EU FUNDED CYBERGUARD PROJECT CONSORTIUM IDENTIFIED INNOVATIVE SOLUTIONS TO FORTIFY SECURITY OPERATION CENTERS AGAINST CYBER THREATS AT THE KICK-OFF MEETING IN BRAȘOV, ROMANIA

18th February 2025, Carina Ioana NITA

CYBERGUARD Consortium successfully organized the Kick-Off Meeting of a New European Project - „*Fortifying SOCs Against Evolving Cyber Threats*". 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; implement proactive vulnerability management and incident response mechanisms to mitigate cybersecurity risks effectively; enhance the resilience of SOCs against emerging threats; and promote cybersecurity awareness to foster a culture of security within European societies and organizations.

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).

The Kick-Off Meeting of CYBERGUARD Project took place on 20th-21st February 2025, in a hybrid format with the physical meeting in Brasov, Romania. CYBERGUARD Kick-Off Meeting Agenda highlighted key activities and tasks as following: Objectives of the CYBERGUARD Kick-Off Meeting; Project Management and Coordination; Technical Management; AI-Driven Cybersecurity Analysis and System Design; Detailed Scenarios and Use-Cases Definition; System Design and Platform Architecture; CTI Management and Offensive Strategies; Malware Analysis and CTI Development; Data Poisoning and Research; Advanced Threat Detection and Mitigation; Integration, Pilot Use-Cases, Deployment and System Validation; Dissemination, Communication, Exploitation; and Resource Planning, Financial Coordination and Reporting.

In addition, two **Open Debates** were part of the Agenda in order to exchange Innovative Ideas and enhance Communication between Partners: ***Pilots ready to test Use Cases and CYBERGUARD developments in real life of Transportation, Health, Energy;*** **and** ***Publicity & Media Outreach, Market Analysis Business Modelling and Exploitation Activity***.

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. "*CYBERGUARD addresses the escalating complexity of cyber threats targeting Critical Infrastructure Sectors such as Energy, Transportation, Finance, Maritime, Government, and Health. The Project takes a holistic approach to cybersecurity, utilizing advanced methodologies in malware analysis, penetration testing, privilege escalation detection and research and mitigation of attacks. The Development of Scalable and Interoperable Solutions that integrate with existing SOC Infrastructure and security tooling is the Key Focus of the Project",* highlighted Dr. Mihai PAUN.

CLONE SYSTEMS Representatives – CYBERGUARD Technical Coordinators presented key aspects regarding the Technical Functionalities. *"It is crucial to enhance cybersecurity defenses through advanced threat detection, through AI-driven defense mechanisms, and to create a user-friendly CYBERGUARD dashboard. The key focus areas from the Technical Perspective are the adversarial attack simulation on Machine Learning (ML) models, detection & mitigation of adversarial threats & data poisoning, AI-powered cybersecurity solutions, and AI remediation*

This Project has received funding from the European Union's Digital Europe Programme under Grant Agreement no. 101190251

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

guidance for security teams. In order to harmonize these we need to align the objectives and tasks, to set up collaboration frameworks and to define initial adversarial attack scenarios for simulation and testing", underlined Mr. Giorgos MALOGIANNIS - Senior Developer.

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.

Its Innovative Solutions are: the deployment of machine learning algorithms for the detection and prevention of cybersecurity threats on networks and hosts, addressing complex security challenges posed by new and multifaceted threat actors. The aim is to enhance traditional detection mechanisms; advancing the generation, management, and secure dissemination of CTI within CYBERGUARD, by creating and implementing advanced tools and platforms to ensuring data security and privacy; systematizing the assimilation, organization, and scrutiny of diverse and voluminous data sets.

It will aid comprehensive analyses of cybersecurity incidents to improve threat detection, investigation, and response activities; and will employ Business Process Modelling Notation to encapsulate and streamline business continuity and incident response procedures, minimizing operational disruptions.

The Project results and outcomes will carry open-source licenses and will be disseminated within Events such as: Hackathons, Workshops and Conferences. The key action of the dissemination is to create awareness for CYBERGUARD services and products globally, establishing and promoting a market where Europe holds a prominent and influential position.

ENERGY
CYBERGUARD
WELCOME AND PROJECT INTRODUCTION
Fortifying SOCs Against Evolving Cyber Threats
K-OFF MEETING

This Project has received funding from the European Union's Digital Europe Programme under Grant Agreement no. 101190251

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE