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

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

LiU LINKÖPING UNIVERSITY

AEGIS IT RESEARCH

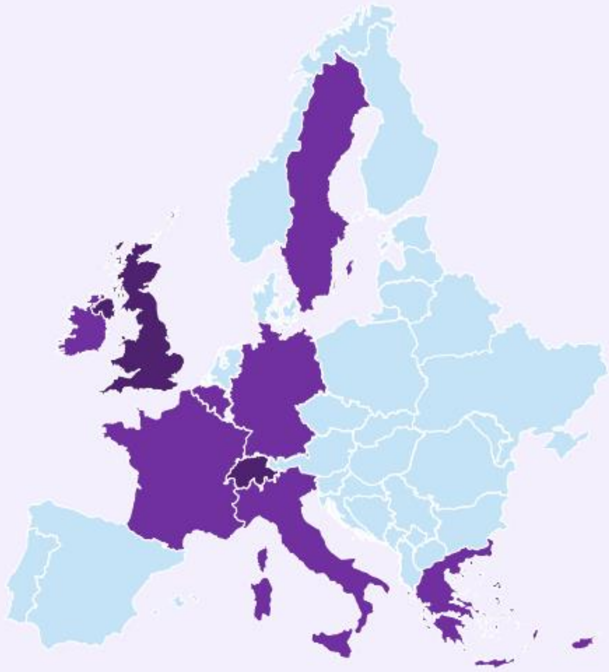
ΠΟΛΥΤΕΧΝΕΙΟ ΚΡΗΤΗΣ TECHNICAL UNIVERSITY OF CRETE

Cyberalytics

itml innovation applied

Sphynx Technology Solutions

a.r.u. Anglia Ruskin University



NEWSLETTER NO 2

February 2024 (M6) – April 2024 (M8)

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, 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 improved 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

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

In February 2024, CyberSecDome partners have gathered in Munich for the 2nd Plenary meeting of the project. The meeting was hosted by Technical University of Munich (TUM).

The main purpose of the meeting was to present the results achieved since the last plenary we had in November 2023 (M3) and produce a solid plan towards the next action items of each work package objectives. Moreover, some of the discussion points were the CyberSecDome pilots' experimentation, their existing infrastructure, reference scenarios, CyberSecDome use cases and their run-time evaluation approach. Also, partners shared ideas about the project's Communication and Dissemination plan, while we focused specifically on the Stakeholder's engagement strategy and joint exploitation activities.

On April 10-11, 2024, at the Athens Conservatory, CyberSecDome participated in the 14th InfoCom Security 2024 Conference showcasing its commitment to advancing cybersecurity solutions. With a rich history of participation in such events, CyberSecDome continues to lead in addressing evolving cyber threats. Partners of OTE, ITML and AEGIS joined the event in order to expand the project's visibility and offerings.

Moreover, Mr. Nikos Kogios, ICT Security Services Senior Manager from OTE Group of Companies, delivered a compelling presentation titled "CyberSecDome: Use of AI & VR in Offensive & Defensive Cybersecurity," shedding light on innovative approaches to cybersecurity.

Use of AI & VR in Offensive & Defensive Cybersecurity
The OTE Pilot Scenarios
Nikos Kogios
ICT Security Services Senior Manager
HYBRID WORLD CYBERSECURITY

CyberSecDome was thrilled to be part of the EIT Digital "Cybersecurity First" event! There is no technology without cybersecurity, on any level you need to have the assurance that the tech you are using or deploying is safe" - a crucial reminder from the discussions! The event, held at EIT Digital's offices in Budapest on April 23rd, and brought together a diverse range of stakeholders from academia, research, and industry to delve into the cybersecurity challenges ahead and explore collaboration opportunities. During the event, Mrs. Annalisa Andaloro shared insights into CyberSecDomeEU's vision, architecture, and its upcoming OpenCall opportunities.

Also, partners from TUC have participated in 2 events, a) at the 8th Cybersecurity Standardisation Conference contributing in discussions of EU legislation, challenges and opportunities for standardisation; and b) at the Webinar "Unlocking NIS2 Compliance with Saviynt and iC Consult", focused on the vital role of Identity Security in achieving compliance with the EU's NIS2 Directive. The session highlighted how Saviynt's Enterprise Identity Cloud (EIC) aligns with the Directive's requirements, offering comprehensive identity governance and security capabilities.

MILESTONES & ACTION ACHIEVED BY OUR PARTNERS

MAGGIOLI SPA (MAG)

Maggioli (MAG) as the Project Coordinator for the CyberSecDome project, initiated the project's activities with a virtual kickoff meeting on September 18th, setting the stage for the subsequent physical kickoff meeting. This latter meeting was hosted by MAG in Athens, Greece, on November 30th and December 1st, attended by representatives from the 15 partner organizations. Some participants also joined remotely, ensuring broad participation.

As the coordinator, MAG managed daily project activities and communications with the Project Officer and held monthly coordination meetings to discuss progress across various work packages and plan future activities. In its role as the leader of Work Package 6 (WP6), which focuses on dissemination and exploitation, MAG maintained regular contact with task leaders to facilitate the broad dissemination of project results.

From a technical standpoint, MAG contributed significantly to discussions on system architecture and technical specifications. It was responsible for the dynamic risk assessment component and played a crucial role as one of the main technical partners in system integration. Additionally, MAG engaged in stakeholder analysis, a part of deliverable D2.1, ensuring a comprehensive approach to understanding and involving relevant stakeholders. These efforts mark the beginning of a long and promising journey in the CyberSecDome project, with MAG and its partners committed to steering the project towards successful outcomes.

Technical University of Munich (TUM)

As part of TUM efforts in WP2 (Requirements, Evaluation Metrics and Architecture from M1-M8) concluded this month, various activities were conducted by the consortium. Specifically, within T2.1, a comprehensive state-of-the-art analysis was performed, identifying research and technology gaps relevant to the tools and solutions CyberSecDome will implement. To understand and analyze the requirements, needs, and interests of key stakeholders, the CyberSecDome consortium executed a stakeholder analysis questionnaire as part of T2.2. The questionnaire was distributed to representatives from critical infrastructure operators, cybersecurity solution providers, research organizations, and policymakers, yielding 37 responses in total. In T2.3, efforts were made to align the technical architecture of CyberSecDome with existing legal and ethical standards, such as GDPR and the NIS Directive, ensuring compliance and creating a reliable digital infrastructure. Additionally, T2.4 involved describing the various scenarios planned for evaluating CyberSecDome. Finally, as part of T2.5, a comprehensive overview of the reference architecture for the CyberSecDome project was conducted, emphasizing its purpose and significance. This task collected functional and non-functional requirements for each project component and outlined their architectural structures, resulting in the collection of 68 requirements. The outcomes of these tasks were presented in two deliverables: D2.1 (State of the Art, Reference Pilot Scenarios, Requirements, and Analysis) and D2.2 (Architecture and Technical Specification of CyberSecDome), both submitted this month.

Athens International Airport (AIA)

AIA coordinated Task 2.2 - Stakeholder requirements, needs, and interests of WP2 in the CyberSecDome project, preparing at the same time the alignment of partners towards the drafting of Deliverable - D2.1 State of the art, Reference Pilot Scenarios, Requirements and Analysis.

Apart from leading this work, AIA designed and developed a comprehensive questionnaire to map the landscape of stakeholder needs in cybersecurity across different sectors. The questionnaire focused on the unique challenges and expectations of each stakeholder group identified in the CyberSecDome project, including telecom and cloud service providers, aviation operators, and sectors like healthcare and finance.

Furthermore, the questionnaire (link) focused on the elicitation, analysis, and documentation of stakeholders' requirements associated with incident detection and response for digital infrastructures and systems.

The results of the questionnaire were described in Deliverable D2.1, which also laid a comprehensive foundation by analyzing the state of the art, reference pilot scenarios, requirements, and analysis pertinent to the project's scope. It has highlighted the critical role of playbooks in Security Orchestration, Automation, and Response (SOAR) tools, the potential of VR in cybersecurity for immersive analytics and situational awareness, and the importance of Federated Learning (FL) for privacy-aware information sharing.

It has also underscored the challenges and opportunities in privacy-aware information sharing, emphasizing the role of FL as a collaborative and privacy-preserving paradigm. The specification of use cases and attack scenarios serves as a basis for pilot demonstrations and validations, showcasing the effectiveness of CyberSecDome tools against representative scenarios.

AEGIS Research (AEGIS)

In a commendable stride towards ensuring ethical, privacy, and security coordination within the CyberSecDome framework, AEGIS has been instrumental across several pivotal tasks from M01 to M08. Leading the charge in Task T1.5, AEGIS developed and disseminated a comprehensive questionnaire targeting data management insights from consortium partners, crucial for identifying and managing datasets throughout the project's lifecycle. This effort culminated in successfully submitting the "Privacy Protection and Data Management Plan" (D1.2) by M06, establishing a foundational document slated for regular updates until project completion at M36.

Simultaneously, under Task T2.3, AEGIS, in collaboration with TUC, undertook a thorough preliminary analysis of the existing national and European legal frameworks and regulatory environments impacting the CyberSecDome. This task involved a detailed literature review and a collaborative questionnaire distributed among partners to gauge their security, privacy, and data protection cultures and perspectives. This phase provided critical inputs for deliverables D2.1 and D2.2, including a detailed standalone report and a set of legal and ethical requirements tailored for the CyberSecDome architecture. A highlight of this task was an online workshop at M8, where key findings and the implications of impending regulations such as the AI ACT and the Cyber Resilience Act were discussed, marking the conclusion of T2.3.

As we progressed to M8, AEGIS also took the lead in Task T3.3, which is related to designing and developing the AI-enhanced incident investigation component of the CyberSecDome framework. A draft version of the ToC for D3.1, titled "Specifications of the AI-empowered security tools", which is now also led by AEGIS, is the first activity for AEGIS during M08 for this task.

DISSEMINATION MATERIAL

As we approach the ninth month 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.

DELIVERABLES SUBMISSION

By the M6 of the project (February 2024), the CyberSecDome consortium have successfully submitted 3 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.

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 Transactions on Consumer Electronics*. (2023). https://doi.org/10.1109/tce.2023.3318754

Randhir Kumar, Ahamed Aljuhani, Danish Javeed, Prabhat Kumar, Shareeful Islam, *et al.* Digital Twins-enabled Zero Touch Network: A smart contract and explainable AI integrated cybersecurity framework. *Future Generation Computer Systems*, *Volume 156*. (2024). Pages 191-205, ISSN 0167-739X. https://doi.org/10.1016/j.future.2024.02.015

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
@CYBERSECDOME-EUproject

Funding

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

EUROPEAN UNION