CYBERGUARD PROJECT MANAGEMENT HANDBOOK HIGHLIGHTS

1st September 2025, Stefan Andrei SIMA

CYBERGUARD Consortium successfully Submitted the Project Management Handbook, a foundational Document that supports the overarching goal of the Project: to strengthen the resilience of Security Operations Centers (SOCs) in the face of rapidly evolving cyber threats. Building on a collaborative, cross-sector approach, CYBERGUARD Project is dedicated to enhancing detection, prevention, and response capabilities within SOCs through the integration of advanced AI-driven techniques, secure information exchange, and structured project governance. The project targets critical infrastructure sectors such as energy, healthcare, finance, and maritime, ensuring that they are equipped to tackle threats like adversarial AI attacks, malware, and LLM vulnerabilities. This Handbook marks a key milestone in aligning all Consortium Partners under Shared Processes and Best Practices to deliver on this mission effectively and securely.

The ***Project Management Handbook*** plays a central role in guiding the internal workings of the project. It defines how CYBERGUARD operates on a day-to-day basis while offering a unified set of procedures, templates, and workflows that help all partners collaborate efficiently and transparently. From defining governance structures to detailing the planning and reporting mechanisms, the handbook provides a clear roadmap for the implementation of the project's ambitious objectives. It ensures that every contributor, regardless of their technical or managerial role, understands the project's structure, expectations, and standards from the outset.

The Document introduces a well-defined framework that governs collaboration and coordination across the CYBERGUARD Consortium. It outlines the roles and responsibilities of the key governing bodies, such as the General Assembly, Project Management Committee (PMC), and Technical Management Committee (TMC), and describes how decisions are made, escalated, and documented. These mechanisms ensure that the project stays aligned with both its strategic goals and the regulatory obligations imposed by the European Union.

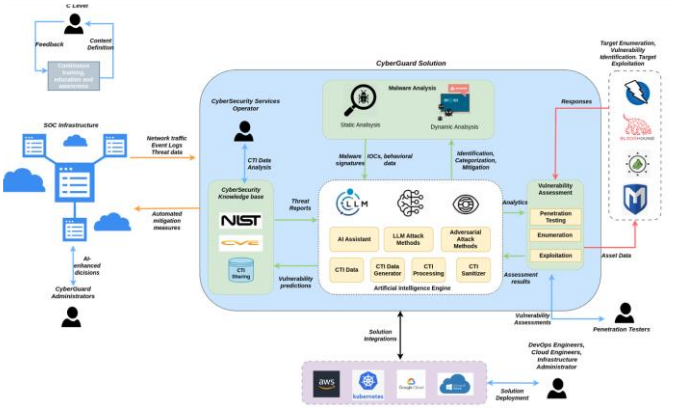
Another major focus of the handbook is the establishment of **effective communication channels** and **collaborative tools**, such as Microsoft Teams for internal coordination and GitHub for technical documentation and code management. These tools are paired with structured naming conventions, shared folders, and access protocols to ensure consistency and security in information flow.

In addition, the Project Management Handbook sets the standard for **Quality Assurance and Deliverable Management** by introducing a structured internal review process, deadlines, and responsibilities tied to each deliverable. Partners are expected to follow a clear timeline—from drafting to review and submission—ensuring that outputs meet the technical, ethical, and operational requirements of the Project.

Ultimately, the **Project Management Handbook** serves as the backbone of CYBERGUARD's operational setup. It reflects the Consortium's shared vision for structure, transparency, and ensures that all Partners move forward together, with clarity, precision, and mutual trust.

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).



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