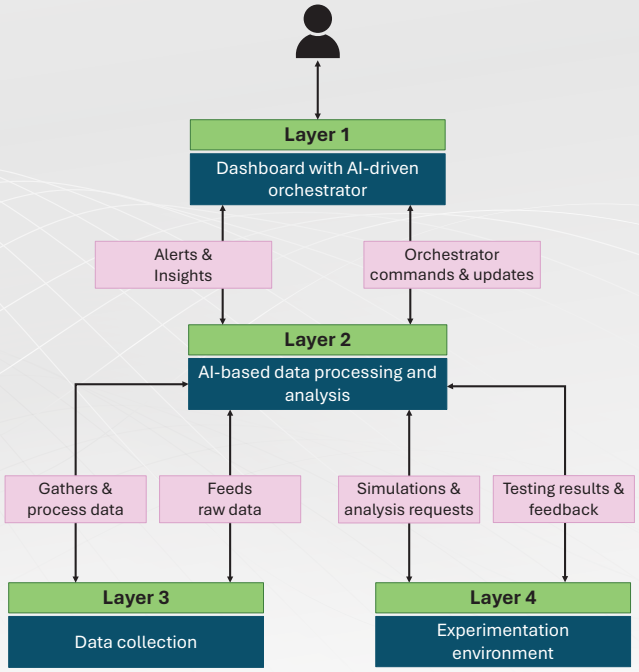
How LLM4CIP Works

The platform is built around four main components. First, an intuitive LLM powered dashboard lets users interact with the system in natural language, launch simulations, and easily view security insights. Second, an advanced AI analysis layer examines logs, behaviours, and vulnerabilities to detect threats and generate smart, adaptive attack scenarios using reinforcement learning. Third, a real time data collection framework gathers information from networks, endpoints, cloud systems, and IoT devices to create a complete view of infrastructure health. Finally, an experimentation environment, powered by a digital twin of the real system, enables safe penetration testing, hands on training, and validation of defences without affecting live operations.

Platform Architecture



LLM4CiP

Preparedness Through **Intelligence**
Protection Through **Innovation**

Follow us on LinkedIn
LLM4CIP

Check our website
www.llm4cip.eu

LLM-Powered Cybersecurity Preparedness and Risk Mitigation for **Critical Infrastructure Protection**

Start Date: **01/01/2026**
End Date: **31/12/2028**

LLM4CIP Motivation

LLM4CIP is a European initiative focused on building a robust and scalable cybersecurity platform designed to help critical infrastructure operators and essential service providers to proactively counter emerging cyber threats. By integrating LLMs with advanced AI/ML techniques, digital twin technology, and hybrid AI-powered red teaming, the platform delivers a unified ecosystem for vulnerability testing, strategic threat mitigation, and dynamic risk evaluation.

What makes it innovative?

It combines advanced AI with digital twins and reinforcement learning to transform how critical infrastructures prepare for cyber threats. It replaces complex, expert-only security tools with a simple conversational dashboard that anyone can use. By uniting automated penetration testing, continuous risk monitoring, and AI-driven guidance, LLM4CIP delivers a unique next-generation cybersecurity preparedness ecosystem.

Key Objectives

1. Development of an intelligent AI-orchestrated cybersecurity hub.
2. Integration of high-fidelity cybersecurity digital twin technology for cyber-range environment and cybersecurity simulations.
3. Continuous evaluation of vulnerabilities, threats, and operational risks using real-time data and AI-driven analysis.
4. LLM-enhanced test cases for improved effectiveness and efficiency of cyber-range training.
5. Intuitive visualisation of threat models to understand the potential impact of different threats.
6. Support NIS2 directive compliance across sectors.
7. Create a European ecosystem of cyber range technologies and activities for joint capability development.
8. Deploy a robust European cybersecurity platform.
9. Enhance cybersecurity preparedness and resilience across different important European organisations and industries.
10. Create a collaborative cybersecurity knowledge base.

Consortium

- ASSIST Innovative Minds — Romania
- ubitech — Greece
- ENISEY ICCS — Greece
- eBOSRD Engineered for Excellence Driven by Passion For Innovation — Cyprus
- European DIGITAL SME Alliance — Belgium
- Eunomia Ltd. Consulting Services — Ireland

Funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.