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 7

November (M27) – February (M30)

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 capabilities. 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.

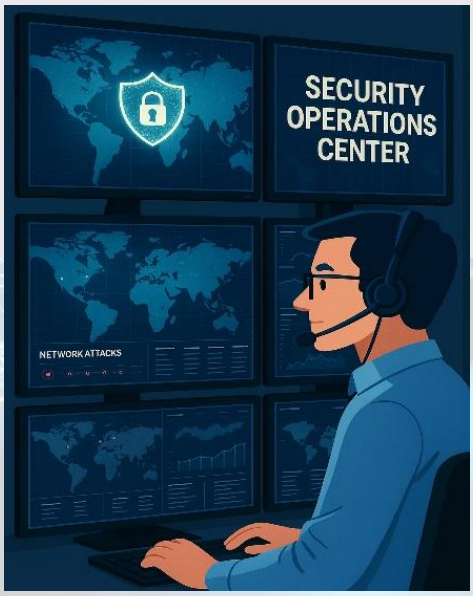
CyberSecDome's Pilots

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 at COcyber's first Concertation Workshop in Brussels, November 2025

On 19 November 2025, CyberSecDome joined the first COcyber Concertation Workshop at DIGITALEUROPE in Brussels, organised by AMETIC under the COcyber project. The event brought together ten EU-funded cybersecurity projects to launch a practical collaboration model across Europe's cybersecurity and digital trust ecosystem.

CyberSecDome contributed to discussions focused on five cooperation pillars: networking and communication, policy alignment, knowledge and technology transfer, research and innovation, and skills and training. Through the breakout sessions, participating projects identified shared priorities, explored opportunities to reuse tools and datasets, and defined initial joint actions with clear responsibilities and timelines.

The workshop marked the start of a 12-month collaboration that will continue through working groups, quarterly check-ins and a shared repository. For CyberSecDome, this is an important step in strengthening cooperation and contributing to joint outputs that will support the wider European cybersecurity community.

CyberSecDome at Cybersecurity Future: Building Trust in a Digital Europe in Munich, November 2025

On 26 November 2025, CyberSecDome was featured at Cybersecurity Future: Building Trust in a Digital Europe, an event hosted by 28DIGITAL in Munich in collaboration with Start2Group. Bringing together 50–70 stakeholders from the Bavarian cybersecurity ecosystem, including policymakers, academia, SMEs, corporates and EU-level representatives, the event provided an important platform for dialogue on Europe's digital future.

Presented in the “Research & Innovation” segment, CyberSecDome was highlighted as a strong example of EU-supported cybersecurity innovation, with its objectives, open call approach and role in supporting innovative cybersecurity solutions introduced to the audience. Its participation helped raise awareness of funding and innovation opportunities in the field, while further strengthening CyberSecDome’s visibility within the wider European cybersecurity ecosystem.

CyberSecDome M30 Plenary Meeting in Braunschweig, February 2026

The CyberSecDome consortium held its M30 Plenary Meeting in Braunschweig, Germany, on 25-26 February 2026, hosted by project partner AEGIS. As the project moves through its final implementation phase, the meeting provided a valuable opportunity to assess overall progress, confirm key priorities and consolidate the roadmap for the closing phase. Key areas of focus included:

- Core platform & Open Call technical progress
- System integration towards the final demonstrator
- Interoperability & robustness validation
- Final pilots, impact assessment & operational validation

The meeting helped align consortium partners on the final technical and operational priorities, ensuring a coordinated approach to the last phase of implementation. It also confirmed the consortium’s shared commitment to delivering an innovative and robust cybersecurity framework for the protection of critical infrastructures.

CyberSecDome Internal Pilots (OTE/AIA)

The CyberSecDome internal pilots at **Athens International Airport (AIA)** and the **Hellenic Telecommunications Organisation (OTE)** play a central role in validating the project in realistic operational environments provided by project partners. Their purpose is to test, validate and evaluate the CyberSecDome approach against real organisational needs, while also supporting the broader assessment of the project's technical, operational and business value. The internal pilots serve several specific functions within the project:

- **Validation and Evaluation**: They validate the technical, technological and business aspects of the project against established objectives and Key Performance Indicators (KPIs).
- **Customization**: The CyberSecDome process is adapted to the specific characteristics and needs of each pilot environment, such as the **OTE Digital Ecosystem** and the **AIA Digital Ecosystem**.
- **Security Posture Strengthening**:
  - For **OTE**, the pilot aims to strengthen its security posture against new types of cyber-attacks using up-to-date detection and prediction tools.
  - For **AIA**, the pilot focuses on enhancing the capacity of its Security Operations Center to monitor infrastructure traffic and identify anomalies under real-time constraints.
- **Business Resilience and Continuity**: The pilots aim to support the continuity of operations for complex and heterogeneous systems despite potential disruptions caused by cyber-attacks.
- **Situational Awareness**: They are used to demonstrate how the Virtual Reality interface can enhance the awareness of cyber incidents through an Interactive Collaborative User Interface.
- **Risk Mitigation**: The pilots test the system's ability to minimize cybersecurity cascading effects by assessing compromised systems and sharing threat and risk information.
- **Feedback for Refinement**: Feedback from these internal operations is reviewed and adopted to fine-tune the final full operational version of the CyberSecDome system.

The Airbus CyberRange acts as the primary hosting infrastructure for CyberSecDome's virtual validation environment. It enables the consortium to integrate, test and validate the platform in a safe and controlled setting before real-world deployment. Within this environment, digital twin replicas of real-world systems can be created, pilot infrastructures can be reproduced for secure experimentation, and the project's main security, risk

analysis, incident investigation and visualisation capabilities can be integrated and assessed end to end. This controlled setup supports realistic testing while avoiding disruption to live operational systems.

The **AIA Digital Ecosystem pilot** focuses on enhancing the security and resilience of critical airport communication infrastructure within an "Airport's Smart City" environment. Its overall aim is to assess how CyberSecDome can support the protection of communication-related services that are essential for the continuity of airport operations. Its primary objectives are to:

- **Enhance Capacity Building**: Improve the airport's Security Operations Center (SOC) capabilities in monitoring Telephony Infrastructure traffic to identify and mitigate anomalies under real-time constraints.
- **Minimize Cascading Effects**: Utilize CyberSecDome's dynamic risk assessment to assess compromised systems or cyber-dependent infrastructures, preventing the spread of threats across the network.
- **Strengthen Threat Sharing**: Facilitate the sharing of relevant threat and risk information among stakeholders within the Aerotropolis ecosystem to enable an effective coordinated response.
- **Protect Critical Services**: Ensure the resilience of IP-based telephony and unified communications against attacks (such as DDoS on SIP protocols or phishing) that could disrupt travel information or flight operations.
- **Performance Validation**: Test and validate CyberSecDome tools from both socio- and techno-economic perspectives in a demanding 24/7 operational environment serving more than 100,000 passengers daily.

The **OTE Digital Ecosystem pilot** focuses on evaluating the behaviour and impact of various DDoS attack techniques in a controlled and non-operational environment. Its overall aim is to generate realistic malicious traffic and use it to support the validation of CyberSecDome's monitoring, detection and mitigation capabilities, while also illustrating the operational consequences of service disruption in a telecommunications context. Its primary objectives are to:

- **Evaluate Attack Behaviour in a Controlled Environment**: Examine how different DDoS attacks affect service performance and availability under safe experimental conditions.
- **Generate Realistic Validation Data**: Produce representative malicious traffic that can support the testing and refinement of CyberSecDome's detection and mitigation capabilities.
- **Assess Operational Impact**: Explore how service degradation, timeouts and disruptions could affect legitimate users and critical business processes.
- **Support Faster Detection and Response**: Help validate how CyberSecDome can improve visibility, incident understanding and response efficiency in the face of disruptive attack scenarios.
- **Strengthen Organisational Resilience**: Demonstrate the importance of enhanced monitoring, resilience and defense mechanisms for complex digital infrastructures in the telecommunications sector.

The success of the internal pilot operations is measured through a set of project-level and pilot-specific KPIs. These indicators are designed to assess how CyberSecDome performs in realistic operational settings and to measure progress in areas such as anomaly detection, coordinated response, resilience and incident management. For the two internal pilots, the KPIs are tailored to the specific characteristics and priorities of each environment.

AIA pilot KPIs

The AIA pilot Digital Ecosystem KPIs are defined through specific metrics that address the complexities of the airport Aerotropolis smart city environment:

- **Traffic Analysis**: Identify and mitigate anomalies in real-time by 20% compared to current systems.
- **Response Coordination**: Reduce coordinated incident response time by 30%.
- **Knowledge Sharing**: Effective sharing of threat-related information among Aerotropolis stakeholders based on reported incidents.
- **Risk Mitigation**: Improve the identification and mitigation of individual and cascading risks.

OTE pilot KPIs

The success of OTE pilot Digital Ecosystem operations is measured through four distinct KPIs, reflecting the pilot's focus on incident efficiency, service continuity and overall operational impact. The KPIs are:

- **Downtime Reduction:** Reduce downtime during an incident by 25% compared to the case where CyberSecDome is not used.
- **Incident Detection Time:** Reduce the time required to detect an incident by 25% compared to the case where CyberSecDome is not used.
- **Reported Incidents**: The absolute number of reported incidents.
- **Major Security Incidents**: Percentage (%) and absolute number of major security incidents.

These KPIs will continue to be measured across the AIA and OTE scenarios in the coming months to provide a more comprehensive view of CyberSecDome's performance and to ensure full coverage of the validation scope.

The internal pilots at AIA and OTE provide CyberSecDome with an essential bridge between prototype development and real-world applicability. They help verify whether the platform can deliver meaningful value in demanding operational settings, while also generating practical lessons that support the further refinement of the system.

At this stage, the pilots confirm the importance of validating CyberSecDome in realistic environments and show that the project is progressing from conceptual development toward evidence-based operational maturity. As KPI measurement continues and additional validation results are consolidated, the internal pilots are expected to provide an even stronger foundation for the final refinement and overall impact assessment phases of the project.

CyberSecDome
Open Call Round 2

Following the launch of CyberSecDome's Open Call Round 2 and the strong interest highlighted in the previous newsletters, this phase has now progressed from outreach and applicant support to portfolio selection and implementation. Round 2 was designed as the consolidation phase of the CyberSecDome Financial Support to Third Parties scheme, with the objective of extending and deepening the validation of the fully integrated CyberSecDome platform in real-world and near-operational environments. Building on Round 1, it was intended to broaden validation across additional sectors and use cases while focusing on **the validation of the complete CyberSecDome solution**, enabling funded projects to contribute data, attack scenarios and practical feedback that will support the project's final technical refinement and impact assessment.

The response to Open Call Round 2 confirmed the strong interest of the wider innovation ecosystem in CyberSecDome's approach. A total of **79 proposals** were submitted, of which **67 were eligible**, demonstrating both high engagement and a strong level of relevance to the call scope. Among these, **57 eligible proposals scored above threshold**, highlighting the quality and competitiveness of the applicant pool. The process ultimately resulted in the **selection of six funded projects**, while an additional **10 proposals** were placed on the reserve list. The selected projects account for a total approved budget of **€708,250 out of the €780,000 Round 2 envelope**.

The selected Open Call Round 2 portfolio broadens CyberSecDome's validation reach across a diverse set of domains and use cases, including **smart-city parking, medical and finance applications, physical security in critical infrastructures, manufacturing, finance and consulting, and automotive** environments. In this way, Round 2 strengthens CyberSecDome's ability to assess the relevance, applicability and operational value of its platform across heterogeneous environments and sector-specific needs.

#	Acronym	Lead	Domain / Use Case
1	CASPER	DOTSOFT	Smart-city parking
2	SECURE-CLAIM	Covariance	Medical & Finance
3	DRACOS	TERRACOM S.A.	Physical Security in CIs
4	PRINIA-CSD	HUMAN OPSIS G.P	Manufacturing
5	FINCARE	MindTheHack S.A.	Finance and Consulting
6	AutoDome	Binarial	Automotive

By the time of publication of this newsletter, the onboarding of the Round 2 projects has been completed, and the selected projects are already in the implementation phase. This marks an important transition from portfolio selection to practical execution, with the funded projects now contributing to CyberSecDome's broader validation and demonstration activities. The next key milestone for this cohort will be the mid-term review at M32, corresponding to month 5 of the 8-month implementation period, which will provide an important checkpoint on progress, technical alignment and early results.

DISSEMINATION MATERIAL

During this reporting period, the consortium continued to make extensive use of the dissemination material. Project brochures, roll-up banners and posters supported CyberSecDome's presence at key conferences, workshops and other events, ensuring a consistent visual identity and clear messaging around the project concept, pilots and Open Call activities.

In parallel, the project's online dissemination channels remain a central point of access for CyberSecDome material. All public dissemination resources are available through the CyberSecDome website and the project's Zenodo community. Together with recordings from webinars and the Open Call Info Days, these digital resources extend the project's reach beyond physical events and enable stakeholders to engage with CyberSecDome content on demand. All videos are fully accessible on the project's YouTube channel.

PUBLICATIONS – JOURNAL & CONFERENCE PAPERS

The CyberSecDome project has been highly active in disseminating its research results through conference and journal publications. The list of our latest published and accepted articles is shown below:

Conference/Workshop Papers

"CATI – An Open-Source Framework to Evaluate Attacks on Cameras for Autonomous Vehicles",
Michael Kühr, Maximilian Mittmann, Mohammad Hamad, Sebastian Steinhorst,
28th Euromicro Conference Series on Digital System Design (DSD), 10-12/09/2025, Published on 09/12/2025
https://doi.org/10.1109/DSD67783.2025.00078

Journal Papers

"Enhancing Security Through Task Migration in Software-Defined Vehicles",
Mohammad Hamad, Zain A. H. Hammadeh, Davide Alessi, Monowar Hasan, Mert Pese, Daniel Luedtke, Sebastian Steinhorst,
IEEE Internet of Things Journal, Volume 12, Issue 24, 15/12/2025
https://doi.org/10.1109/JIOT.2025.3611875

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

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

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