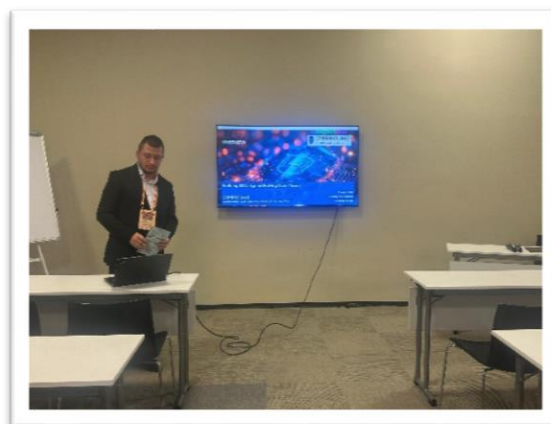


CYBERGUARD REPRESENTATIVES ACTIVELY PARTICIPATED AT COMPLY.LAND EVENT

12th September 2025, Carina Ioana NITA

CYBERGUARD Representatives actively participated at the Comply.Land Event organized on 11-12 September 2025, in St. Julian's, Malta. CYBERFORT Project was presented in the Workshop Session entitled: "Making CRA Compliance Work: Tools and Support for SMEs". The Project objectives are: develop and deploy advanced AI-driven technologies within Security Operation Centers (SOCs) to enhance their capabilities in analyzing, detecting, and preventing cyber threats; establish a secure and efficient Cyber Threat Intelligence (CTI) sharing framework to facilitate collaboration and information exchange amongst stakeholders; enhance the resilience of SOCs against emerging threats; and promote cybersecurity awareness to foster a culture of security within European societies.

The Workshop Session offered valuable insights into the Cyber Resilience Act. During the event, Mr. Daniel NITA – ICT Expert – I-ENERGYLINK, introduced CYBERGUARD, an EU-funded Project. CYBERGUARD aims to make the activities more practical and accessible, especially for SMEs and open-source developers. Mr. Daniel NITA highlighted the main objectives of the project, the main assets, the progress done, and the status of the work accomplished over the past months.



The CYBERGUARD project significantly contributes to reinforcing the digital technology supply chain in the EU through several key initiatives. Enhancing cybersecurity for SMEs is a crucial aspect of this effort. SMEs face significant cybersecurity challenges that can severely impact their operations. CYBERGUARD addresses these challenges by implementing awareness programs to educate SMEs about cybersecurity threats and best practices and offering advanced cybersecurity tools and resources tailored to the needs of SMEs, helping them protect their digital assets more effectively.

Furthermore, seven Use Cases were presented during the Workshop Session as following: Use Case #1: Securing Industrial Control Systems (ICS) from Cyber Threats (Energy Sector); Use Case #2: Securing Patient Data in Healthcare Networks (Healthcare Sector); Use Case #3: Defending Against POS Attacks in the Retail Sector Pilot UC; Use Case #4: Safeguarding Shipping Operations from Cyber Threats (Maritime Sector); Use Case #5: Fraudulent traffic detection and Fake Digital Marketing Campaigns; Use Case #6: Fortifying Clone Systems' SOC with CYBERGUARD solution (Cybersecurity Sector); and Use Case #7: Powering Up DSO's SOC with CYBERGUARD's AI (Energy Sector).

CYBERGUARD addresses the escalating complexity of cyber threats targeting critical infrastructure sectors such as Transportation, Energy, Finance, Maritime, Government, and Health. The key point of this approach is the deployment of sophisticated defense & attack strategies, driven by experts specializing in AI and enabling technologies.

The Project is committed to enhance the cybersecurity infrastructure across various organizations, aiming to proactively predict, detect, and mitigate cyber threats and vulnerabilities. By integrating a range of advanced technologies and methodologies, CYBERGUARD seeks to advance the security posture of organizations significantly.

CYBERGUARD Project funded by the European Cybersecurity Competence Centre (ECCC), under the Digital Europe Programme, with the Topic: DIGITAL-ECCC-2024-DEPLOY-CYBER-06-ENABLINGTECH, started its implementation on 1st December 2024, and gathers 13 Consortium Partners Organizations from Cyprus, Greece, Spain and Romania.

The European Consortium Partners is coordinated by I-ENERGYLINK (RO) working together with ARISTOTLE UNIVERSITY OF THESSALONIKI (GR), BOLTON TECHNOLOGIES (CY), CACTUS DIGITAL (GR), CLONE SYSTEMS (CY), COLUMBIA SHIPMANAGEMENT (CY), ROMANIAN NATIONAL CYBERSECURITY DIRECTORATE (RO), ELIAS NEOCLEOUS (CY), INTERNATIONAL HELLENIC UNIVERSITY (GR), JOT INTERNET MEDIA (ES), ROMGAZ (RO), BUCHAREST EMERGENCY HOSPITAL (RO), and SIQSESS TECHNOLOGY (RO).

