THE CONSORTIUM OF CYBERFORT EU FUNDED PROJECT IDENTIFIES INNOVATIVE CYBERSECURITY SOLUTIONS FOR SMEs AT THE KICK-OFF MEETING IN BRASOV, ROMANIA

28th January 2025, Carina Ioana NITA

CYBERFORT Consortium successfully organized the Kick-Off Meeting of a New European Funded Project – CYBERFORT „*Strengthening Cyber Defenses of SMEs for Cyber Resilience Act (CRA) Compliance*". The Project objectives are: aiming to simplify the process of CRA compliance for Small and Medium Enterprises (SMEs), making it more accessible and manageable; enhancing the efficiency of compliance documentation processes through automation, thereby reducing the administrative burden on SMEs; creating flexible tools that not only serve SMEs but are also adaptable to the needs of a broader range of stakeholders. 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 key cybersecurity networks and initiatives across Europe to maximize impact.

The CYBERFORT Project funded by the European Cybersecurity Competence Centre (ECCC), under the Digital Europe Programme, with the Topic: DIGITAL-ECCC-2024-DEPLOY-CYBER-06-COMPLIANCECRA, started its implementation on 1st December 2024. The Project gathers a robust and complementary International Consortium 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).

The Kick-Off Meeting of CYBERFORT took place on 30th-31st January 2025, in a hybrid format with the physical meeting in Brasov, Romania. CYBERFORT Kick-Off Meeting Agenda addressed key topics, activities and tasks including: Project Description, Consortium Structure, Partners Presentations; CYBERFORT Project Objectives and Guidelines; Cyber Resilience Act; Project Technical Coordination; Use Cases and Scenarios; Project System Design and Architecture; CRA Compliance Automated Tool Development; CYBERFORT Platform Requirements, Design, Architecture and Integration Plan; Platform Evaluation through Pilots Execution; Cybersecurity CRA specific training sessions; and Dissemination, Exploitation and Stakeholders Engagement.

In addition, Agenda underlined an Open Debate in order to inspire innovative ideas and communication amongst Partners: Open Debate on *Cyber Resilience Act Compliance for European Small and Medium Enterprises*. The *Business Modelling and Exploitation Activities, Replicability and Market Analysis* was an engaging subject on the CYBERFORT Kick-Off Meeting Agenda.

The Kick-Off Meeting started with the Project Introduction and Objectives and Dr. Mihai PAUN – Founder I-ENERGYLINK Partner welcomed all Participants physically present in the Conference Room and those who joined remotely. "*CYBERFORT initiative represents an Innovative Project designed to equip European Small and Medium-Sized Enterprises with the tools to strengthen their cybersecurity measures and comply with the Cyber Resilience Act, as well as other relevant cybersecurity compliance standards. The Project proposes an integrated approach to enhance cybersecurity posture through the implementation of the CRA requirements*", pointed out Dr. Mihai PAUN.

CLONE SYSTEMS Representatives – CYBERFORT Technical Coordinators presented key aspects regarding the Technical Functionalities for CYBERFORT Platform Development. *"It is essential to develop a Robust Cybersecurity Platform in order to create a secure, scalable, and efficient Platform for organizations to enhance their Cybersecurity posture and to ensure compliance with evolving cyber risk analysis standards. A sophisticated interface needs to be build up for situational awareness and data analysis and to conduct rigorous Penetration Testing to identify vulnerabilities in order to assess the effectiveness of the platform's defenses against potential Cyber Threats"*, underlined Giorgos MALOGIANNIS - Senior Developer.

CYBERFORT Market Analysis is an innovative topic that was outlined during the Kick-Off Meeting such as: to perform a competitive analysis of existing Cybersecurity Solutions; to analyze the market trends and emerging threats in Cybersecurity; to segment potential customers and assess their requirements; and the need to Evaluate barriers to entry and market adoption risks.

Strengthening Cyber Defenses of SMEs for Cyber Resilience Act (CRA) Compliance

CYBERFORT Project presents a comprehensive approach designed to strengthen the cybersecurity defenses of SMEs, with a particular focus on micro and small businesses. 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.

Strengthening Cyber Defenses of SMEs for Cyber Resilience Act Compliance Project aims to introduce innovative ideas and possibilities for various energy stakeholders across Europe, particularly in Southeastern Europe. The project's communication efforts will share this vision to inspire leaders in different sectors to leverage the contributions of the CYBERFORT initiative. CYBERFORT will develop free, open-source tools to support and automate 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.

CYBERFORT seeks to create a strong support framework, which includes cascade financing mechanisms to provide targeted financial assistance, an open platform for CRA-related resources, and extensive training and upskilling programs. The initiative also emphasizes building a collaborative ecosystem for knowledge sharing, standardization, and the exchange of cybersecurity best practices.

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE