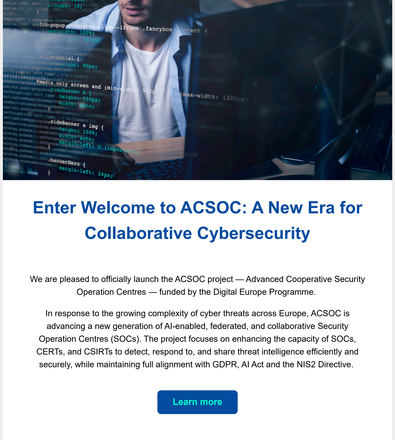
acsoc-project.eu

ACSOC



Enter Welcome to ACSOC: A New Era for Collaborative Cybersecurity

We are pleased to officially launch the ACSOC project — Advanced Cooperative Security Operation Centres — funded by the Digital Europe Programme.

In response to the growing complexity of cyber threats across Europe, ACSOC is advancing a new generation of AI-enabled, federated, and collaborative Security Operation Centres (SOCs). The project focuses on enhancing the capacity of SOCs, CERTs, and CSIRTs to detect, respond to, and share threat intelligence efficiently and securely, while maintaining full alignment with GDPR, AI Act and the NIS2 Directive.

Learn more

About ACSOC

ACSOC brings together advanced tools, expertise, and innovation to support cybersecurity operations across the EU. It introduces:

- AI-powered threat intelligence and anomaly detection tools, including evolutions of Lucy (previously named Joshua) and Sofia platforms, part of the Almaviva CyberRiskVision framework, supporting SOCs, CERTs and CSIRTs operation.
- An AI based Federated Machine Learning approach enabling secure cooperation and data exchange across institutions without transferring sensitive data.
- Practical guidelines and procedure supporting SOC operations aligned with European cybersecurity regulations and policies.
- Support of SaaS operation simplifying SMEs and Public Authorities with limited in-house cybersecurity capacity, offering simplified access to Cybersecurity services including threat information and indicators of compromise (IoCs).
- A viable tool (Euro Tech CDSES) in alternative to the use of comparable non European Technology

Learn more

Enter Kick-off Meeting in Rome

The ACSOC project began with a two-day Kick-off Meeting, held on 11–12 February 2025 at Almaviva's premises in Rome. All project partners gathered to discuss the work plan, presented the objectives and structure of each work package, and coordinated the project Start Up. The event also included presentations from the European Commission and technical demonstrations. The meeting marked the beginning of an ambitious joint effort to enhance Europe's cybersecurity capabilities.

Meet the Partners

ALMAVIVA | Coordinator

ALMAVIVA, Italy's leading IT company in System Integration and Digital Transformation, with 40 years of experience supporting both public administrations and private enterprises. ALMAVIVA's Cyber Security Practice provides a modular and scalable security framework combining proprietary and market technologies.

Learn more

Romanian National Cyber Security Directorate (DNSC)

DNSC is the national authority for civilian cyberspace in Romania, coordinating cyber risk management, incident response, awareness, training, and certification. With a mandate from the Romanian Government, DNSC ensures national cyber resilience through regulation, forecasting, and strategic collaboration.

Learn more

SisInfLab (Politecnico di Bari)

SisInfLab (Information Systems Laboratory) is a research laboratory at the Politecnico di Bari, dedicated to developing intelligent systems and smart data management solutions.

Learn more

JOIST Innovation Park

JOIST Innovation Park is a cutting-edge phygital innovation ecosystem based in Larissa, Greece, strategically connecting people, ideas, and technology through a powerful network across Europe.

Learn more

What Comes Next

In the coming months, ACSOC will:
Publish insights into the tools under development and their benefits. Launch the first round of training and awareness-building activities. Engage directly with European cybersecurity stakeholders, policymakers, and SMEs. Share ongoing progress through newsletters, articles, and events.

We invite you to stay connected, subscribe for updates, and take part in building a stronger, more resilient digital Europe.

ACSOC

acsoc-project.eu

Co-funded by the European Union

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 or ECCC. Neither the European Union nor the granting authority can be held responsible for them.

If you have reason to believe that you are not the intended recipient or you wish to unsubscribe from this mailing list please visit the following link (unsubscribe).