Co-funded by the European Union

ΕΣΠΑ 2021-2027 Partnership Agreement 2021-2027

Programme Central Macedonia

Programme: "CENTRAL MACEDONIA" 2021–2027

Action: "Investments for the creation, expansion or upgrading of RTDI infrastructure in public academic or research institutions in the Region of Central Macedonia"

Project Title:

«CyberSentinel: Unified Next-Generation Infrastructures with SOC, Cyber-Range, and CPS for Enhancing Cyber Resilience and Protecting Critical Infrastructures».

Description:

The Centre for Research & Technology Hellas (CERTH), is participating in the "Central Macedonia" Programme of the "Partnership Agreement on Regional Development 2021-2027" through the Action "Investments for the creation, expansion or up grading of RTDI infrastructure in public academic or research institutions in the Region of Central Macedonia" co-funded by the European Union and National Resources.

The project titled "**CyberSentinel: Unified Next-Generation Infrastructures with SOC, Cyber-Range, and CPS for Enhancing Cyber Resilience and Protecting Critical Infrastructures**" aims to procure and install advanced computational, network, and specialized technological infrastructures (cutting-edge hardware and software) to enhance the capability for developing innovative applications, conducting high technological value research projects, and carrying out educational and operational activities in the field of cybersecurity, networks, and wireless communications (5G and beyond). Specifically, the project seeks to: (i) create an advanced Security Operation Centre (SOC) that will serve as a cybersecurity hub for enterprises and organizations in Central Macedonia and Northern Greece, (ii) install a specialized Cyber Range interconnected with cyber-physical systems (such as Smart Home) to provide advanced training and testing services, and (iii) create the first wireless communications cybersecurity hub through Radio Frequency Cyber Range infrastructure and a private 5G network.

Indicative expected benefits of this specific project, through its included interventions, are:

- Upgrading CERTH to a center of excellence for cybersecurity and wireless communications in Northern Greece.
- Enhancing CERTH's security and efficiency through real-time infrastructure monitoring, with continuous surveillance capability and rapid response to cyber threats.
- Conducting advanced applied research and developing prototype security systems.
- Participation in European research projects of high technological value in the cybersecurity domain.
- Provision of specialized training services through the Cyber Range and its interconnection with cyber-physical systems.

- Strengthening the cybersecurity posture of enterprises and organizations in Central Macedonia and Northern Greece through SOC services.
- Protection of critical infrastructures of enterprises and organizations in the region.

The social impact of the project lies in:

- Enhancing regional cybersecurity resilience and protecting critical infrastructures by establishing CERTH as a cybersecurity hub serving enterprises, organizations, and public entities in Central Macedonia and Northern Greece, with collaboration with the National Cybersecurity Authority for nationwide SOC interconnection.
- Developing cybersecurity expertise and strengthening the digital transformation through specialized training programs, workshops, and educational activities targeting researchers, students, and enterprise personnel, while raising public awareness about cybersecurity issues.
- Increasing citizen safety in the digital sphere through improved cybersecurity in daily-use services, contributing to overall security enhancement in the public and private sectors.

The objective of the project is to establish CERTH as a center of excellence in the field of cybersecurity and wireless communications, providing top-tier infrastructures and services that enhance innovation, knowledge, and security in the digital world. Through the creation of an integrated environment, the project aims at simulating and evaluating cyber threats, strengthening security mechanisms in critical infrastructures, developing skills for analyzing and responding to security incidents, supporting multiple users and teams (Red, Blue, White teams), as well as testing prototype wireless communication systems in high-demand environments.

The project's results are:

- Three integrated advanced infrastructures: a Security Operation Centre (SOC) for real-time threat monitoring and response, a specialized Cyber Range interconnected with cyber-physical systems enabling realistic attack simulations, and a Radio Frequency Cyber Range for wireless communications security including private 5G network infrastructure.
- Comprehensive technical documentation and knowledge transfer including technical specifications, installation, testing, and evaluation reports, complemented by demonstration and training activities for stakeholders and the research community.

Duration: 15 Months

Total Project Budget: 973.225€