

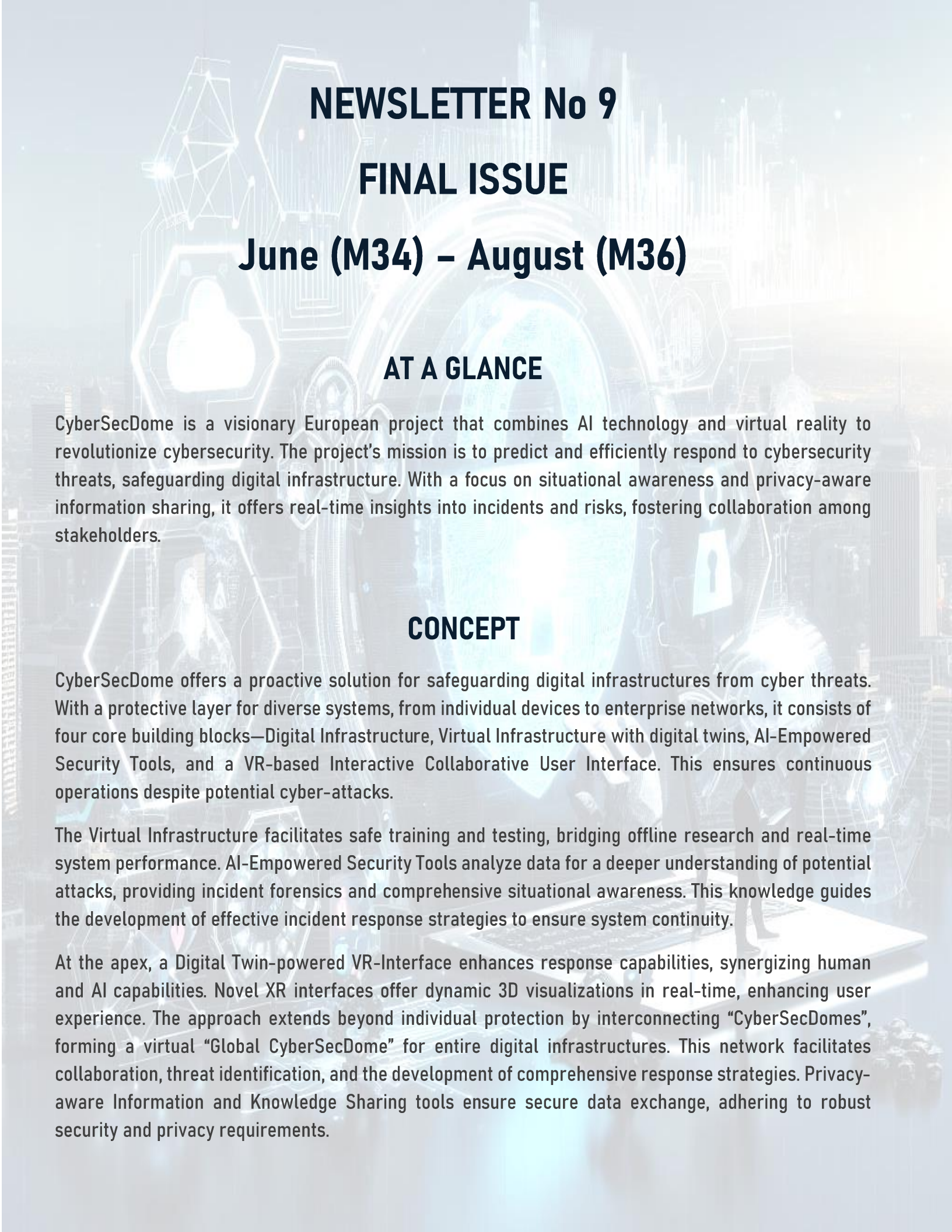
CyberSecDome



*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 9

FINAL ISSUE

June (M34) – August (M36)

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.



CyberSecDome in Numbers – 36 Months of Dissemination and Communication Impact

Over its 36-month duration, CyberSecDome combined scientific dissemination, professional outreach, stakeholder engagement and digital communication to make its results visible and accessible to researchers, industry representatives, policymakers, cybersecurity practitioners, SMEs and the wider public. The figures below present the project's cumulative dissemination and communication impact from M1 to M36.

SCIENTIFIC AND PROFESSIONAL DISSEMINATION

17	29	6	9
Journal outputs	Conference papers	International magazine articles	Newsletters
14 publications in international refereed journals and 3 special issues	27 published and 2 accepted	3 published and 3 accepted	Covering progress, technical activities, Open Calls, events and results

EVENTS AND COLLABORATION

16	34	10	200+
Dissemination events	Third-party events attended	Sister projects identified	Printed copies
Organised or co-organised by CyberSecDome partners	Extending visibility across scientific, professional, industrial and policy communities	Engaged through 3 jointly organised clustering workshops	Distributed at more than 14 events

DIGITAL REACH AND ACCESSIBLE RESOURCES

8,484	2,401	838	1,912
Website visitors	Website downloads	LinkedIn followers	YouTube views
Generating 16,684 pageviews	Plus 3,055 downloads through the project's Zenodo community	Together with 3,566 profile views by M36	

Together, these results reflect CyberSecDome's strong scientific visibility, broad stakeholder engagement and continued commitment to making its public outputs accessible beyond the formal end of the project.

MEETINGS & EVENTS: M34-M36

CyberSecDome M34 Plenary Meeting in Chania, June 2026

On 2–3 June 2026, the CyberSecDome consortium gathered in Chania, Crete, for its M34 plenary meeting, marking another important step towards the final stages of the project. The meeting brought together CyberSecDome partners for productive discussions, progress updates and alignment on the remaining activities. Partners actively contributed to the exchange, reviewing key achievements, addressing next steps and strengthening collaboration across the consortium. This plenary meeting provided a valuable opportunity to consolidate progress and support the successful completion of CyberSecDome, while reaffirming the consortium's shared commitment to delivering a robust cybersecurity framework for the protection of critical infrastructures.



CyberSecDome at 21st ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS 2026) in Bangalore, India, June 2026

From 1 to 05 June 2026, CyberSecDome was represented at the 21st ACM ASIA Conference on Computer and Communications Security in Bangalore, India. Michael Kühr from the Technical University of Munich (TUM) presented the paper “SoK: Security of the Image Processing Pipeline for Camera-based Sensing in Autonomous Vehicles” which acknowledged CyberSecDome. The work focused on the security challenges of camera-based sensing in autonomous vehicles and received a Distinguished Paper Award at the main conference.



CyberSecDome at The American College of Greece in Athens, June 2026

On 10 June 2026, AIA organised a CyberSecDome dissemination event at The American College of Greece in Athens, dedicated to advanced cybersecurity solutions for critical infrastructures. The event presented the project's core framework through real-world applications, featuring mission and infrastructure overviews from Athens International Airport (AIA), as well as attack scenarios presented by OTE.

Students and faculty had the opportunity to explore simulated attack scenarios, examine how specialised cybersecurity tools can support the protection of vital networks, and experience a live VR/AR demonstration of the CyberSecDome technology in action. The event concluded with an open Q&A session, encouraging discussion on the role of AI, immersive technologies and operational validation in strengthening cyber resilience.



CyberSecDome at Vivatech Fair in Paris, France, June 2026

On 18 June 2026, CyberSecDome was presented at the VivaTech Fair in Paris by Marc-Oliver Pahl from IMT Atlantique and Mohammad Hamad from TUM, through the Cyber CNI Chair's participation at the German-French Academy for the Industry of the Future booth. The activity highlighted CyberSecDome's contribution to AI-supported cybersecurity, situational awareness and the protection of critical infrastructures, while strengthening the project's visibility within the European innovation ecosystem.





Internal Pilots: Final Validation Results

The CyberSecDome internal pilots evaluated the integrated platform in controlled environments representing two critical infrastructure domains: **aviation**, through Athens International Airport (AIA), and **telecommunications**, through OTE. They assessed technical performance, interoperability, incident detection and response, while identifying priorities for further development.

Athens International Airport (AIA) Internal Pilot

The **AIA (Athens International Airport)** pilot, part of the CyberSecDome project, successfully implemented and validated four specific attack scenarios within the **CyberRange environment** to test the security and resilience of the airport's Unified Communication Network.

Pilot Objectives & Scenarios

The pilot focused on enhancing SOC capabilities in monitoring AIA's Unified Communication Network infrastructure, minimizing cascading risks, and strengthening threat information sharing. The validation process successfully executed the following scenarios:

- **Scenario #1:** Network/Port Scanning and Network-based DDoS.
- **Scenario #2:** Attack on the SIP protocol causing a distributed denial-of-service.
- **Scenario #3:** Phishing and Reverse TCP attack delivered via malicious email.
- **Scenario #4:** Brute Force Attack on critical servers/workstations.

Key Validation Outcomes

The validation provided critical insights for technical refinement and system optimization:

- **System Integration Baseline:** The pilot successfully established the stability of the CyberRange infrastructure and validated cross-component APIs, ensuring seamless data flow between tools such as the IDPS (Intrusion Detection and Prediction System) and the VR Interface.
- **Technical Feedback Loops:** Successful mapping of attack stories confirmed the technical feedback path from the VR Interface to the IDPS, validating that alerts and data could be accurately processed and visualised.

- **ML & Data Refinement:** The pilot identified discrepancies between synthetic and real-world datasets, allowing for the recalibration of machine learning algorithms (IPS, DAIR, and Swarm Learning) to better handle high-entropy data.
- **Incident Investigation Capability:** The use of tools such as the FVT (Forensics Visualization Toolkit) and XAI (Explainable AI) successfully demonstrated the ability to cluster anomalies, identify alert families, and provide actionable insights, such as grouping data in Scenario #3 or processing alert statistics for SIP attacks.
- **KPI Alignment:** The pilot served as a diagnostic phase to validate progress towards project KPIs, including metrics on real-time anomaly identification and response coordination, providing a controlled baseline for full-scale validation.

Taken together, the AIA pilot established a stable integration and validation baseline for evaluating CyberSecDome in a critical aviation context. By exercising the platform against four representative attack scenarios, it demonstrated how AI-supported analysis, incident investigation and VR-based visualisation can support the monitoring and protection of airport communication services. The findings also highlighted priorities for continued maturation, particularly performance optimisation, calibration with representative operational data, scalable knowledge sharing and impact assessment. They therefore provide a practical basis for the potential future application of the CyberSecDome approach in airport and other critical-infrastructure environments.

OTE Internal Pilot

The **OTE pilot** completed its second and final evaluation cycle, validating the full CyberSecDome platform against realistic attack conditions in a dedicated laboratory environment replicating a telecom operator's monitored infrastructure.

Building on the first evaluation round, the final cycle expanded to two complete attack scenarios: a **Denial-of-Service (DoS/DDoS) campaign** combining application-layer and network-layer flooding, and an **end-to-end ransomware attack simulation** covering the full attack lifecycle, from phishing-based delivery and payload execution through file encryption, detection and automated response. Together, the scenarios exercised all four CyberSecDome workflows and generated a rich dataset of legitimate and malicious traffic used to validate the platform's detection and monitoring chain.

The results confirmed strong performance against the pilot's key performance indicators. **Incident detection time was reduced from 31–60 minutes to 5–15 minutes**, a reduction of roughly **70%**, far exceeding the 25% target, while **incident downtime dropped below one hour**, compared to a baseline of 1–4 hours. Automated response actions were triggered within seconds of detection, and the **Automated Penetration Testing module delivered a 50–75% improvement in vulnerability discovery efficiency**.

The platform was validated across **19 evaluation criteria**, with the large majority fully confirmed. Remaining refinements, such as fine-tuning incident severity classification and improving VR navigation on large infrastructures, feed directly into the platform's final optimization.

For OTE, the pilot demonstrated that CyberSecDome's integrated approach, combining **AI-driven detection, dynamic risk analysis, automated response and immersive VR-based situational awareness**, can measurably strengthen the detection and response capabilities of a modern Security Operations Centre.



Open Call Results: From External Experiments to Real-World Validation

CyberSecDome's Open Call programme was designed to bring external organisations into the project and to test its tools against use cases, infrastructures and threats beyond those covered by the consortium's internal pilots. Across two rounds, 15 third-party projects were funded, providing the consortium with additional technical evidence and practical feedback from sectors including healthcare, finance, manufacturing, smart cities, public services and automotive logistics.

Interest from the wider cybersecurity community was strong. The first Open Call received 107 applications; 55 were completed, and 39 were found eligible. Nine projects were selected and completed their activities. The second round attracted 79 applications, of which 67 passed the eligibility checks. Six projects were funded: CASPER, AUTODOME, FINCARE, PRINIA-CSD, DRACOS and SECURE-CLAIM.

The two rounds served distinct yet complementary purposes. Round 1 enabled external teams to develop and test solutions addressing different aspects of the CyberSecDome concept. Round 2 focused on deploying and validating the integrated framework within complete use cases. Experience from the first round also helped strengthen the monitoring arrangements for the second. Each OCR2 project worked with an assigned mentor and followed a structured process covering onboarding, deployment planning, technical milestones, deliverables, demonstrations, validation questionnaires and evidence collection.

Final results from Open Call Round 2

The six Open Call Round 2 projects concluded their implementation activities on 31 July 2026 and presented their work in dedicated final reviews. These reviews examined the status of the planned use cases, integration with CyberSecDome components, achievement of project-specific KPIs, technical evidence, deliverables, and remaining limitations.

SECURE-CLAIM tested CyberSecDome in an anonymised insurance-claims environment. Its scenarios covered ransomware, volumetric denial-of-service attacks, coordinated fraudulent-claim submissions, and progressive poisoning of an AI model. The project demonstrated an operational chain spanning several CyberSecDome tools. Its preliminary comparison with selected baselines showed promising detection results, although data poisoning remained the most challenging scenario.

CASPER applied the framework to the protection of smart-city parking infrastructure. Its work generated baseline and attack network traffic, structured JSON results, and supporting technical documentation. These outputs informed the assessment of security and resilience in a connected urban environment and provided evidence for the use of CyberSecDome components in a setting with distributed physical and digital assets.

DRACOS examined cybersecurity risks affecting drone-based systems. The project produced network-traffic evidence and a structured asset inventory for the Dynamic Risk Assessment process. Its work helped test how information on drone assets, communication flows and detected indicators could be processed within the wider CyberSecDome framework.

PRINIA-CSD focused on privacy-preserving biometric authentication. The project tested six attack scenarios through the IDS and IPS components and produced an extended-reality attack dataset, an evaluation dataset and two open-access scientific publications. The use case also highlighted the need to handle security evidence and personal data under clearly separated access and protection arrangements.

FINCARE explored the use of CyberSecDome's AI, risk-analysis and visualisation capabilities in a financial-sector setting. Its outputs included a risk-assessment asset list, visualisation schemas, network-traffic and JSON datasets, testbed configurations and supporting scripts. The final evaluation also identified areas requiring further attention, including technical testing, user validation and the documentation of evidence.

AUTODOME deployed the framework in an automotive logistics and Industry 4.0 environment. Penetration testing identified seven critical vulnerabilities affecting the robot infrastructure, while preliminary IPS results successfully detected the evaluated attack scenarios. The pilot also tested the Dynamic Risk Assessment, visualisation and advanced persistent threat analysis functions. At the same time, it revealed practical integration issues, including timestamp precision, reporting scripts and dependencies between the test environment and individual components.

Taken together, the six projects reported 55 datasets and technical results for inclusion in the project's final data inventory. These included PCAP files, logs, indicators, asset lists, reports, configuration files, scripts, visualisation schemas and publications. Five records are openly available, while most remain under restricted or controlled access due to security-sensitive content. This is an expected outcome for work involving attack traffic, infrastructure details and evidence of vulnerabilities.

Assessment of the Open Call programme

All nine Round 1 projects completed their activities. The final assessment linked project completion to documented evidence, deliverables and achieved results, with financial adjustments applied where the reported level of completion was not fully substantiated. This was an important part of the programme's governance: funding decisions were tied to documented work, deliverables and results rather than participation alone.

The same evidence-based approach was followed for OCR2, where assessments considered the approved proposals, deliverables, KPI evidence, demonstrations, validation results and mentor feedback. Where an activity was incomplete or could not be independently verified, it was recorded in the assessment rather than treated as completed by default.

The Open Calls expanded CyberSecDome's validation base and tested the framework against environments that would have been difficult to cover through the consortium pilots alone. They provided a realistic view of the work required to deploy an integrated cybersecurity platform. Access to suitable test environments, availability of representative data, interoperability between tools, and timely production of evidence were recurring challenges.

These findings are as relevant as the successful demonstrations. They show where the framework performed well, where further integration and automation are needed, and what future adopters will require in terms of

documentation, technical support and deployment planning. In this respect, the Open Call programme did more than fund a set of external experiments: it provided a rigorous external validation of CyberSecDome's technologies across varied operational conditions.

PUBLICATIONS – JOURNAL & CONFERENCE PAPERS & ARTICLES

By the end of the project (M36), CyberSecDome actively disseminated its scientific and technical results through international journals and conferences. Overall, the project produced **17 journal publications** (14 publications in international referred journals and 3 special issues) and **29 conference papers**, of which 27 were published and 2 accepted. These outputs covered key CyberSecDome research areas, including AI-supported cybersecurity, intrusion detection and response, digital twins, explainable AI, cyber-physical systems, autonomous systems and critical infrastructure protection.

CyberSecDome also communicated its technical results and validation experience to the wider professional cybersecurity community through **six articles prepared for CyberSecurity Magazine**, covering the overall platform, the two internal pilots and three Open Call Round 2 use cases.

“Keeping Airport Communications Resilient: Cybersecurity Validation Lessons from Critical Aviation Infrastructure”

AIA internal pilot – Airport communication resilience, critical infrastructure protection and validation lessons.

“Strengthening Cyber Resilience in Smart City Infrastructures: Practical Lessons from a Real-World Smart Parking Validation Pilot”

CASPER – Open Call Round 2 – Smart-city cybersecurity, smart-parking validation and operational resilience.

“Testing Cybersecurity in Realistic Conditions: Lessons from AutoDome”

AUTODOME – Open Call Round 2 – IT/OT security, automotive manufacturing and realistic validation.

“Beyond Detection: Strengthening Cyber Resilience through AI-Driven Investigation, Response and Collaboration”

Project-level article – Overall CyberSecDome platform, AI-driven investigation, response, collaboration and cyber resilience.

“Testing DDoS Resilience Before Deployment: Cybersecurity Validation Lessons from Telecommunications”

OTE internal pilot – DDoS resilience, telecommunications validation and service continuity.

“Testing Cybersecurity in Realistic Conditions: Lessons from AI-Assisted Drone Patrolling”

DRACOS – Open Call Round 2 – Drone-assisted patrolling, cyber-physical security and evidence-based validation.

Explore the complete collection of **CyberSecDome** publications is available through the [CyberSecDome website](#) and the project's [Zenodo](#) Community.

DISSEMINATION MATERIAL & PUBLICLY AVAILABLE RESOURCES

Throughout the project, CyberSecDome maintained a broad dissemination and communication presence to support the visibility of its activities, technical developments, pilots, Open Calls and final results. This was achieved through participation in events, scientific and professional publications, newsletters, digital communication, audio-visual content and dedicated dissemination actions targeting scientific, industrial and wider stakeholder communities.

A wide range of CyberSecDome outputs is publicly available through the project's main online channels. The [CyberSecDome website](#) serves as the central access point for project news, events, publications, newsletters, press releases and downloadable communication material, while the [Zenodo Community](#) provides open access to scientific publications, public deliverables and other research outputs.

The project's [YouTube channel](#) complements these resources with the CyberSecDome promotional video, webinar and Open Call recordings, podcast content, and the series of short videos presenting the Open Call-funded projects. Together with the project's brochures, flyers, posters and other supporting material, these resources provide a lasting record of CyberSecDome's work and ensure that its public results remain accessible to interested stakeholders beyond the formal end of the project.

Explore CyberSecDome

[Website](#) – project news, activities, publications, newsletters and downloadable material

[Zenodo Community](#) – scientific publications, public deliverables and research outputs

[YouTube Channel](#) – project videos, webinars, Open Call recordings and funded-project videos

Three Years of CyberSecDome: Overall Outcomes and Final Words

Over 36 months, **15 organizations** from **10 countries** worked together to develop and integrate the CyberSecDome framework. The project combined digital twins and CyberRange environments, AI-enabled security tools, automated penetration testing, dynamic risk analysis, privacy-aware information and knowledge sharing, and an immersive VR interface. Its common objective was to strengthen preparedness, situational awareness and coordinated incident response across complex digital infrastructures.

Validation was central to this work. The internal pilots at Athens International Airport and OTE assessed CyberSecDome in the aviation and telecommunications domains, while 15 third-party projects supported through two Open Call rounds extended the evaluation to a wider range of sectors, infrastructures and threat scenarios. These activities generated practical evidence on component interoperability, anomaly detection, incident investigation, risk analysis and visualisation. They also identified areas requiring continued attention, including access to representative data, integration across heterogeneous tools, scalability, deployment support and the documentation of technical evidence.

Alongside its technical work, CyberSecDome established a strong basis for continued research and uptake through scientific and professional publications, datasets and technical results, events, collaboration activities and publicly accessible resources. Engagement with external innovators, sister projects and other stakeholders broadened the exchange of knowledge beyond the consortium and helped assess the project's technologies in different operational contexts.

As CyberSecDome reached its formal conclusion, its legacy is an integrated and broadly evaluated foundation, together with practical lessons for developing more collaborative, explainable and operationally relevant cybersecurity solutions.

The consortium thanks all partners, pilot organizations, Open Call beneficiaries, advisers, reviewers and stakeholders who contributed throughout the project. Their combined effort shaped CyberSecDome's results and provides a basis for their continued refinement, dissemination and potential uptake beyond the funded period.

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 organizations: 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