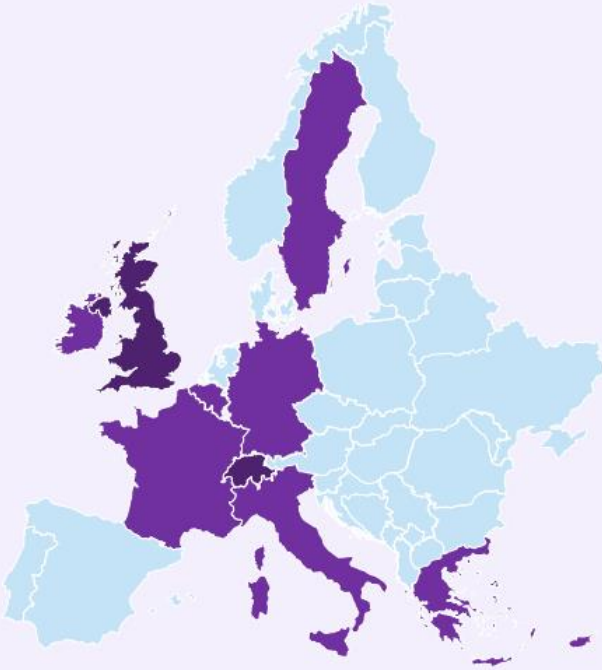
CyberSecDome

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 1

JAN 2024

At a GLANCE

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

CONCEPT

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

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

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

OBJECTIVES

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

CyberSecDome's Pilots

Hellenic Telecommunications Organisation

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.

MEETINGS & EVENTS

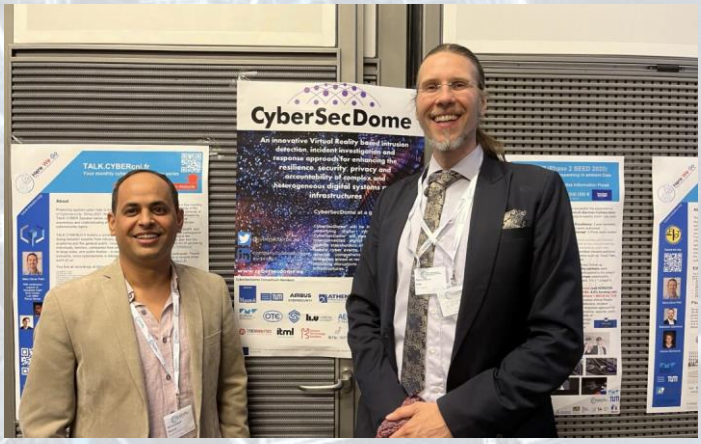
The #CyberSecDome project started its journey in September 2023! The 1st online kick-off meeting was held on the 18th of September, with the partners meeting online and looking forward to a fruitful 3-year collaboration!

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

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

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

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



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

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

DISSEMINATION MATERIAL

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

PUBLICATIONS - JOURNALS

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

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

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

Key Facts

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

Follow us

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

Funding

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

EUROPEAN UNION