

CYBERFORT REPRESENTATIVES ACTIVELY PARTICIPATED AT CRA CLUSTER EVENT

9th October 2025, Carina Ioana NITA

CYBERFORT Representatives actively participated at the CRA Cluster Event, organized on 9th October 2025, in Bucharest, Romania. The objectives of the **Strengthening Cyber Defenses of SMEs for Cyber Resilience Act (CRA) Compliance Project** are: aiming to simplify the process of CRA compliance for Small and Medium Enterprises (SMEs); enhancing the efficiency of compliance documentation processes through automation. The Project is delivering training to elevate the cybersecurity knowledge and practices among SMEs; ensuring the tools evolve in response to new cybersecurity challenges and feedback from users; and fostering collaborations with cybersecurity networks and initiatives across Europe.

CRA Cluster Event highlighted important and key topics as following: meeting chair introduction and objectives; expectations, needs, and work streams for the CRA; lightning talks from related Projects in line with the Cyber Resilience Act; SMEs toolkits, landscape view of what are the priorities and next steps. Furthermore, the event also featured an interactive session using a Mural board, where participants exchanged and brainstorming about the activities of each Project presented and their outcomes. This interactive session brought useful insights regarding the tools and services, Use Cases, technical and standards developments, target stakeholders, relevant KPIs, and very important events.

During the event, Dr. Mihai PAUN – Founder of I-ENERGYLINK, introduced CYBERFORT EU-funded Project. CYBERFORT aims to make CRA compliance more practical and accessible, especially for SMEs and open-source developers. Dr. Mihai PAUN highlighted the main objectives of the project, the assets, the progress done, and the status of the work accomplished over the past ten months. He presented the project actions and achievements of implementing CYBERFORT Project: setting the requirements and creating the design of the platform; developed the Smart Document Generating feature together with the required policy templates; designed the Risk Assessment Methodology; designed the dashboard which will present the status of compliance together with the identified vulnerabilities.

Moreover, the Communication and Dissemination Plan has been finalized and shared. The project's visual identity was developed, along with templates for deliverables, presentations, and flyers. The project website was successfully launched and is regularly updated. In addition, three external events were organized, with CYBERFORT actively participating.

Furthermore, **four Complementary Use Cases under implementation were introduced by the Project Coordinator Drd. Paul LACATUS:** Shipboard Cybersecurity Training Program (Maritime Sector); Compliance Management Platform for Financial Institutions (Finance Sector); Critical Infrastructure Vulnerability Assessment Tool (Energy Sector); and Strategically Aligning Cybersecurity Solutions with CRA Compliance Standards. He elaborated on Justification and Applicability of CRA to the Use Cases.

The Cyber Resilience Act is a European Union Regulation designed to enhance cybersecurity standards for products with digital elements, including hardware and software, placed on the EU market. It requires manufacturers and retailers to ensure these products are designed, developed, and maintained with robust cybersecurity in mind throughout their lifecycle. The CRA entered into force on December 10, 2024, and will be fully implemented in three years, with some requirements becoming mandatory on September 11, 2026. The Key features and objectives of the CRA are the following: Mandatory Cybersecurity Requirements; Security-by-Design; Product Lifecycle Management; and Transparency.

The Project's development is driven by an International Consortium that is both complementary in expertise and united in its objectives. The CYBERFORT Project funded by the European Cybersecurity Competence Centre (ECCC), under the Digital Europe Programme, started its implementation on 1st December 2024. The Project gathers experts from Cyprus and Romania - 8 Consortium Partners Organizations. The European Consortium Partners is coordinated by I-ENERGYLINK (RO) working together with BOLTON TECHNOLOGIES (CY), CLONE SYSTEMS (CY), COLUMBIA SHIPMANAGEMENT (CY), DEALIO LIMITED (CY), ROMANIAN NATIONAL CYBERSECURITY DIRECTORATE (RO), ELIAS NEOCLEOUS (CY) and EXIMPROD ENGINEERING (RO).

CYBERFORT presents a comprehensive approach designed to strengthen the cybersecurity defenses of SMEs. It offers an integrated strategy to improve SMEs' cybersecurity by implementing the CRA requirements. The project emphasizes creating and sharing tailored compliance tools, best practices, and educational resources to help SMEs tackle the challenges posed by cybersecurity threats. CYBERFORT will develop free, open-source tools to support the internal compliance process in line with the CRA. Throughout the project's implementation, workshops, hackathons, and conferences will be organized to share results and outcomes.

