NCC-FR
FRANCE CYBERSECURITY COORDINATION CENTRE

TLP:AMBER+STRICT

Co-funded by the European Union

PARTNER SEARCH FORM
For
Digital Europe Programme (DEP)/Horizon Europe Programme (HEP)

GENERAL INFORMATION

Organisation	Université de Lorraine / LORIA (CNRS Joint Research Unit)
Country	*France*
Activity sector	Cybersecurity research, artificial intelligence, cybercrime, disinformation, systems security, software analysis,
Legal entity	*Research institution*
Call Reference (ID)	Horizon–CL3-2026-02-CS-ECCC-02
Call deadline	
Deadline to join the consortium	ASAP / Open to discussion

PARTNERING NEEDS AND EXPECTATIONS

Potential role in the project	Research / Technology provider / Dissemination
What specific expertise or resources are you ideally looking for in a partner for this call?	We are looking for partners with expertise in: • secure and trustworthy AI (robustness, explainability, privacy), • adversarial machine learning and attack/defense mechanisms, • large-scale AI systems and deployment environments, • data protection, privacy-preserving techniques (e.g., federated learning, PETs), • AI system evaluation, benchmarking, and certification, • industrial use cases involving AI in critical domains (cybersecurity, defense, infrastructure). We particularly welcome industrial partners and public stakeholders providing real-world AI systems and datasets
What is the responsibility your entity wishes to assume in the project consortium ?	WP leader / Task leader / Contributor (Potentially interested in a coordination role depending on consortium maturity)
What are your expectations regarding	We aim to build a consortium combining expertise in cybersecurity and AI.

the collaboration and contribution of partners in the project?	We expect partners to: • contribute to the design of robust and secure AI systems, • evaluate attack and defense mechanisms under realistic threat models, • provide datasets and experimental platforms, • support the integration of research outcomes into operational systems. Particular attention will be paid to **realistic adversarial settings** and **evaluation at scale**. We are also interested in contributing to the analysis of AI misuse in cybercrime ecosystems, through a data-driven observatory approach. This includes the large-scale collection and analysis of real-world practices related to the malicious use of AI (e.g., automation of attacks, obfuscation, disinformation, malware development). Such an approach enables the design of **realistic threat models** and supports the **evaluation of AI systems under adversarial conditions**, bridging the gap between theoretical robustness and operational security.
Are there any specific requirements or conditions you have for potential partners?	No strict requirements, but we value: • strong technical expertise in AI or cybersecurity, • ability to contribute to experimental validation, • commitment to collaborative and interdisciplinary work.

EXPERIENCE IN EUROPEAN AND NATIONAL PROJECTS (IF ANY)

Experience in national funded projects	Yes – multiple national projects in cybersecurity (e.g., France 2030, PEPR Cybersecurity, BPI, ANR, PTCC)
Experience in EU funded projects	Yes – participation in several EU projects (e.g., ENSEMBLE, Concordia), with strong experience in collaborative research and innovation actions

CONTACT INFORMATION

Contact person	*Maira Nassau*
Organisation	*Lorraine University*
Position/title	*Project Manager*
Email address	*Maira.Nassau@loria.fr*
Phone number	
Website	*www.loria.fr (dept web site)*

Thank you for your interest in partnering!