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 8

March (M31) – May (M33)

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 operation 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 visualisations 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 national and European level.
- Provide high levels of cybersecurity through policies and AI-based methods for proactive and real-time management of all security issues.
- Provide better interfaces between humans and cybersecurity algorithms.
- Develop solutions to automate penetration testing for proactive security using data-driven AI.
- Achieve pilot-driven prototypes of CyberSecDome security services ready for FSTP deployment and validation.

CyberSecDome's Pilots

Hellenic Telecommunications Organisation

OTE, a leading telecommunications provider, operates a comprehensive digital infrastructure, including a Security Operations Center (SOC). CyberSecDome intends to improve OTE's incident response and cybersecurity awareness capacity by testing scenarios such as ransomware, malware, and DDoS attacks, focusing on reducing detection time and downtime, and improving incident monitoring and mitigation.

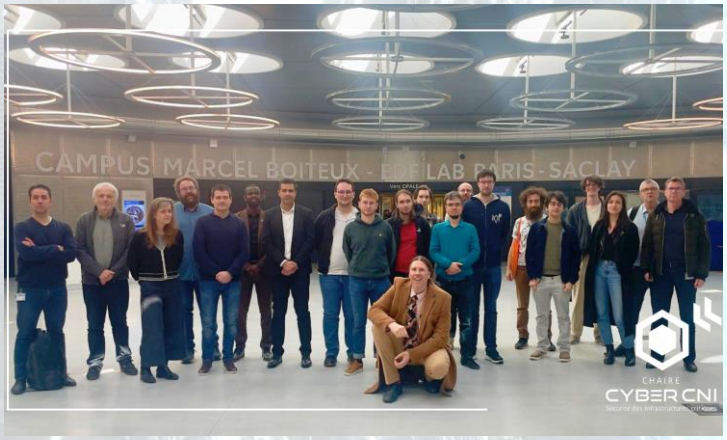
Athens International Airport

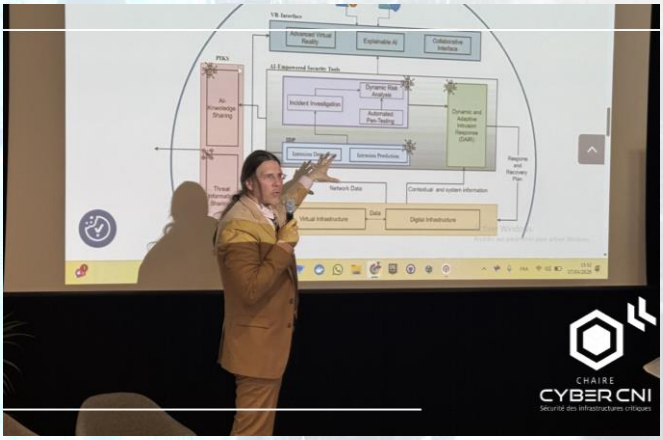
AIA, the primary infrastructure provider for Athens International Airport, supports airlines, handlers, stores, employees, and associated entities. AIA operates a Security Operations Center (SOC) to face cybersecurity risks, enhance risk detection, and mitigate threats. CyberSecDome will improve AIA's ability to counter targeted attacks on call center infrastructure and disruptions vital communication services.

MEETINGS & EVENTS

CyberSecDome at the Cyber CNI Research Update in Paris, April 2026

On 7 April 2026, CyberSecDome was presented at the Cyber CNI Research Update Spring 2026, held at EDF Labs in Paris, France. The event brought together academic and industrial partners to discuss recent research developments in cybersecurity for critical infrastructures. CyberSecDome was featured in discussions related to incident response, digital twins, threat intelligence and XR-based interfaces, highlighting its contribution to cybersecurity management, visualisation and situational awareness. The event offered a valuable opportunity to connect the project with the wider Cyber CNI ecosystem and reinforce its relevance for the resilience of critical digital infrastructures.





CyberSecDome 2nd Cluster Synergies Webinar, April 2026

On 22 April 2026, CyberSecDome organised the 2nd Cluster Synergies Webinar, bringing together several EU-funded cybersecurity projects to exchange knowledge and strengthen cooperation across the cybersecurity research landscape. The session provided space for participating projects to present their progress, key milestones, technical developments and emerging results, while also identifying opportunities for future collaboration. The webinar further reinforced CyberSecDome's role in supporting cross-project synergies and knowledge sharing within the European cybersecurity ecosystem.

CyberSecDome at the 1st AIMLOps Workshop at IEEE/IFIP NOMS Symposium in Rome, May 2026

On 18 May 2026, CyberSecDome co-organised the 1st IEEE/IFIP International Workshop on AI-driven Management and ML Ops for Networks and Services (AIMLOps), which took place in Rome in the context of the IEEE/IFIP NOMS 2026 Symposium. The workshop focused on the growing role of AI and MLOps in the management of networks and services, with discussions covering AI-supported cybersecurity, anomaly detection, generative AI, autonomous network operations and related research challenges. CyberSecDome's contribution to the organisation of the workshop helped strengthen links with the research community and promoted exchange on intelligent, resilient and self-adaptive cybersecurity solutions.

CyberSecDome at the "Management of Complex Threats" workshop at IEEE/IFIP NOMS 2026 in Rome, May 2026

On 22 May 2026, the Management of Complex Threats workshop took place at IEEE/IFIP NOMS 2026 in Rome, bringing together researchers and practitioners to explore the future of AI-driven cybersecurity. The workshop addressed emerging challenges in managing complex threats across critical infrastructures, covering topics such as AI-based anomaly detection, LLM security, autonomous penetration testing, and cyber-physical attacks. A key takeaway was that AI is becoming both the attack surface and the defence mechanism, requiring new approaches to resilience and operational security. The workshop was co-organised by CyberSecDome, highlighting the project's contribution to advancing research and innovation in this field.

CyberSecDome at the final event of the New Master Cybersecurity Program at IMT in Rennes, May 2026

On 27 May 2026, CyberSecDome co-organised the final session of the new Master Cybersecurity Program at IMT Atlantique in Rennes, marking the completion of an engaging learning journey on securing critical infrastructures. The session covered key topics such as OT/IT security, industrial systems, cyber resilience, anomaly detection and human-centred cybersecurity, highlighting both technical and operational challenges. It also featured insights into next-generation cybersecurity approaches, including immersive interfaces and advanced SOC environments developed in the context of CyberSecDome. The event underlined the importance of education and knowledge transfer in preparing the next generation of cybersecurity professionals.

CyberSecDome XR Cybersecurity Demo at IRISA laboratory in Rennes, May 2026

On 27 May 2026, CyberSecDome co-organised an XR cybersecurity demonstration at the CNRS UMR IRISA laboratory in Rennes, during the visit of Les Jeunes IHEDN. The session presented how AI and XR technologies can support cyber experts through improved situational awareness, clearer incident visualisation and reduced cognitive load. Following an introduction to the CyberSecDome concept and architecture, participants experienced a live demonstration of the immersive platform and discussed its relevance for operational cybersecurity and critical infrastructure protection.

CyberSecDome Open Call Round 1 Results

CyberSecDome successfully completed the first round of its Open Call activities, bringing together **nine funded third-party projects to validate and enhance the project's cybersecurity framework** across a wide range of practical environments. The projects contributed to the testing and assessment of key CyberSecDome capabilities, including Dynamic Risk Analysis, Intrusion Detection and Prediction, Incident Investigation, Dynamic and Adaptive Incident Response, Automated Penetration Testing, and dataset generation for AI-supported cybersecurity.

Overall, Open Call Round 1 demonstrated the value of engaging external innovators in validating CyberSecDome. The funded projects addressed diverse use cases, ranging from **smart homes and Industry 4.0 to fintech platforms, fact-checking services, smart elevators, IoT infrastructures and cyber range environments**. Their work generated useful datasets, technical evidence, validation feedback and operational insights that will support the further refinement of the CyberSecDome platform and its future pilot activities.

Project-level highlights

CASeR-Safe focused on the cyber resilience of smart-home environments, exploring how CyberSecDome capabilities can support vulnerability identification, risk assessment, penetration-testing readiness and intrusion detection in IoT-based domestic settings. The project provided useful feedback on the practical needs of smart-home validation, including asset modelling, vulnerability visualisation and secure access to distributed environments.

DomeSentinel developed high-fidelity cyber range scenarios covering both enterprise IT and smart-home IoT environments. The project generated realistic, attack-labelled datasets, asset inventories and supporting evidence for use by CyberSecDome partners in further testing, benchmarking and detection-rule development. It also enabled visualisation of cyber assets and security alerts via the CyberSecDome VR interface.

ACRYS validated CyberSecDome's Dynamic Risk Analysis capabilities in a fintech cloud environment. The project used assets, vulnerability and process-related information to assess how dynamic risk visibility can support operational decision-making and governance. Its outcomes provided valuable feedback on risk visualisation, vulnerability mapping, usability and the use of risk assessment results in compliance-oriented contexts.

ATTENTO tested Dynamic Risk Analysis in a simulated Industry 4.0 environment, using a realistic digital twin of a smart factory with industrial assets, services and dependencies. The project assessed how CyberSecDome can

support asset registration, vulnerability association, CVSS-based risk refinement and industrial risk modelling, and identified useful requirements for future improvements to data ingestion and risk propagation.

SCAF-DOME applied CyberSecDome tools in the context of digital media and fact-checking services, using a replicated cloud-native environment inspired by Truly Media and EDMO services. The project executed realistic security scenarios involving availability stress, reconnaissance, authentication abuse, malware-like behaviour, and database exploitation, providing valuable evidence for monitoring, alerting, and incident analysis in Kubernetes-based environments.

ELEVATE explored cybersecurity for smart, IoT-enabled elevator ecosystems. Using a controlled testbed, the project generated datasets and evidence across several threat scenarios, including brute-force authentication, malware installation, firmware/service-tool abuse, denial-of-service and SQL injection. Its work contributed to CyberSecDome's validation in IoT-heavy environments where safety, availability and operational continuity are critical.

ADAPT focused on AI-driven automated penetration testing in a real-world fintech/cloud environment. The project tested CyberSecDome's automated penetration-testing capabilities across API, authentication, authorization and business-logic scenarios, while also supporting the extension of testing approaches to cloud-hosted environments. Its results provided useful feedback on cloud-readiness, safe testing procedures and operator-facing usability.

CATT46 validated automated penetration testing in an IoT and web/API environment. The project supported testing across the website, network, host-level and backend application layers, helping identify configuration weaknesses and improve the practical validation of CyberSecDome's automated penetration-testing capabilities. The work also highlighted the importance of secure isolation, contextual information, and clear reporting for actionable penetration testing results.

SHIELD contributed high-quality, GDPR-compliant labelled PCAP datasets to support the training and validation of AI-driven intrusion detection and prevention capabilities. The project generated representative traffic datasets covering benign and attack conditions, including port scanning, DDoS, ICMP flooding and baseline activity. These datasets provide valuable material for improving and evaluating CyberSecDome's AI-supported detection capabilities.

The completion of Open Call Round 1 provided CyberSecDome with important validation evidence from external stakeholders and practical use cases. The results confirmed the relevance of the project's approach across heterogeneous cybersecurity contexts and generated lessons that will support the next phase of technical refinement, pilot execution and Open Call activities.

CyberSecDome Open Call Round 2 Projects in Focus

With onboarding completed and implementation already underway, the six Open Call Round 2 projects are now advancing their validation activities within the CyberSecDome ecosystem.

From smart-city parking and healthcare insurance to drone-assisted critical infrastructure protection, industrial XR, financial services and automotive logistics, the Round 2 projects bring CyberSecDome into a broad range of practical environments. Each use case offers a different perspective on how the platform can support cybersecurity operations, address sector-specific challenges and respond to realistic threat scenarios.

Through their work, the projects are helping CyberSecDome gather valuable technical feedback, validation evidence and operational insights on key capabilities such as threat detection, dynamic risk assessment, incident investigation, situational awareness and response.

Below, the six funded projects are introduced through their validation focus, practical use cases and expected contributions to the CyberSecDome ecosystem.

CASPER – Collaborative Assessment of Security for Smart City Parking Enhanced Resilience

Coordinator: DOTSOFT (Greece)

Participating organisation(s): PRVACT P.C (Greece)

Domain: Smart Parking System

Key use case: The protection of the INTEL ANN smart parking service by deploying CyberSecDome to detect threats, assess risks, investigate incidents, and provide real-time cybersecurity situational awareness through a VR-based interface.

Description of work: CASPER aims to identify, assess, and manage security risks and incidents within the INTEL ANN smart parking service in a controlled environment. The project focuses on protecting the data flows between network components, applications, and services. This will be achieved through the deployment and validation of the integrated CyberSecDome prototype. The prototype supports threat detection, dynamic risk assessment, incident investigation, and situational awareness. An immersive VR interface will also be used to improve the understanding of threats, risks, and incidents, helping operators respond more proactively and maintain the reliability and continuity of smart-city parking services.

Main expected results:

- AI-assisted threat detection, dynamic risk assessment, and real-time incident investigation.
- Secure data flows between applications, supporting service resilience, reliability and continuity.
- Enhanced response and awareness, including VR-based visualisation of threats, risks, and incidents.

Contact: info@dotsoft.gr

SecureClaim - Cybersecure Claim Management in Co-Assess

Coordinator: Covariance (Greece)

Participating organisation(s): N/A

Domain: Healthcare Insurance / InsurTech / Cybersecurity

Key use case: Ransomware attack: A compromised healthcare partner silently delivers ransomware into Co-Assess via a trusted API connection, encrypting critical claims databases and halting operations. CyberSecDome detects the anomalous traffic, isolates the threat, and automates recovery before irreversible damage occurs.

Description of work: SecureClaim applies the CyberSecDome tools to Co-Assess, a commercial AI-driven platform for fraud detection and claims management in healthcare insurance. Operating across the multi-stakeholder PHIdelity ecosystem, which connects insurers, Third-Party Administrator (TPAs), patients, doctors, and healthcare providers, the project integrates AI-enhanced threat detection (TDE), automated incident response (IMS), collaborative threat intelligence sharing (CISM), dynamic risk assessment (DRA), and VR-enhanced situational awareness. Validation is performed through four realistic attack scenarios: (i) ransomware deployment via a compromised TPA endpoint, (ii) volumetric DoS against claim APIs, (iii) a coordinated fraud ring campaign, and (iv) progressive AI model data poisoning. All activities use exclusively anonymised data, in full compliance with GDPR, NIS2, and DORA.

Main expected results:

- ≥20% improvement in anomaly detection accuracy across four attack scenarios
- ≥30% reduction in Mean Time to Detect and Respond to cyber incidents
- Validated GDPR-, NIS2-, and DORA-compliant cybersecurity framework for EU InsurTech platforms

Contact: info@covariance.gr

DRACOS - DRone security with Ai CybersecdOme Security framework

Coordinator: TERRACOM S.A (Greece)

Participating organisation(s): HOVERAP L.P (Greece)

Domain: Critical infrastructure protection, physical security, drone-assisted patrolling and cybersecurity for cyber-physical systems.

Key use case: Secure drone-assisted patrolling for critical infrastructure, where live aerial monitoring, AI-based object recognition and guard route support are assessed together with CyberSecDome tools for cybersecurity risk assessment, threat detection and incident response.

Description of work: DRACOS validates CyberSecDome tools in the context of an AI-assisted drone patrolling service for critical infrastructure protection. The pilot combines TERRACOM's QR-Patrol guard monitoring

platform with HOVERAP's drone patrolling service, where live drone video streams are processed through AI-based object recognition and made available to security operators. Within CyberSecDome, DRACOS provides a realistic cyber-physical environment for assessing risk, detecting cyber threats, supporting incident investigation and improving situational awareness. The project generates asset information, operational data and controlled cybersecurity scenarios to help evaluate how CyberSecDome tools can support secure drone-based patrolling operations.

Main expected results:

- Validation evidence for CyberSecDome tools in drone-assisted patrolling.
- Improved understanding of cyber risks affecting live drone security operations.
- Practical feedback for refining CyberSecDome in critical infrastructure use cases.

Contact: info@terracom.gr

PRINIA-CSD - Privacy-pReservINg biometric Authentication to validate CyberSecDome

Coordinator: Human Opsis (Greece)

Participating organisation(s): Algolysis (Cyprus)

Domain: Privacy-preserving technologies in Extended Reality

Key use case: Secure access control for industrial XR training and digital environments using privacy-preserving biometric authentication.

Description of work: PRINIA-CSD supports the validation of the CyberSecDome cybersecurity platform in industrial Extended Reality (XR) environments. The project combines privacy-preserving biometric authentication with secure XR access control, ensuring that only authorised users can interact with sensitive training systems, industrial simulations, and digital workflows. Through realistic industrial scenarios, PRINIA-CSD evaluates how CyberSecDome technologies can improve security, resilience, and trust in immersive environments. The project also explores how privacy-aware cybersecurity solutions can support safer and more reliable XR applications for manufacturing and Industrial IoT, contributing to the broader adoption of secure and human-centred digital technologies across Europe.

Main expected results:

- Validation of CyberSecDome in industrial XR scenarios
- Secure and privacy-aware biometric authentication workflows
- Improved resilience and trust in XR industrial applications

Contact: hello@humanopsis.com

FINCARE - Financial Services Cross-silo AI-enabled Cyber Resilience

Coordinator: Mind the Hack (Greece)

Participating organisation(s): Grant Thornton - AI Centre of Excellence (Greece)

Domain: Financial and Consulting Services

Key use case: Protecting continuity of financial and consulting services against advanced network-based attacks such as credential-based attacks, covert exfiltration, and lateral movement; aligning with the platform's mission

to validate resilience against sophisticated threats, while ensuring interoperability and usability.

Description of work: The finance and professional services sector faces escalating risk due to the criticality of IT in protecting client data, making firms prime targets for cyber-attacks. The disclosure or loss of such data can have systemic financial consequences and erode trust, significantly affecting business capacity. Responding to this challenge, FINCARE validates the CyberSecDome platform in this high-risk domain; leveraging its AI-enhanced threat detection, VR-based situational awareness, dynamic risk assessment and collaborative threat intelligence modules. The pilot involves conducting a series of red/blue team exercises in a simulation testbed, created to represent a target enterprise. Mind the Hack simulates advanced adversarial attacks, while Grant Thornton utilises CyberSecDome to detect, respond to and investigate the threats. To ensure scalability, the pilot supports three environments; Greece, Germany and Cyprus, enabling privacy-preserving collaborative intelligence across jurisdictions.

Main expected results:

- Realistic enterprise-grade simulation environments providing scalable, interoperable testbeds for traffic generation and penetration testing.
- Traffic Dataset containing real and synthetic information, enriched with standardized annotations for reproducible testing.
- Solution Development Roadmap detailing a technical and business development strategy, including a market analysis.

Contact: ContactUs@gr.gt.com

AutoDome - Experimentation with CyberSecDome in Automotive Logistics Environments

Coordinator: Binarial (Spain)

Participating organisation(s): Centro Tecnológico de Automoción de Galicia (CTAG) (Spain)

Domain: Industrial cybersecurity in manufacturing and automotive logistics (IT/OT systems)

Key use case: AutoDome tests cybersecurity detection and response in a simulated automotive logistics environment, including scenarios where cyberattacks may affect Autonomous Mobile Robots (AMRs), industrial communications or logistics missions.

Description of work: AutoDome addresses an increasingly important challenge: how can connected factories stay protected as automation grows? The project tests CyberSecDome in an automotive manufacturing scenario, using CTAG's Booster Manufacturing Lab to recreate automated logistics operations in a safe and realistic way. The scenario includes Autonomous Mobile Robots (AMRs) and factory systems working together, similar to what can be found in modern industrial plants. By bringing CyberSecDome into this environment, AutoDome helps understand how the platform can support safer, more reliable and resilient manufacturing operations, while providing useful feedback from a real industrial perspective.

Main expected results:

- Practical validation of CyberSecDome in an automotive manufacturing environment.
- Better understanding of how cyber threats can affect connected logistics systems and AMRs.
- Feedback to improve the platform's detection, response, usability and integration capabilities.

Contact: Jorge Pérez-Roget Blanco; AutoDome Project contact at Binarial; jorge.perez-roget@binarial.es

DISSEMINATION MATERIAL

During this period, CyberSecDome dissemination material continued to support the project's visibility across conferences, workshops, webinars, educational activities and live demonstration events. Project brochures, roll-up banners, posters and digital material were used to present CyberSecDome's concept, technical approach, pilots, Open Call activities and validation progress in a consistent and accessible way.

In parallel, the project's online dissemination channels continued to serve as a central point of access to CyberSecDome outputs. All public dissemination resources remained available through the CyberSecDome website and the project's Zenodo community, while recordings, webinars and videos shared through the project's YouTube channel enabled stakeholders to engage with CyberSecDome content on demand. Together, these digital resources extended the project's reach beyond physical events and supported continued communication with research, industry and cybersecurity communities.

PUBLICATIONS – JOURNAL & CONFERENCE PAPERS

CyberSecDome partners continued to actively disseminate scientific results through a strong publication record, with **13 conference/workshop papers** and **6 journal papers** reported in this issue. The list of published and accepted articles is shown below:

Conference/Workshop Papers

"Pouvez-vous détecter le piège? Détection de pots de miel face à l'évolution des tactiques d'évasion",
M. Durand, A. Dey, Y. Kermarrec & M.O. Pahl,
32nd Computer & Electronics Security Application Rendezvous (C&ESAR 2025), 19-20/11/2025, Published on 12/12/2025

"L'Apprentissage Machine au Sein des Jumeaux Numériques pour l'Estimation et la Détection des Menaces",
H. Bourreau, M.O. Pahl, F. Dagnat & F. Jaafar,
32nd Computer & Electronics Security Application Rendezvous (C&ESAR 2025), 19-20/11/2025, Published on 12/12/2025

"Real-time Instruction-Level Anomaly Detection for Embedded Applications using AI",
M. Mezaouli, Y. Nasser, S. Saoudi & M.O. Pahl,
IEEE/IFIP Workshop on Management of Complex Threats (MCT), 22/05/2026, Published on 09/03/2026

"Closing the Loop in Embedded Security: Evolution of an AIOps Framework for Threat Hunting",
M. Mezaouli, Y. Nasser, S. Saoudi & M.O. Pahl,
1st IEEE/IFIP International Workshop on AI-driven Management and ML Ops, 18/05/2026, Published on 09/03/2026

"Revealing Embedded System Behaviors: A Comparative Analysis of Power Consumption and Hardware Performance Counters",

M. Mezaouli, Y. Nasser, S. Saoudi & M.O. Pahl,
1st Workshop on Hardware-Supported Software Security, 25/09/2025, Published on 01/04/2026

“Origin Lens: Reclaiming Trust on the AI-Mediated Web Through On-Device Image Provenance Verification”,
A. Loth, D. C. Rosario, P. Ebinger, M. Kappes & M.O. Pahl,
18th ACM Web Science Conference 2026, 26-29/05/2026, Published on 25/05/2026

“The Verification Crisis: Expert Perceptions of GenAI Disinformation and the Case for Reproducible Provenance”,
A. Loth, M. Kappes & M.O. Pahl,
ACM Web Conference 2026, 03/07-29/06/2026, Published on 28/05/2026

“Eroding the Truth-Default: A Causal Analysis of Human Susceptibility to Foundation Model Hallucinations and Disinformation in the Wild”,
A. Loth, M. Kappes & M.O. Pahl,
ACM Web Conference 2026, 03/07-29/06/2026, Published on 28/05/2026

“Industrialized Deception: The Collateral Effects of LLM-Generated Misinformation on Digital Ecosystems”,
A. Loth, M. Kappes & M.O. Pahl,
ACM Web Conference 2026, 03/07-29/06/2026, Published on 28/05/2026

“An empirical study of privacy-utility trade-offs in gaze-based authentication for extended reality”,
Raptis, G. E., Chrysopoulou, E., & Katsini, C.,
2026 Symposium on Eye Tracking Research and Applications (ETRA ’26), 01-04/06/2026, Published on 31/05/2026

“SoK: Security of the Image Processing Pipeline for Camera-based Sensing in Autonomous Vehicles”,
Michael Kühr, Mohammad Hamad, Sebastian Steinhorst,
The 21st ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS 2026) – Accepted

“Secure Automotive Ethernet: Implementing and Benchmarking MACsec, IPsec, and TLS”,
Lukas Eugster, Friedrich Wiemer, Mert D. Pese, Mohammad Hamad, Sebastian Steinhorst,
The 2026 IEEE 103rd Vehicular Technology Conference: VTC2026-Spring – Accepted

“Perspective-Shift Attacks Against Optical Perception Sensors: A Novel Attack Vector on LiDAR and Camera”,
Marco Calipari, Michael Kühr, Dominik Kulmer, Maximilian Luedecke, Mohammad Hamad, Sebastian Steinhorst,
4th USENIX Symposium on Vehicle Security and Privacy – Accepted

Journal Papers

“Large language model-based hybrid framework for automatic vulnerability detection with explainable AI for cybersecurity enhancement”,
Nihala Basheer, Shareeful Islam, Mohammed K. S. Alwaheidi, Haralambos Mouratidis and Spyridon Papastergiou,
Integrated Computer-Aided Engineering, Volume 33, Issue 1, 19/08/2025
https://doi.org/10.1177/10692509251368663

“Decentralized Anomaly Detection Using Deep Feed-Forward Neural Networks”,
C. Lübben & M.O. Pahl,

International Journal of Network Management 35, no. 6 (2025): e70032, 14/11/2025
https://doi.org/10.1002/nem.70032

"Explainable AI based dynamic cybersecurity risk management for cyber insurability",
Spyridon Papastergiou, Nihala Basheer, Kostas Lampropoulos, Panayiotis Verrios & Shareeful Islam,
International Journal of Information Security, Volume 25, article number 36, 22/01/2026
https://doi.org/10.1007/s10207-025-01189-8

"Hybrid AI-Based dynamic risk assessment framework with explainable AI practices for composite product cybersecurity certification",
Shareeful Islam, Bilal Sardar, Eleni Maria Kalogeraki, Kostas Lampropoulos & Spyridon Papastergiou,
International Journal of Information Security, Volume 25, article number 51, 10/02/2026
https://doi.org/10.1007/s10207-026-01218-0

"A responsible AI-driven framework for robust and transparent software vulnerability detection",
Nihala Basheer, Shareeful Islam, Prabhat Kumar, Danish Javeed, Najmul Islam,
Information and Software Technology, Volume 195, 28/03/2026
https://doi.org/10.1016/j.infsof.2026.108126

"Gaze as an implicit second authentication factor when using PIN mechanisms in extended reality",
Chrysopoulou, E., Karlaki, M., Raptis, G. E., & Katsanos, C,
Proceedings of the ACM on Human-Computer Interaction, 10(3), Article ETRA014, Pages 1-17, 28/05/2026
https://doi.org/10.1145/3806028

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