

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-01
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?	<p>We are looking for partners with complementary expertise in:</p> <ul style="list-style-type: none"> • software supply chain security (SBOM, dependency analysis, provenance tracking), • hardware security and embedded systems, • secure software development and CI/CD pipeline security, • certification, compliance, and security evaluation frameworks, • industrial use cases and large-scale deployment environments, • providers of real-world datasets (software, firmware, supply chain artifacts). <p>Industrial partners and state organization are particularly encouraged.</p>
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 the collaboration and	We aim to build a balanced consortium combining academic excellence and strong industrial relevance.

<p>contribution of partners in the project?</p>	<p>In this context, we bring strong expertise combining:</p> <ul style="list-style-type: none"> • data-centric observability platforms for tracking and correlating software artifacts across their lifecycle, • large-scale dynamic analysis techniques for detecting hidden malicious behaviors in third-party components, • experience in transferring research outcomes to operational environments through close collaboration with industrial partners. <p>We expect partners to:</p> <ul style="list-style-type: none"> • contribute actively to the design and evaluation of scalable security solutions, • provide realistic use cases and datasets, • support integration into operational environments, • engage in open collaboration and co-design of methodologies. <p>A strong emphasis is placed on end-to-end validation, from research prototypes to real-world deployment scenarios.</p>
<p>Are there any specific requirements or conditions you have for potential partners?</p>	<p>No strict requirements, but we value:</p> <ul style="list-style-type: none"> • commitment to active collaboration, • ability to contribute to experimental validation, • alignment with EU cybersecurity priorities and standards.

EXPERIENCE IN EUROPEAN AND NATIONAL PROJECTS (IF ANY)

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

CONTACT INFORMATION

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

Thank you for your interest in partnering!

