



Défi clé

« Institut Cybersécurité Occitanie »

Appel 2023 : « Soutien à des événements scientifiques et de sensibilisation en cybersécurité »

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.

Objet de l'appel

L'un des objectifs de l'ICO est d'accroître la visibilité et l'attractivité de l'écosystème de la cybersécurité en région Occitanie aux niveaux régional, national et international. En conséquence, cet appel vise à parrainer et à soutenir l'organisation d'événements scientifiques régionaux, nationaux ou internationaux (conférences, ateliers, écoles d'été, ...) ainsi que des initiatives et des événements liés à la formation visant à diffuser la culture de la cybersécurité, et à amplifier la sensibilisation aux menaces et aux techniques de protection associées.

Règles d'éligibilité

- Les événements soutenus doivent avoir lieu en Occitanie. Les demandes de soutien doivent être déposées par un membre d'un laboratoire de recherche de la région Occitanie développant des activités de recherche en cybersécurité. 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.
- Pour les événements scientifiques, la priorité sera donnée aux événements de portée internationale et nationale et visant à renforcer la collaboration entre plusieurs partenaires au niveau régional. Les demandeurs sollicitant le soutien de l'ICO doivent être membres du comité d'organisation ou du comité scientifique de l'événement.
- Les événements liés à la diffusion de la culture scientifique peuvent être locaux. Ils peuvent cibler l'un des publics suivants : écoliers, étudiants, jeunes, enseignants, grand public / citoyens.
- Les critères suivants seront considérés dans l'évaluation des demandes :
 - La renommée scientifique de l'événement ou, pour les événements de culture scientifique, son impact attendu
 - La contribution de l'événement au renforcement de la visibilité et de l'attractivité de l'écosystème de la cybersécurité en région Occitanie et aux objectifs de l'ICO
 - L'encouragement de la participation de jeunes chercheurs et d'étudiants
 - La dimension collaborative avec les autres partenaires de l'ICO.

Obligations du porteur de l'événement

- Le porteur s'assurera que le logo de l'ICO figure sur tous les supports de communication liés à l'événement (imprimés et électroniques) mis à la disposition des participants et du public.
- Toute publication issue de l'événement devra inclure la mention suivante :

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

Soutien financier

Le Comité Exécutif de l'ICO décidera du montant du soutien financier à accorder en fonction de la demande en tenant compte de la nature et de l'impact attendu de l'événement ainsi que du nombre de participants et du plan de financement.

Procédure pour la demande de soutien

Calendrier et procédure de sélection

- L'ICO organisera 3 appels par an, avec comme **date limite le 30 septembre, le 31 janvier et le 31 mai** de chaque année.
- Les demandes seront traitées par le Comité Exécutif dans un délai de 2 à 3 semaines à compter de la date limite de chaque appel à participation.
- Notification : quelques jours après la réunion du Comité Exécutif.

Dossier de demande de soutien

Le porteur de la demande doit transmettre à minima les éléments suivants :

- Nom de l'événement, date et lieu, nombre de participants attendus et publics ciblés
- Description des objectifs et présentation de l'événement
- Programme prévisionnel incluant le nom des intervenants confirmés et pressentis, thématiques traitées et lien avec les objectifs de l'ICO
- Budget prévisionnel et utilisation du soutien financier
- Autres soutiens acquis et sollicités.

Ces éléments doivent être transmis en un seul fichier pdf (taille max. 10 Mo), en nommant le fichier comme suit :

ICO_Events_Acronyme_NomResponsable.pdf

Demande à transmettre par email à l'adresse : bureau@ico-occitanie.fr

Contact

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



“Institut Cybersécurité Occitanie”

Key Challenge Project

2023 CALL : “Support to scientific and outreach cybersecurity events ”

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.

Scope of the call

One of the goals of the ICO is to increase the visibility and attractiveness of the cybersecurity ecosystem in the Occitanie region at the regional, national and international levels. Accordingly, this call is aimed at sponsoring and offering financial support to the organization of regional, national or international scientific events (conferences, workshops, summer schools, ...) as well as education related initiatives and events aimed at dissemination of cybersecurity culture and increasing awareness about related threats and protection techniques.

Eligibility rules

- The supported events must take place in the Occitanie region. Applications should be submitted by a member of a research lab in the Occitanie region 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 1415UT CAPITOLE/CNRS/INRAE/EHESS). Other labs that are not listed can also apply.
- For scientific events, priority will be given to events with international and national scope and aimed at enhancing collaboration between several partners at the regional level. The applicants requesting ICO support must be members of the organizing committee or the scientific committee of the event.
- Events related to the dissemination of scientific culture can be local. They can target one of the following audiences: school children, students, young people, teachers, general public / citizens.
- The following criteria will be considered for the assessment of applications:
 - The scientific reputation of the event or for scientific outreach events, its expected impact;
 - The contribution of the event to strengthening the visibility and attractiveness of the cybersecurity ecosystem in the Occitanie region
 - The encouragement of the participation of young researchers and students
 - The collaborative dimension with other ICO partners.

Obligations of the event organizer

- The event organizer shall ensure that the ICO logo appears on all communication materials related to the event (printed and electronic documents).
- Every publication related to the supported event shall include the following acknowledgement:

*“This work was supported by ICO, Institut Cybersécurité Occitanie,
funded by Région Occitanie, France”*

Financial support

The ICO Executive Committee will decide on the amount of financial support granted to the event based on the requested budget, taking into account the nature of the event, the number of participants, the expected impact of the event and the financing plan.

Application

Deadline and selection

- ICO will organize 3 calls per year, with **deadlines of September 30th, January 31st and May 31st** of each year.

- Applications will be assessed by the ICO Executive Committee and the applicants will be notified within 2 to 3 weeks after the deadline of each call for participation.

How to apply

Formal applications should include:

- Title of the event, date and location, target audience and estimated number of attendees
- Description of the objectives and scope of the event
- Provisional program including the names of confirmed and prospective speakers, themes/disciplines addressed and link with ICO topics of interest
- Estimated budget and use of ICO support if granted
- Other financial support obtained/ requested.

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

ICO_Events_Acronym_ApplicantName.pdf

Send the pdf file by email to: bureau@ico-occitanie.fr

Contact

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