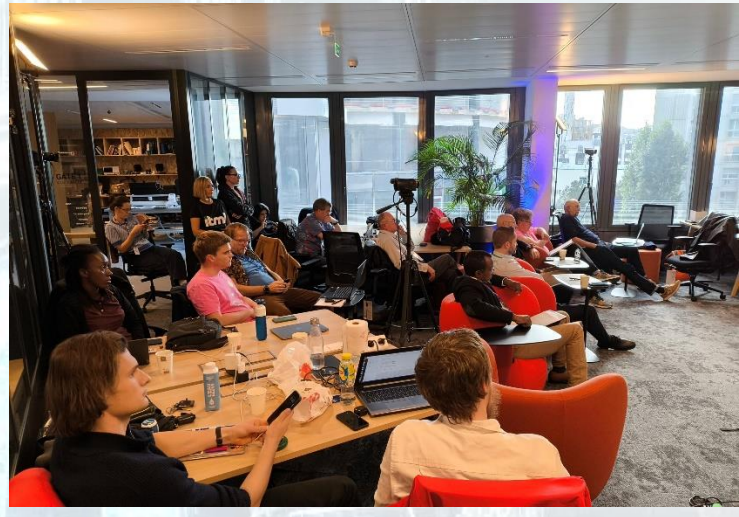


## CyberSecDome in the 6th Future IoT PhD School in Paris, October 2024

The 6th edition of the Future IoT PhD School took place at Campus Cyber in Paris from September 30 to October 4, 2024, fostering innovation in IoT since its launch in 2018. Organized by CyberSecDome partners, Marc-Oliver Pahl from [IMT Atlantique](#) and Nicolas Montavont from [Technical University of Munich \(TUM\)](#), the event brought together PhD students and researchers to explore advancements in IoT. CyberSecDome featured a keynote from our Technical Coordinator, showcasing AI-based security tools, while IMT Atlantique and [ITML](#) engaged



participants in a Hackathon, focusing on innovative technologies like Federated Learning. A thank you to all partners for their invaluable support in making this event a success!



### CyberSecDome participation in the European Big Data Value Forum (EBDVF), October 2024



The [European Big Data Value Forum \(EBDVF\)](#) is BDVA's flagship event that unites the European data-driven AI community to share knowledge and celebrate achievements. Held from October 2-4, 2024, in Budapest, Hungary, CyberSecDome was proudly showcased at our partner [OTE](#)'s booth, featuring our avatar and project video. Attendees learned how CyberSecDome is shaping the future of cybersecurity with innovative solutions. We extend our gratitude to OTE Group for representing us and delivering a talk on AI in Telecoms: The Data Challenge, spotlighting key tech trends.

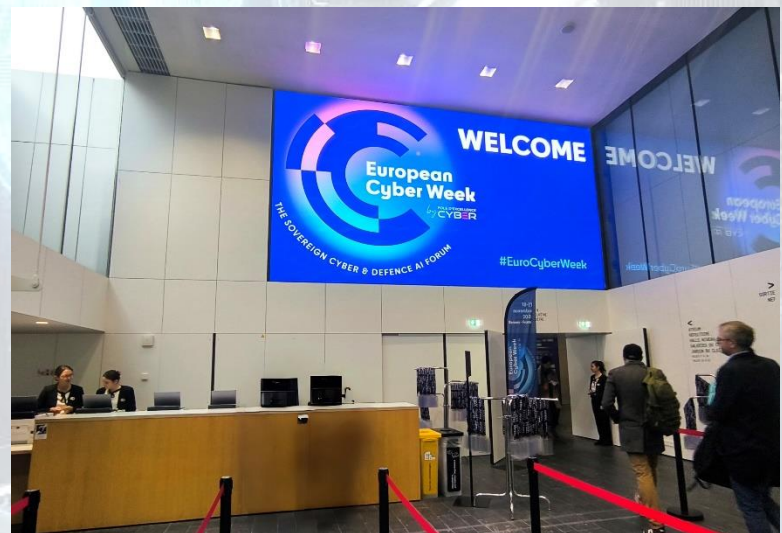
### CyberSecDome at the 26th InfoCom World Conference, November 2024

At the [26th InfoCom World Conference](#), the [OTE Group of Companies \(HTO\)](#) booth featured the CyberSecDome roll-up banner, showcasing the project's innovative cybersecurity solutions. It was a great opportunity to highlight our ongoing collaboration with OTE and engage with attendees about the progress and impact of CyberSecDome in strengthening digital security across Europe.



## CyberSecDome at the European Cyber Week in Rennes, November 2024

The CyberSecDome participated in the European Cyber Week 2024 in Rennes from November 18-20, showcasing our latest advancements in cybersecurity at Booth 103. Attendees engaged with our team to learn about our mission to enhance digital security in Europe and discover collaboration opportunities.



## CyberSecDome 3-Day Technical Meeting, December 2024

The technical meeting on December 4, 2024, kickstarted the CyberSecDome 2nd Info Day & Open Call Launch Event, focusing on initial discussions among partners. The following day, partners reviewed the integration progress of CyberSecDome's components and addressed key technical challenges. On December 6, the final day included sessions on preparing pilot implementations, discussing attack statuses, data availability, and integration with CyberRange.



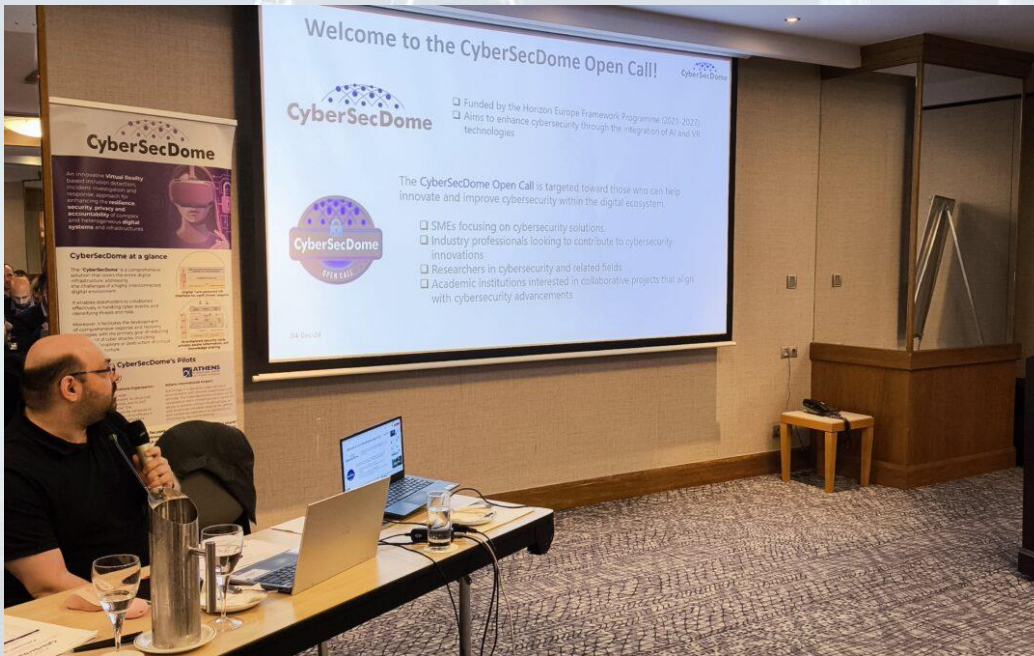
The event concluded with a tour of a pilot site at Athens International Airport, providing insights into CyberSecDome's innovative solutions. We thank all partners for their contributions, which are vital to enhancing digital infrastructure security. Stay tuned for more updates!

## CyberSecDome 2nd Info Day & Open Call Launch Event

We are excited to announce the successful CyberSecDome 2nd Info Day & Open Call launch event, held on December 4, 2024, in Athens, Greece, hosted by ITML.

The Info Day showcased the project's objectives and innovation capabilities, providing insights into various attack scenarios and officially launching the Open Call. This initiative aims to involve cross-sector and cross-border participants to enhance














cybersecurity solutions in digital systems, offering funding of up to €120K per successful proposal for SMEs, startups, and industry stakeholders. We thank all attendees, both in person and online. Event materials, including presentation slides and FAQs about the Open Call, are available on our [website](#). Stay tuned for upcoming webinars and key Open Call dates!



zenodo

All the necessary material uploaded here!

### Templates and Guidelines for Applicants

-  CyberSecDome Open Call Proposal Evaluation Summary Report.pdf
  -  CyberSecDome Open Call Proposal Template Round 1 – [Year].pdf
  -  CyberSecDome Round 1 General Guide.pdf
  -  CyberSecDome Third-Party Funding Agreement (TPFA).pdf
  -  CyberSecDome Open Call General Guide.pdf
  -  CyberSecDome Proposals Submission Guideline.pdf
  -  CyberSecDome Conflict of Interest Declaration Form.pdf
  -  CyberSecDome Open Call FAQs.pdf
- 



Check out the event recording [here](#).





# CyberSecDome Open Call is Now Open!



**The CyberSecDome Open Call aims** to engage cross-sector and cross-border third parties to accelerate the integration of advanced security solutions into digital systems and infrastructures. Through this initiative, we seek to enhance trust, security, and resilience across ICT products, services, and processes within the digital ecosystem.

## To Whom is it Directed

- ❖ Micro, small, and medium-sized enterprises (SMEs): Companies in the IT, ICT, and digital infrastructure sectors seeking to enhance their operations with innovative cybersecurity solutions, including AI and VR technologies.
- ❖ Research institutions and academics: Universities, research centers, and academic professionals specializing in IT, ICT, or cybersecurity research and innovation.
- ❖ Public and private sector entities.
- ❖ Industry professionals and large enterprises: Big companies and industry leaders looking to contribute to or adopt advanced cybersecurity innovations to protect and optimize their digital ecosystems.



## Successful applicants will receive:

- Financial support up to €120,000 per project.
- Access to mentoring and technical support.
- Networking opportunities with industry experts.

## Timeline:

- ✓ Call Opening Date: December 4, 2024
- ✓ Submission System Opens: December 10, 2024
- ✓ Proposal Submission Deadline: February 10, 2025
- ✓ Eligibility and Evaluation Deadline: March 10, 2025
- ✓ Announcement of Selected Projects: March, 2025
- ✓ Grant Agreement Signing: March, 2025
- ✓ Project Start: April, 2025

## DISSEMINATION MATERIAL

As we celebrate the completion of the first year 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 Zenodo community of the project.](#)

# PUBLICATIONS - JOURNALS

The CyberSecDome project had an active performance via journal and conference paper publication by presenting the research work carried out in the frame of the project. **CyberSecDome's** scientific papers are fully accessible through the [CyberSecDome website](#) and the [Zenodo](#) community of the project.

**AS WE ENTER THE NEW YEAR,  
WE WANT TO EXPRESS OUR  
GRATITUDE FOR YOUR  
CONTINUED SUPPORT. WISHING  
YOU A PROSPEROUS AND  
JOYFUL 2025!**



**CyberSecDome**



Funded by  
the European Union

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



## Key Facts

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



<https://cybersecdome.eu/>



[@CyberSecDome - EU project](#)



[@cybersecdome\\_eu](#)



[@CYBERSECDDOME-EUproject](#)

## Follow us

## Funding

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