Défi clé

« Institut Cybersécurité Occitanie »

Appel 2023 : « Projets Scientifiques »

Contexte et objectifs

Le défi clé « Institut Cybersécurité Occitanie » (ICO) a été lancé en janvier 2022. L'ICO est une initiative pluridisciplinaire qui vise à rassembler et fédérer les acteurs de la cybersécurité, du monde académique et de l'industrie, afin de positionner la région Occitanie parmi les leaders dans ce domaine en France ainsi qu'au niveau international. L'Institut a pour objectif de stimuler la recherche amont, de développer la formation et de favoriser la collaboration et l'innovation avec les industriels.

L'ambition de ce projet est de privilégier les secteurs applicatifs qui sont des marqueurs historiques pour la région Occitanie : notamment l'aéronautique, l'automobile, le spatial et la santé. Un autre différenciateur fort de l'écosystème Occitanie concerne l'interdisciplinarité des recherches menées, qui couvrent l'informatique, les mathématiques ainsi que les aspects juridiques, sociologiques, géopolitiques et économiques de la cybersécurité.

L'Institut est financé par la Région Occitanie pour 5 ans. Le financement comprend le soutien d'actions de recherche par le biais d'appels ouverts pour des bourses de doctorat (50%) et de post-docs, des financements d'ingénieurs pour le développement de démonstrateurs et prototypes de recherche, des projets scientifiques et des cofinancements de mobilité, ainsi que le soutien à l'organisation d'événements scientifiques, de sensibilisation et d'actions de formation qui contribuent à renforcer la visibilité et l'attractivité de l'écosystème de la cybersécurité dans la région Occitanie. Les propositions impliquant différents laboratoires ou des sujets interdisciplinaires sont fortement encouragées.

Bénéficiaires

Le projet scientifique doit être réalisé dans un laboratoire de recherche de la région Occitanie. Les projets collaboratifs, impliquant plus d'un partenaire au niveau régional, national ou international, sont encouragés.

Règles d'éligibilité

Le projet doit satisfaire les conditions suivantes :

- Le projet scientifique doit être porté par un membre d'un laboratoire de recherche en cybersécurité de la région Occitanie. La liste inclut : ENAC, CEA, Équipe de droit pénal et sciences forensiques de Montpellier (UR 212 UM), IES (UMR 5214 CNRS/UM), IDETCOM (EA 785 UT CAPITOLE), Institut de droit privé (EA 1920 UT CAPITOLE), IMAG (UMR 5149 CNRS/UM),

IMT (UMR 5219 CNRS/INSA/INUC/UT CAPITOLE/UT2/UT3), IRIT (UMR 5505 CNRS/INP/UT3/UT CAPITOLE/UT2), ISAE-SUPAERO, LAAS-CNRS (UPR 8001), Laboratoire de Droit Privé (UR 207 UM), LERASS (EA 827 UT3), LIRMM (UMR 5506 CNRS/UM), TSE-R (UMR 1415 UT CAPITOLE/CNRS/INRAE/EHESS). D'autres laboratoires sont également invités à répondre à cet appel.

- Les contributions peuvent couvrir différentes disciplines incluant l'informatique, les mathématiques ainsi que des aspects juridiques, sociaux, géopolitiques et économiques de la cybersécurité.
- Le sujet de recherche devra cibler, à court, moyen ou long terme, des défis répondant à un ou plusieurs des objectifs de recherche suivants :

1. Renforcer la sécurité des matériels, des logiciels et des systèmes.
2. Assurer la sécurité des futurs réseaux et environnements connectés/technologies émergentes.
3. Mieux protéger les données et la vie privée, et améliorer la confiance dans les réseaux sociaux.
4. Améliorer la conception par des approches formelles et étudier l'impact/contribution de l'intelligence artificielle.

- Les porteurs seront invités à présenter leurs résultats aux partenaires de l'ICO à la fin du projet.
- Toute publication liée au projet devra inclure la mention suivante :

« Ce travail a bénéficié du soutien de l'ICO, Institut Cybersécurité Occitanie, financé par la Région Occitanie, France »

Financement

- Le financement ne doit pas dépasser **15k€.**
- La durée maximale du projet est de 24 mois (en cas d'extension, le montant du financement par l'ICO reste inchangé).
- Le budget demandé peut être utilisé pour couvrir les gratifications de stage des étudiants, les dépenses d'achat d'équipement, de consommables, de petites fournitures, les frais de voyage et d'hébergement des experts scientifiques invités, le soutien à la mobilité nationale ou internationale, etc.

Modalités et dossier de candidature

Calendrier et procédure de sélection

- La demande doit être déposée au plus tard le **30 Sept. 2023, 11:59 AM.**
- L'évaluation et la sélection des projets seront effectuées par le Comité Exécutif de l'ICO pendant la semaine du **09 au 13 octobre 2023.**
- Notification : quelques jours après la réunion du Comité Exécutif.

Dossier de candidature

Description du projet :

La présentation doit suivre le plan suivant :

- Titre du projet et porteurs
- Partie I. Résumé du projet (10 lignes)
- Partie II. Informations générales:

- Participants (incluant le CV des porteurs du projet)
- Durée du projet
- Budget demandé

- Partie III. Description détaillée du projet (max. 5 pages) :

- Verrous et objectifs scientifiques, avec un bref positionnement par rapport à l'état de l'art
- Programme scientifique et planning des activités
- Résultats attendus (scientifiques, collaboration nationale/ internationale, soutien à la formation, ...)
- Si c'est pertinent, les noms des experts qui seront invités avec une description de leurs domaines scientifiques doit être inclue avec un bref CV

- Partie IV. Financement

- Justification du budget demandé
- Autres ressources qui seront mobilisées

Dépôt des projets :

Les propositions doivent être transmises en un seul fichier pdf (taille max. 10 Mo), en nommant le fichier comme suit :

2023ICO_Project_Acronyme_NomCandidat.pdf

Envoi par email à : bureau@ico-occitanie.fr avant le **30 Septembre 2023, 11:59 AM**.

Contact

Pour toute demande d'information complémentaire, contacter par email : bureau@ico-occitanie.fr

“Institut Cybersécurité Occitanie”

Key Challenge Project

2023 CALL : “Scientific Projects”

Context and objectives

The “Institut Cybersécurité Occitanie” (ICO) Project was launched in January 2022. ICO is a multidisciplinary initiative that aims to gather and federate key players in cybersecurity, from academia and industry, in order to position the Occitanie region among the top leaders in this field in France as well as at the international level. The Institute aims to stimulate upstream research, develop training and promote collaboration and innovation with industry.

The ambition of this project is to privilege the application sectors that are historical markers for the Occitanie region: in particular, aeronautics, automotive, space and healthcare. Another strong differentiator of the Occitanie ecosystem concerns the interdisciplinarity of the research conducted, which covers computer science, mathematics as well as legal, social and business-related aspects of cybersecurity.

The Institute is funded by the Occitanie Region for 5 years. The funding includes the support of research actions through open calls for PhD and postdocs scholarships, funding for engineers to implement research demonstrators and prototypes scientific projects and travel grants mobility cofinancing, as well as the support for organization of scientific and outreach events and education initiatives that contribute to enhancing the visibility and attractiveness of the cybersecurity ecosystem in the Occitanie region. Proposals involving different labs or multidisciplinary topics are highly encouraged.

Beneficiaries

The scientific project has to be carried out in research labs in the Occitanie region. Collaborative projects, involving more than one partner at the region, national or international levels are encouraged.

Eligibility rules

The project must meet the following conditions:

- The principal investigator of the project shall be a member of a research lab located in the Occitanie region, that is involved in research activities in cybersecurity. The list includes: ENAC, CEA, Équipe de droit pénal et sciences forensiques de Montpellier (UR 212 UM), IES (UMR 5214 CNRS/UM), IDETCOM (EA 785 UT CAPITOLE), Institut de droit privé (EA 1920 UT CAPITOLE), IMAG (UMR 5149 CNRS/UM), IMT (UMR 5219 CNRS/INSA/INUC/UT CAPITOLE/UT2/UT3), IRIT (UMR 5505 CNRS/INP/UT3/UT CAPITOLE/UT2), ISAE-SUPAERO, LAAS-CNRS (UPR 8001), Laboratoire de Droit Privé (UR 207 UM), LERASS (EA 827 UT3), LIRMM (UMR 5506 CNRS/UM), TSE-R (UMR 1415 UT CAPITOLE/CNRS/INRAE/EHESS). Other labs that are not listed can also apply.
- Contributions can cover computer science, mathematics as well as legal, social and business-related aspects of cybersecurity. Interdisciplinary projects are encouraged.
- The research topic will have to target, in a short, mid or long run, challenges addressing one or several of the following research goals:

1. Strengthen hardware, software and system security.
2. Ensure the security of future networks and connected environments/emerging technologies.
3. Better protect data and privacy, and improve trust in social networks.
4. Improve design through formal approaches and study the impact/contribution of artificial intelligence.

- Accepted candidates will be invited to present their results to ICO's partners at the end of their projects.
- Every publication related to the project shall include the following acknowledgement:

"This work was supported by ICO, Institut Cybersécurité Occitanie, funded by Région Occitanie, France"

Budget and duration

- The requested budget should not exceed **15 k€.**
- The duration of the project must not exceed 24 months (in case of extension, the amount of regional aid remains unchanged).
- The requested budget can be used to cover students internship gratifications, expenses for the purchase of equipment, consumables, small supplies, travel and accommodation expenses for invited scientific experts, support for national or international mobility, etc.

Application

Deadline and selection

- Completed application file should be submitted before **September 30th 2023, 11:59 AM.**
- The assessment of the applications will be carried out by the ICO Executive Committee during the week of **October 9th – 13th, 2023.**
- Notification: few days after the evaluation meeting.

Project Description

Formal applications should include the following information:

- Project Title & Applicant
- Part I. Brief summary of the project (10 lines)
- Part II. Detailed general information:

- Project participants (and resume of the PIs)
- Project duration
- Requested budget

- Part III. Full description of the project (max. 5 pages):

- Problems and scientific interests, brief bibliography
- Scientific program, planned activities and milestones
- Expected outcomes (scientific, national/ international collaboration, support for education)
- If relevant, the names of potential invited scientific experts and their fields of expertise should be included (brief resume)

- Part IV. Detailed budget

- Justification of the requested budget
- Additional support covered by other sources

How to apply

Applications should be submitted as a single file with a maximum size of 10 Mo. The file name should be the following:

2023ICO_Project_Acronym_ApplicantFamilyName.pdf

Send the pdf file by email to: bureau@ico-occitanie.fr by **September 30th 2023, 11:59 AM**.

Contact

For more information about the call, please send an email to: bureau@ico-occitanie.fr