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

AIRBUS CYBERSECURITY

ATHENS INTERNATIONAL AIRPORT ELEFTHERIOS VENIZELOS

eit Digital

OTE GROUP OF COMPANIES

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

LINKÖPING UNIVERSITY

AEGIS IT RESEARCH

Security Labs Consulting

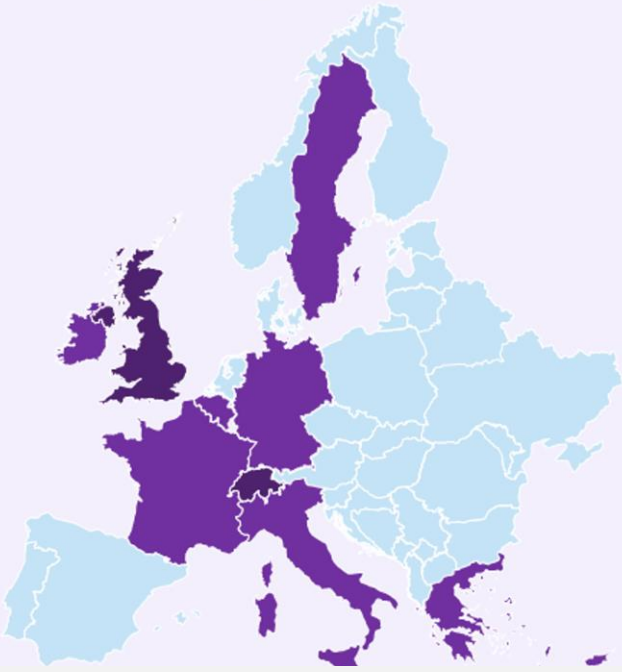
ΠΟΛΥΤΕΧΝΕΙΟ ΚΡΗΤΗΣ
TECHNICAL UNIVERSITY OF CRETE

Cyberalytics
Secure analytics for the interconnected world

itml
innovation applied

Sphynx Technology Solutions

a.r.u. Anglia Ruskin University



NEWSLETTER NO 3

May 2024 (M9) – Aug 2024 (M12)

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

EIT Digital at South Summit, June 2024

EIT Digital, a partner of the CyberSecDome project, had a booth at the South Summit 2024 in Madrid from June 5 to 7, 2024. During the summit, EIT Digital met with many visitors and shared exciting opportunities about the upcoming Open Call for testing the CyberSecDome technology. The discussions with interested organizations were very productive, leading to new connections and possible collaborations.

CyberSecDome participation in the 20th International Federation for Information Processing (IFIP), June 2024

CyberSecDome recently took part in the prestigious 20th International Federation for Information Processing (IFIP) AIAI – International Conference on Artificial Intelligence Applications and Innovations. The event was hosted at the Ionian University of Corfu from June 27th to June 30th, 2024. The AIAI Conference, an established gathering since 2005, operates under the umbrella of IFIP WG12.5 and has grown into a highly regarded platform over the years. With technical and scientific support from the AIAI community—a diverse group of prominent researchers worldwide—this event has become a cornerstone in the field.

Representatives from consortium members OTE, Anglia Ruskin University, and Security Labs showcased the CyberSecDome project at the conference. Additionally, we presented two research papers: 'Enhancing Malware Detection through Machine Learning using XAI with SHAP Framework' and 'Synthetic Data Generation and Impact Analysis of Machine Learning Models for Enhanced Credit Card Fraud Detection'.

Moreover, CyberSecDome has joined the panel discussion that was organised by the EU-project DATAMITE, on the 28th of June 2024. The panel discussion brought together experts from various European projects (EloquenceAI, 6G-PATH, AMBITIOUS Project, Smart5Grid Project) to discuss the importance and impact of data and its monetization in various industries.

CyberSecDome in "Talk.Cybercni.fr" – Your monthly Cybersecurity Speaker Series, June 2024

Since 2021, the TALK.CYBERcni.fr Speaker Series has been raising awareness and fostering dialogue on key cybersecurity topics. This free, monthly event brings together professionals from industry, academia, and the general public to discuss the importance of cybersecurity in today's world.

On June 28, 2024, Mr. Mikael Asplund from Linköping University led a session on "Formally Verifying Security Properties of Cyber-Physical Systems" as part of the TALK.CYBERcni.fr series. His talk focused on the importance of formal verification methods in safeguarding digital infrastructures and highlighted CyberSecDome's proactive approach to addressing cyber threats.

The presentation, followed by a 45-minute interactive discussion, provided valuable insights into implementing security requirements and navigating the evolving cybersecurity landscape. Full session video

Info day, Brussels, July 2024

On July 3rd, 2024, CyberSecDome held a highly successful Info Day at the EIT Digital House in Brussels. The event featured insightful presentations from two of our pilot entities: OTE Group of Companies (HTO) and Athens International Airport (AIA). Fotis Stathopoulos from OTE showcased the telecom sector attack scenarios, while Nikos Papagianopoulos from AIA shared the challenges faced within their dynamic digital ecosystem. These presentations highlighted the critical need for advanced cybersecurity measures in protecting complex digital infrastructures.

Following the pilot presentations, Annalisa Andaloro from EIT Digital and Spiros Fotis from AEGIS IT Research provided valuable insights into our upcoming Open Call. The session ended with a detailed Q&A, fostering an engaging dialogue with attendees for a deeper understanding of the project's objectives and processes. The announcement of our Open Call is scheduled for December 2024, inviting external third parties to test, validate, and provide feedback on the solutions developed within CyberSecDome.

CyberSecDome in "Talk.Cybercni.fr" (2nd session) – Your monthly Cybersecurity Speaker Series

On July 26, 2024, Dr. Shareeful Islam from Anglia Ruskin University (ARU) delivered a compelling talk as part of the series on "Dynamic Cybersecurity Risk Management with Responsible AI Practices." He explored the growing sophistication of cyberattacks and the need for dynamic risk management, drawing from ARU's contributions to CyberSecDome's Dynamic Risk Analysis and PIKS tools. The session also covered how AI-enabled models, such as hybrid approaches combining linear regression and deep learning, can enhance the security and resilience of digital infrastructure. Full session video

MILESTONES & ACTION ACHIEVED BY OUR PARTNERS

MAGGIOLI SPA (MAG)

Maggioli (MAG), as the Project Coordinator for the CyberSecDome Project, along with SCL and ARU, are working on Dynamic Risk Analysis (DRA). DRA is a key sub-component of the CyberSecDome Project, designed to investigate the dynamic parameters of an organization and its security context for identifying and assessing risks. Traditional risk analysis approaches often lack focus on temporal parameters, which can lead to inaccurate risk identification and estimation. DRA addresses this challenge by providing effective risk management practices to enhance the overall resilience of digital infrastructure. The progress of the DRA within the CyberSecDome project context is the adoption of the capability to predict dynamic parameters such as vulnerability exploitation to determine the risk level. Such capability enables learning from evolving data related to threats and vulnerabilities and link them with the related assets so that informed decisions can be taken to mitigate the risk. A novel hybrid model is used which combines Extra Trees Regressor and Neural networks for this purpose and the experiment is performed using widely used exploit and CVEjoin datasets. Moreover, the AI model decision making process is well explained using the explainable AI towards the trustworthy AI enabled model development for the DRA.

Technical University of Munich (TUM)

As part of the efforts in WP2 (M9-M12) concluded this month, various activities were conducted by the consortium. One of the key components of the CyberSecDome framework is the Dynamic and Adaptive Incident Response (DAIR) tool from TUM. DAIR is designed to help organizations respond to cyber threats quickly and automatically. Over the past few months, we have made significant progress in developing DAIR. We've established the tool's internal structure, which uses artificial intelligence (AI) to make optimal decisions and improve response strategies. After researching and testing various AI methods, we selected reinforcement learning, allowing DAIR to adapt its response playbook to evolving threats effectively. Collaboration with our partners ensures that DAIR can seamlessly share data across the CyberSecDome framework, which is vital for its success. We have also prepared DAIR for integration into Cyberspace, paving the way for its full deployment soon.

ITML

Within CyberSecDome, ITML is leading the technical work on the specifications and development of the AI-Empowered Security Tools (Work Package 3). Over the first nine months, substantial progress has been made in developing prototype tools, refining interfaces, and preparing pilot integration plans. ITML has also focused on implementing a federated learning prototype, which aims to provide a privacy-aware, live, and collaborative training solution for CyberSecDome's AI models. This approach will allow organizations to collaborate by sharing AI insights while keeping their data local. Looking ahead, ITML will continue advancing the federated learning mechanism, ensuring it is ready for integration and real-world application in the coming months.

Hellenic Telecommunications Organisation S.A (OTE)

Over the first year of the project, OTE concentrated on identifying and refining the use cases that would serve as the foundational material for developing detailed attack scenarios. This process involved a comprehensive review and analysis of several critical aspects related to each use case. These aspects included:

Roles and Responsibilities: The project team assessed the roles and responsibilities of individuals and groups involved in each use case. Organizational Structures: An examination of the existing organizational frameworks was conducted to determine how different departments or teams interact and support each other, especially in the context of cybersecurity. Assets: The identification and classification of key assets were undertaken. These assets could be anything

from data, hardware, software, or any other resources critical to the organization's operation. Understanding what needs protection is vital for creating relevant and realistic attack scenarios. Security Measures: Current security measures in place were reviewed to assess their effectiveness in defending against potential attacks. Digital Infrastructure and Related Processes: The digital infrastructure, including networks, systems, and processes, was mapped out. This detailed analysis ensured that all components of the organization's digital environment were considered when developing attack scenarios.

The information gathered during this phase was not only crucial for developing detailed attack scenarios but also for summarizing the essential data needed for later stages of the project, particularly for deployment within the CyberSecDome environment. Additionally, through the exploration of use cases and attack scenarios, valuable insights were gained concerning the visualization aspects of cybersecurity. Specifically, this involved examining how users interact with cybersecurity tools and interfaces, which is critical for designing effective visualizations. These insights will inform subsequent work packages, ensuring that the user interface and interaction dimensions are tailored to the needs and behaviors of the end-users. This focus on user interaction is essential for creating tools that are not only technically sound but also intuitive and user-friendly, ultimately enhancing the overall cybersecurity posture of the organization.

EIT Digital

EIT Digital coordinated the preparatory actions to launch the Open Call for Pilots, expected for December 2024.

The consortium partners worked on setting-up the strategy and approach to be adopted in order to deliver the Open Call for Pilots in the months to come. Regular meetings have been taking place and the process for the Open Call set-up and management is now defined. Two rounds of the Open Call will take place, one consecutive to the other, starting in December 2024.

This work resulted in successful delivery of the Open Call approach and technical specifications at the end of August 2024.

In preparation for the launch of the Open Call for Pilots, the first Open Call Info Day was hosted during July 2024 at the EIT House in Brussels, organized by EIT Digital with live contributions and keynote speeches by Maggioli, AEGIS Research, ITML, Athens International Airport and OTE Group. Around 25 participants attended the event and an interesting discussion among prospect applicants and the consortium took place. This action helped to further sharpen and focus the strategy on the Open Call approach and technical specifications.

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.

DELIVERABLES SUBMISSION

By the M12 of the project (August 2024), the CyberSecDome consortium have successfully submitted the below 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.
- ✓ D1.3 Annual Management Report (Lead: MAG); M12.
- ✓ D5.2 Open call methodology and procedures (Lead: EIT); M12.

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:

MDPI

Katrakazas, P., & Papastergiou, S. (2024). A Stakeholder Needs Analysis in Cybersecurity: *A Systemic Approach to Enhancing Digital Infrastructure Resilience*. https://zenodo.org/records/13254710

SPRINGER LINK

Islam, S., Javeed, D., Saeed, M. S., Kumar, P., et al., (2024). Generative AI and Cognitive Computing-Driven Intrusion Detection System in Industrial CPS. *Cognitive Computing* (V. 16, pages 2611–2625). https://zenodo.org/records/13254989

ScienceDirect

Hamad, M., Finkenzeller, A., Kühr, M., Roberts, A., Maennel, O., Prevelakis, V., & Steinhorst, S. (2024). REACT: Autonomous Intrusion Response System for Intelligent Vehicles. *Computers & Security* (V. 145). https://zenodo.org/records/13255072

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 Horizon Europe Framework Programme (2021-2027) under the grant agreement No 101120779.

European Commission | HORIZON EUROPE 2021-2027