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

28DGTL

OTE GROUP OF COMPANIES

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

LiU 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

a.r.u. Anglia Ruskin University

NEWSLETTER No 6

June (M22) – October (M26)

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.

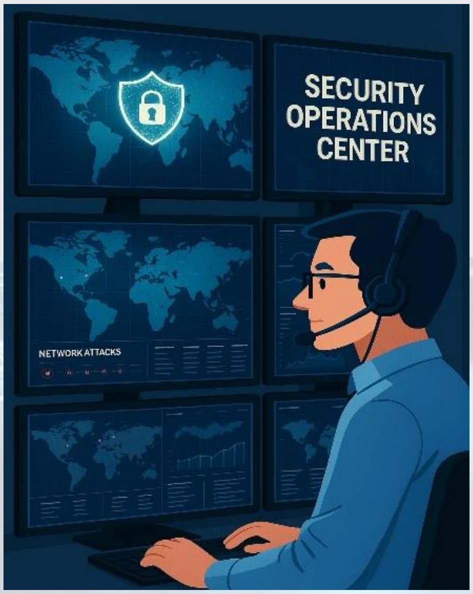
CyberSecDome’s Pilots

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 Cluster Synergies Webinar, May 2025

On May 15, 2025, CyberSecDome hosted a dedicated Cluster Synergies Webinar, bringing together several Horizon Europe projects in the field of cybersecurity to foster knowledge exchange and explore collaboration opportunities. The session featured presentations from key initiatives including COcyber, Phoeni2x, SecAwarenessTruss, SYNAPSE, CUSTODES, CONSOLE, CoEvolution, and CRACoWi, with speakers sharing insights into their project goals, current results, and areas of potential synergy. This interactive discussion reinforced the importance of cross-project collaboration in tackling Europe's evolving cybersecurity challenges and laid the groundwork for future joint actions within the cybersecurity cluster.

CyberSecDome at CyberHOT Summer School 2025, May 2025

On May 25, 2025, CyberSecDome opened the floor at the CyberHOT Summer School 2025, hosted by the Technical University of Crete in Chania, Greece. Dr. Andreas Miaoudakis from CBL delivered the opening presentation, introducing the project's vision, scope, and core activities in strengthening Europe's cybersecurity landscape. CyberHOT is one of Europe's leading hands-on training events in cybersecurity, gathering students, researchers, and professionals for immersive learning experience. CyberSecDome was proud to contribute to this dynamic setting, engaging with the next generation of cybersecurity experts.

CyberSecDome at Security Research Event 2025 (SRE2025), June 2025

CyberSecDome was proudly presented at the Security Research Event 2025 (SRE2025), held on June 2025 at the EXPO XXI venue in Warsaw, Poland. With the support of our partner ITML, the project's innovative approach to immersive, AI-enabled threat detection and incident response was showcased to a diverse audience of researchers, policymakers, and security professionals. SRE2025 provided an excellent platform to connect with stakeholders across Europe's security research ecosystem, engage in insightful discussions, and explore potential synergies with other EU-funded initiatives.

CyberSecDome at 10th IEEE European Symposium on Security and Privacy (EuroS&P 2025) in Venice, Italy, June 2025

CyberSecDome was represented at the EuroS&P 2025, held in June 2025 in Venice, Italy. Our partner Kostas Drakonakis from the Technical University of Crete (TUC) contributed to the "User, Web & Measurement" session with a presentation of the paper "Dredging the River Styx: Fortifying the Web through Robust and Real-Time Script Attribution". Following the conference session, a dedicated poster session enabled more extensive Q&A and networking with attendees. During these interactions, CyberSecDome was further acknowledged and communicated at a high level, helping raise the project's visibility within the security and privacy research community and fostering new connections with stakeholders interested in its outcomes.

CyberSecDome at Euromicro Conference on Real-Time Systems (ECRTS) in Brussels, Belgium, July 2025

Technical University of Munich (TUM) organized the 2nd Workshop on Real-Time Autonomous Systems Security (RT-AUTOSEC) as part of the main ECRTS 2025 conference. During the workshop, our partner Mohammad Hamad (TUM) presented the CyberSecDome project and highlighted the Open Call funding opportunities to the real-time and autonomous systems community. In the main ECRTS 2025 conference, the paper "Sensor Fusion Desynchronization Attacks", which acknowledged CyberSecDome, was also presented, further strengthening the project's visibility within the real-time systems and security research ecosystem.

Workshop on Real-Time Autonomous Systems Security (RTAutoSec 2025)

Mohammad Hamad – TUM
Monowar Hasan – WSU

CyberSecDome at 28th Euromicro Conference Series on Digital System Design (DSD) in Salerno, Italy, September 2025

CyberSecDome was represented at the 28th Euromicro Conference Series on Digital System Design (DSD 2025), held in September 2025 in Salerno, Italy. Our partner Michael Kühr from the Technical University of Munich (TUM) presented the paper "CATI – An Open-Source Framework to Evaluate Attacks on Cameras for Autonomous Vehicles", which acknowledged CyberSecDome. The contribution addressed security challenges in autonomous vehicle perception and the evaluation of camera-based attacks and further increased CyberSecDome's visibility within the digital systems and security research community.

CATI – An Open-Source Framework to Evaluate Attacks on Cameras for Autonomous Vehicles

Michael Kühr, Maximilian Mittmann, Mohammad Hamad, Sebastian Steinhorst

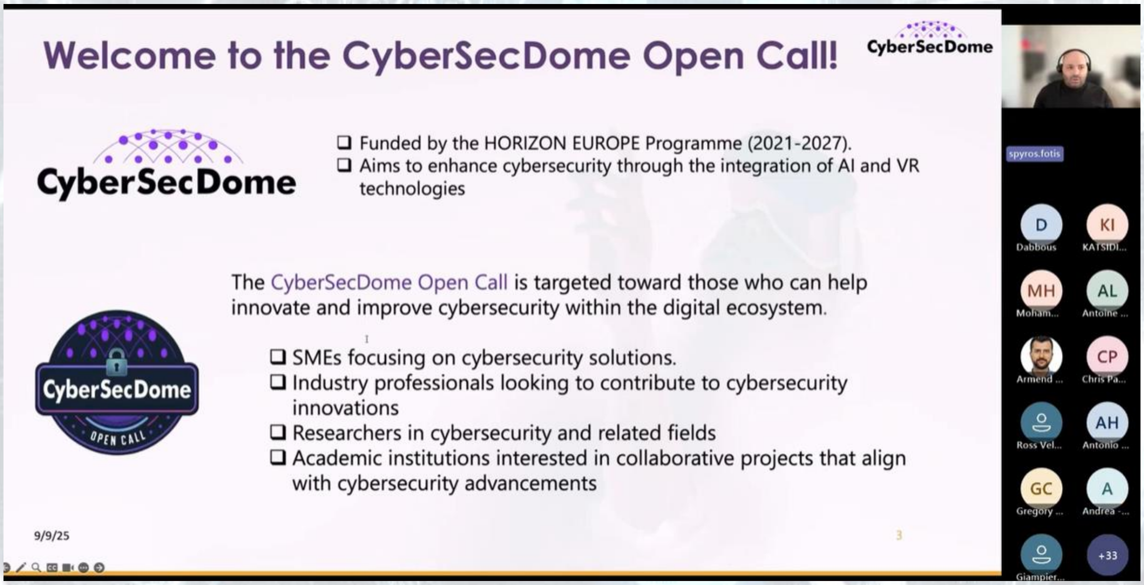
Associate Professorship of Embedded Systems and Internet of Things
TUM School of Computation, Information and Technology
Technical University of Munich

September 12th, 2025

CyberSecDome Open Call Round 2 Info Day and Q&A session, September 2025

CyberSecDome organised the Open Call Round 2 Info Day and Q&A session, which was held online on 9 September 2025. The event, which attracted 49 participants, was fully dedicated to presenting the details of the second-round open call and providing potential applicants with structured guidance on the objectives, requirements, and conditions of participation. During the session, the consortium outlined the objectives and requirements of Open Call Round 2, including the types of solutions and use cases CyberSecDome aims to attract. Participants received a step-by-step overview of the application procedure, covering key timelines, evaluation criteria, and available funding opportunities.

A dedicated Q&A session allowed attendees to raise both technical and administrative questions directly with the project team, helping them assess the fit of their solutions and refine their application strategy. Further documentation, guidelines, and contact points were shared to enable participants to continue engaging with the consortium beyond the event. The recording of the session is available here.



Welcome to the CyberSecDome Open Call!

❑ Funded by the HORIZON EUROPE Programme (2021-2027).
❑ Aims to enhance cybersecurity through the integration of AI and VR technologies

The CyberSecDome Open Call is targeted toward those who can help innovate and improve cybersecurity within the digital ecosystem.

❑ SMEs focusing on cybersecurity solutions.
❑ Industry professionals looking to contribute to cybersecurity innovations
❑ Researchers in cybersecurity and related fields
❑ Academic institutions interested in collaborative projects that align with cybersecurity advancements

9/9/25

3

CyberSecDome M24 Plenary Meeting in Cambridge, September 2025

CyberSecDome held its M24 Plenary Meeting in Cambridge, UK, on 15–16 September 2025, hosted by project partner Anglia Ruskin University (ARU). The two-day meeting marked a key coordination point for the next phase of the project, combining strategic review with hands-on technical and exploitation planning.

On the first day, partners focused on the status and next steps of the Open Call Round 1 funded projects, reviewing their progress and aligning on upcoming activities. The second day was dedicated to discussing overall project progress, including tools' integration, pilot activities, and dissemination and exploitation plans. Engaging discussions, demos, and collaborative planning helped consolidate a shared roadmap for the coming period, effectively setting the stage for the continued advancement of CyberSecDome's objectives.

CyberSecDome Open Call Round 1

Following the successful completion of the submission, validation and onboarding process of the nine funded third-party projects under the CyberSecDome Open Call Round 1, implementation has now reached its mid-term stage. The selected projects are actively executing their planned activities, integrating and testing their cybersecurity solutions within the CyberSecDome ecosystem and preparing their mid-term reports. This work is being carried out in close collaboration with the Open Call Management Team (OCMT) and the Open Call Implementation Team (OCIT), who provide continuous technical guidance, monitoring and coordination support to ensure alignment with the project's architecture, use cases and overall objectives.

Building on these activities, this edition puts the spotlight on the nine funded projects of Open Call Round 1. The following profiles provide a snapshot of their focus, illustrating how each of them contributes to the CyberSecDome ecosystem and to strengthening cybersecurity capabilities in real operational environments.

CASeR-Safe - Collaborative Assessment of Security and Robustness of Smart Home as Safety Critical Environments

Coordinator: Smartotum (Italy)

Participating organisation(s): N/A

Domain: Smart Home

Key use case: Wireless smart home with multiple gateways and several (around 80) devices including sensors and actuators, potentially prone to cyber-attacks.

Description of work: CaSER-Safe delivers a measurable and practical improvement to smart-home cybersecurity by assessing, validating, and enhancing the resilience of the Smartotum framework using next-generation tools from the CyberSecDome ecosystem. The project provides a rigorous baseline security evaluation, identifies real-world vulnerabilities, and demonstrates how advanced monitoring, threat detection, and forensic capabilities can significantly reduce the attack surface of consumer IoT environments. By combining real deployments, systematic assessment, and CyberSecDome technologies, CaSER-Safe showcases a concrete, scalable pathway to strengthen the protection of connected homes, improve user trust, and support the wider adoption of secure-by-design smart-home solutions.

Main expected results:

- Increased awareness on cybersecurity flaws and vulnerabilities for the Smartotum framework
- Risk analysis and prioritization of hardening actions
- Increased system security and resilience

Contact: Dimitris Koutras, Senior Researcher, kdimitris@focalpoint-sprl.be

DomeSentinel - AI-Driven Threat Detection and VR Cyber Defence

Coordinator: Focal Point SPRL (Belgium)

Participating organisation(s): Plaixus

Domain: Cybersecurity, Cyber Ranges, AI-driven Threat Detection

Key use case: Evaluation of CyberSecDome tools using realistic Smart Home and Manufacturing CPS attack scenarios within advanced cyber ranges.

Description of work: DomeSentinel deploys two advanced cyber ranges —Smart Home and Manufacturing CPS, deployed in Ludus to evaluate CyberSecDome's AI-driven threat detection, incident response, and VR-based situational awareness tools. The project develops relevant attack scenarios and collects high-quality telemetry for benchmarking detection accuracy, false positives, and incident response time. By leveraging realistic APT-style behaviour, DomeSentinel ensures robust validation of CyberSecDome's technologies in safe, reproducible environments.

Main expected results:

- Fully deployed Smart Home and Manufacturing CPS cyber ranges
- Executed relevant attack scenarios and telemetry collection
- KPI-based evaluation of CyberSecDome tools

Contact: Dimitris Koutras, Senior Researcher, kdimitris@focalpoint-sprl.be

ACRYS - Cyber Risk Assessment via Dynamic Risk Analysis (DRA)

Coordinator: CYBERFLIP S.A. (Greece)

Participating organisation(s): WOLI SERVICES L.T.D (Cyprus)

Domain: Cyber Risk Management /Fintech /Cloud-based digital services

Key use case: The DRA tool will be utilized to perform a cyber risk assessment on WOLI Environment. Results will be thoroughly reviewed and confirmed in cooperation with WOLI's experts, while also CYBERFLIP's experts will assess the percentage of efficiency in terms of time and results comparing to traditional risk assessment method.

Description of work: ACRYS aims to modernize cyber risk assessment by integrating Dynamic Risk Analysis (DRA) into the security processes of WOLI, a fintech platform serving young users. The project focuses on enhancing risk visibility across a highly interconnected cloud environment, mapping asset dependencies, and enabling data-driven evaluation of probability and impact. By comparing traditional assessment methods with fully dynamic, continuously updated risk insights, ACRYS helps bridge the gap between technological risks and business decision-making. Its overarching objective is to support proportional cybersecurity investments while contributing to safer digital experiences, especially important in environments handling sensitive data from minors.

Main expected results:

- Enhance visibility of cyber risks across cloud assets
- Achieve reduced time for risk profiling in comparison to manual process
- Improve risk assessment process efficiency

Contact: info@cyberflip.eu

ATTENTO - Advanced Threat deTEctioN in facTOry 4.0

Coordinator: Buontech Solutions srl (Italy)

Participating organisation(s): N/A

Domain: Industry 4.0, Manufacturing Security

Key use case: Automated factory with 27 robots experiences sensor manipulation attack; DRA detects cascading risks across production lines in under 3 minutes, preventing €500K potential damage.

Description of work: ATTENTO leverages CyberSecDome's Dynamic Risk Analysis (DRA) platform to provide comprehensive risk assessment for Industry 4.0 environments. The project employs a sophisticated digital twin of a manufacturing complex with multiple interconnected assets including robots, PLCs, and IoT devices. By simulating cyber-attack generated cascading failures based on MITRE ATT&CK framework, ATTENTO identifies interdependencies, quantifies threat impacts, and provides actionable mitigation strategies.

Main expected results:

- 25% improvement in threat detection and response
- Risk prediction under 3 minutes
- 25% improvement in risk prediction accuracy

Contact: info@buontech.com

SCAF-DOME - Strengthening Cybersecurity and Authentication for Fact-checking

Coordinator: Athens Technology Center (ATC) (Greece)

Participating organisation(s): N/A

Domain: Cybersecurity in Media Organizations

Key use case: Simulating cyberattacks on a replicated fact-checking infrastructure to evaluate and enhance the performance, accuracy, and robustness of CyberSecDome's security tools.

Description of work: The SCAF-DOME project focuses on strengthening cybersecurity for fact-checking infrastructures by replicating an EDMO-like environment and evaluating CyberSecDome tools. The work includes deploying cloud-native infrastructure, developing realistic cyberattack scenarios—such as DDoS, brute force, port scanning, and supply-chain attacks—and integrating SIEM, Prophecy, and FVT for performance assessment. The project measures detection accuracy, false positives, prediction quality, and visualization effectiveness. Continuous feedback will refine tool functionality and guide their optimisation for large-scale deployment within CyberSecDome. The final outcome is a validated, scalable security framework suitable for modern fact-checking ecosystems.

Main expected results:

- Validated security tools under realistic cyberattack conditions
- Improved detection, prediction, and false-positive performance
- Optimised, deployment-ready cybersecurity framework for fact-checking systems

Contact: Maritini Kalogerini, Project Manager at ATC, m.kalogerini@atc.gr

---

ELEVATE - Advanced Security for Cyber-Enabled Networked Elevators and Devices

Coordinator: Pragma-IoT S.A (Greece)

Participating organisation(s): N/A

Domain: Cybersecurity for Cyber-Physical Systems

Key use case: ELEVATE evaluates a set of realistic cyberattack scenarios targeting IoT-enabled elevator systems and validates CyberSecDome's detection, forensic and automated response capabilities. Scenarios include: 1. Unauthorized access on remote maintenance (SSH) service of the cloud server and malware installation; 2. Remote unauthorized access to the Elevator Control System Web Portal; 3. Malware Introduction via Service Tools; 4. Unauthorized data exfiltration attempt via SQL injection; 5. Denial-of-Service (DoS) on cloud server.

Description of work: ELEVATE brings cyber resilience to next-generation smart elevators by combining cybersecurity assessment, real-world IoT attack scenarios and AI-assisted detection tools. ELEVATE aims to strengthen the cybersecurity of smart elevators through a twofold approach. First, it collects and generates comprehensive datasets representing both normal elevator operation and a variety of realistic cyberattack conditions. These datasets are provided to the CyberSecDome framework to support the assessment, training and optimisation of its internal detection, forensics and response tools across different scenarios. Second, ELEVATE evaluates and benchmarks its own security mechanisms using the same data, producing Key Performance Indicators (KPIs) that enable direct comparison with CyberSecDome's results. Through this dual process, the project contributes valuable insights into the effectiveness of cybersecurity solutions for smart IoT-enabled elevator systems.

Main expected results:

- Comprehensive IoT elevator cyberattack datasets for training and evaluation of detection tools
- Deployment of AI-assisted intrusion detection and automated incident response mechanisms
- Benchmarking KPIs for assessing and comparing CyberSecDome platform's cybersecurity effectiveness

Contact: info@pragma-iot.com

ADAPT - AI-Driven Automated Penetration Testing

Coordinator: CYBERFLIP S.A. (Greece)

Participating organisation(s): WOLI SERVICES L.T.D (Cyprus)

Domain: Penetration testing /Fintech /Cloud-based digital services

Key use case: Applying AI-driven penetration testing in a cloud fintech ecosystem to compare automated and manual methods, improve detection accuracy, and accelerate vulnerability assessment across modern cloud architectures.

Description of work: ADAPT aims to validate and improve CyberSecDome's AI-powered automated penetration testing tools by applying them in a real fintech environment. Using WOLI's cloud-based ecosystem as a demanding use case, the project assesses how AI can simulate attack scenarios, identify vulnerabilities, and enhance system resilience more efficiently than traditional approaches. ADAPT focuses on improving detection accuracy, reducing false positives, and validating whether automated methods can reliably scale across complex architectures. By combining expert-driven manual penetration testing with AI-assisted techniques, the project generates actionable insights, strengthens cybersecurity readiness, and supports safer digital services—particularly in environments handling sensitive data such as those used by young users.

Main expected results:

- Validated AI penetration-testing framework with improved detection accuracy
- Reduced vulnerability discovery time compared to manual testing
- Actionable recommendations to enhance CyberSecDome's automated tools

Contact: info@cyberflip.eu

CATT-46 - CyberSecDome AI Tool Testing with i46

Coordinator: i46 s.r.o (Czechia)

Participating organisation(s): CyberSecDome project

Domain: Evaluation & Testing of Cybersecurity Solutions

Key use case: The primary use case is providing a realistic, multi-layered testbed for CyberSecDome's AIdriven penetration testing tools, focusing on vulnerability identification and compliance with Cyber Resilience Act (CRA).

Description of work: The project's core objective is the rigorous validation of AI-driven automated penetration testing tools against a realistic, multi-layered IoT infrastructure. This commences with establishing a secure, isolated testing environment, comprising an AWS cloud server and a dedicated physical server in Prague. The subsequent evaluation employs a systematic SMART testing methodology, simulating sophisticated attacks in the following three scenarios: website penetration with and without credentials, general penetration to the i46 server and i46 client, and penetration via API. This includes challenging the AI tools with artificial constraints like programmed device failures. The final output will be a comprehensive report with actionable insights and recommendations for improving CyberSecDome's tools.

Main expected results:

- Testing of the 3 scenarios
- Vulnerability discovery rate in simulated attacks
- Final report with actionable recommendations to CyberSecDome

Contact: SeongEun, Project Manager, seongeun@i46.cz

SHIELD - Secure High-Impact Enhanced Learning Datasets

Coordinator: i46 s.r.o (Czechia)

Participating organisation(s): CyberSecDome project

Domain: Evaluation & Testing of Cybersecurity Solutions

Key use case: The prepared datasets will enable rapid exploitation of data for pen-testing, network vulnerability analysis, and proactive defense, enhancing the effectiveness and training of CyberSecDome's AI models.

Description of work: SHIELD will leverage i46's extensive IoT telemetry dataset, which is derived from real-life production devices. The raw data provides a substantial foundation for cybersecurity analysis. The core process involves systematic data cleaning and optimization, using techniques like redundancy removal and outlier detection. This refinement is crucial for removing redundant, irrelevant, or inconsistent records while deliberately preserving the dataset's richness and diversity. The final, high-quality, and GDPR-compliant dataset will be delivered, validated, and analyzed by CyberSecDome to enhance threat detection modeling, dynamic risk assessment, and automated pen-testing tools. The expected outcome is a set of refined data supporting the training of diverse AI models.

Main expected results:

- Delivery of network flow data
- Dataset supports training for at least 3 distinct AI models/tools
- Improved cybersecurity capabilities and cost savings for CyberSecDome

Contact: SeongEun, Project Manager, seongeun@i46.cz

CyberSecDome
Open Call Round 2

Following the launch of the CyberSecDome Open Call Round 2 on 1 August 2025, the call attracted strong interest from stakeholders across Europe, including its primary target sectors of aviation and telecom, as well as underrepresented sectors such as healthcare, finance, energy, industrial IoT, public services, smart cities, and more, where Round 2 aims to broaden its impact. Round 2 focuses on the deployment, testing, and validation of the fully integrated CyberSecDome platform in real-world operational environments, enabling third-party beneficiaries to act as pilot sites and to provide structured technical and operational feedback on the platform's performance, scalability, and interoperability.

To further support potential applicants, the project organised the Open Call Round 2 Info Day and Q&A session on 9 September 2025. Held online, the event attracted 49 participants from across Europe and provided a detailed walkthrough of the call objectives and scope, eligibility rules, evaluation criteria, funding conditions, and application procedure. A dedicated Q&A session allowed attendees to raise technical, administrative, and strategic questions directly with the CyberSecDome team. The session's recording and presentations have been made available on the project website, ensuring that interested organisations can still benefit from the guidance provided during the Info Day.

The submission window for Open Call Round 2 closed on 30 September 2025. In total, the call received 79 proposals, submitted via the F6S platform from a diverse set of applicants across multiple countries. After the completion of the eligibility checks carried out in early October 2025, 67 proposals were confirmed as eligible and advanced to the expert evaluation and ranking phase. At the time of writing, Open Call Round 2 is in evaluation and ranking stage, with notification of results and sub-grant agreement preparation and signing scheduled for early December 2025, and the funded projects expected to start their activities in December 2025.

Milestone	Tentative Date / Period	Description	Status
Finalisation of Documentation	July 2025 (M23)	Open Call documentation and internal procedures finalised by the OCMT.	✓
Open Call Announcement	August 2025 (M24)	Official call launch, full documentation bundle published on F6S and website.	✓
Proposal Submission Window	August – September 2025 (M24–M25)	Applicants submit proposals via F6S. Deadline: September 30, 2025 at 17:00 Brussels Time	✓
Eligibility Check	October 1–7, 2025 (M26)	Formal verification of applicant and proposal eligibility.	✓
Evaluation Period & Ranking	October 8 - November 24, 2025 (M27)	• Independent review and scoring by external evaluators and HoTs. • Consensus process and final ranking by topic.	🔄
Notification of Results	Late November – early December 2025 (M27–M28)	Applicants receive Evaluation Summary Reports and funding decisions.	Upcoming
Sub-Grant Agreement Signing	Early December 2025 (M28)	Selected beneficiaries sign their Sub-Grant Agreements with the coordinator.	Upcoming
Project Start	December 2025 (M28)	Funded projects officially commence activities; exact start dates to be agreed per sub-grant.	Upcoming
Project End - Final Review & Reporting	August 15, 2026 (M36)	• End of implementation period for Round 2 projects. • Final progress assessment and reporting against KPIs.	Planned

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, while the podcast episode introducing the project and its Open Call rounds continues to complement these efforts. Together with recordings from recent 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 - JOURNALS

The CyberSecDome project has been highly active in disseminating its research results through conference and journal publications. The list of published and accepted articles from June (M22) to October (M26) is shown below:

Conference/Workshop Papers

Andrew Roberts, Mohsen Malayjerdi, Mauro Bellone, Raivo Sell, Olaf Maennel, Mohammad Hamad, Sebastian Steinhorst, "Analysis of Autonomous Driving Software to Low-Level Sensor Cyber Attacks", 2025 IEEE/ACM 20th Symposium on Software Engineering for Adaptive and Self-Managing Systems (SEAMS), 13/06/2025, https://doi.org/10.1109/SEAMS66627.2025.00021

Andreas Finkenzeller, Andrew Roberts, Mauro Bellone, Olaf Maennel, Mohammad Hamad, Sebastian Steinhorst, "Sensor Fusion Desynchronization Attacks", Euromicro Conference on Real-Time Systems (ECRTS 2025), 07/07/2025, https://doi.org/10.4230/LIPIcs.ECRTS.2025.6

Kostas Drakonakis, Sotiris Ioannidis, Jason Polakis, "Dredging the River Styx: Fortifying the Web through Robust and Real-Time Script Attribution", 2025 IEEE 10th European Symposium on Security and Privacy (EuroS&P), 26/08/2025, https://doi.org/10.1109/EuroSP63326.2025.00020

Michael Kühr, Maximilian Mittmann, Mohammad Hamad, Sebastian Steinhorst, "CATI – An Open-Source Framework to Evaluate Attacks on Cameras for Autonomous Vehicles", 28th Euromicro Conference Series on Digital System Design (DSD) 2025 – Accepted

Journal Papers

Zain A. H. Hammadeh, Monowar Hasan, Mohammad Hamad, "RESCUE: A Reconfigurable Scheduling Framework for Securing Multi-Core Real-Time Systems", ACM Transactions on Cyber-Physical Systems, Volume 9, Issue 3, Article No.: 28, Pages 1 – 23, 04/08/2025, https://doi.org/10.1145/3728364

Andreas Finkenzeller, Arne Fucks, Emanuel Regnath, Mohammad Hamad, Sebastian Steinhorst, "Securing the Precision Time Protocol with SDN-enabled Cyclic Path Asymmetry Analysis", ACM Transactions on Cyber-Physical Systems, Volume 9, Issue 3, Article No.: 33, Pages 1 – 25, 04/08/2025, https://zenodo.org/records/17294266

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