

# CyberSecDome

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

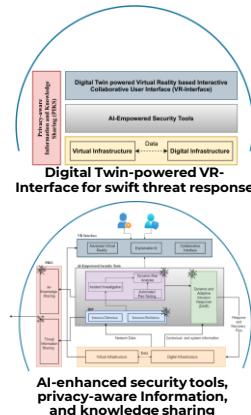


## **CyberSecDome at a glance**

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

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

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



## 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:

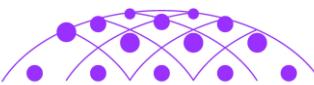
AIA brings in a dynamic cyber-physical environment, with diverse stakeholders and services. The CyberSeC-Dome solution will be validated on AIA's infrastructure in terms of its ability to protect critical infrastructures, as well as provide valuable insights for refining and validating cybersecurity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



Co-funded by the  
European Union

The work was supported by the CyberSecDome project (GA No 101120779), funded by the European Union under the Horizon Europe (HORIZON) Framework Programme for research and innovation.

“Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the European Commission can be held responsible for them.”



# CyberSecDome

## Consortium Members



Technical University of Munich



**AIRBUS**  
CYBERSECURITY

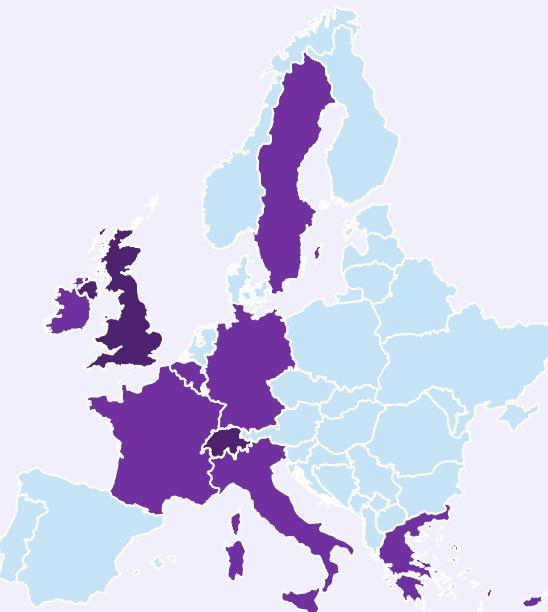


LINKÖPING  
UNIVERSITY

**AEGIS**  
IT RESEARCH



Cyberalytics



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](http://www.cybersecdome.eu)



[@cybersecdome\\_eu](http://@cybersecdome_eu)



[CyberSecDome - EU project](http://CyberSecDome - EU project)



[CYBERSEC DOME-EU project](http://CYBERSEC DOME-EU project)

**Contact us:** [info@cybersecdome.eu](mailto:info@cybersecdome.eu)



Co-funded by the  
European Union

The work was supported by the CyberSecDome project (GA No 101120779), funded by the European Union under the Horizon Europe (HORIZON) Framework Programme for research and innovation.

"Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the European Commission can be held responsible for them."