Journée scientifique du Défi Clef ICO « Institut de Cybersécurité de l'Occitanie »

19 avril 2023, LAAS-CNRS

Programme

- **09:00 – 09:30 Accueil – Posters (13)**
- **09:30 - 10:00 Introduction ICO- Actions en cours**
- **10:00 - 11:20 - Session 1 - Présentations Thèses ICO**
  - **Céline Bellanger**. Cybersécurité pour les systèmes embarqués à base d'IA. Direction: Pierre-Loïc Garroche (ENAC) et Matthieu Martel (Université de Perpignan)
  - **Van Tien Nguyen**. Auto-protection des environnements nomades. Direction: Eric Alata, Daniela Dragomirescu (LAAS-CNRS); Guillaume Doyen, NAVAS, Renzo E. (IMT Atlantique)
  - **Gabin Noblet**. Utilisation de réseaux de neurones "adversariaux" pour générer des données d'intrusion réseau réalistes Direction: Philippe Owezarski (LAAS-CNRS), William Ritchie (Cyblex Technologies)
  - **Antony Dalmiere**. Ingénierie sociale pour la cybersécurité : « Social Engineering », Direction: Pascal Marchand (UT3) et Vincent Nicomette (LAAS-CNRS)
- **11:20 – 12:15 Discussion générale**
- **Déjeuner - Posters**

Programme

- **14:00- 15:00 Présentations partenaires : SHS et cybersécurité**
  - **Jessica Eynard (IDP, UTC) et Giorgia Macilotti (IRIT, CNRS) :** Sécurité et identité(s) numérique(s)
  - **Jérôme Ferret (IDETCOM, UTC) et Mario Laurent (docteur en Sciences du langage) :** Approche interdisciplinaire des discours de haine en ligne : résultats et perspectives
  - **Pascal Marchand (LERASS, UT3) :** Détecter des traces complotistes en ligne : analyse textométique de 135.000 commentaires sur les vaccins.
- **15:00 – 16:20 Présentation partenaires : Sécurité matériel, logiciel, système**
  - **Jean-Christophe Deneuville (ENAC)**, Cryptographie post-quantique, introduction et enjeux
  - **Brahim Hamid** (IRIT), Rigorous development of secure architecture within the negative and positive statements
  - **Sophie Dupuis (LIRMM),** Comment prévenir la surproduction de vos ICs ? Etat de l'art du Logic locking.
  - **Vincent Migliore (LAAS)**, Détection d'attaques matérielles par analyse de signaux micro-architecturaux
- **16:20 – 17:30 Discussion générale**

Défi Clef
Institut de cybersécurité de l'Occitanie

Mohamed Kaâniche
Vincent Nicomette

Fabien Laguillaumie
Florent Bruguier

Abdelmalek Benzekri

Giorgia Macilotti

Contact: bureau@ico-occitanie.fr
Site web : http://www.ico-occitanie.fr

Période : 1er janvier 2022 - 31 décembre 2026
Tutelle gestionnaire : CNRS (DR14)

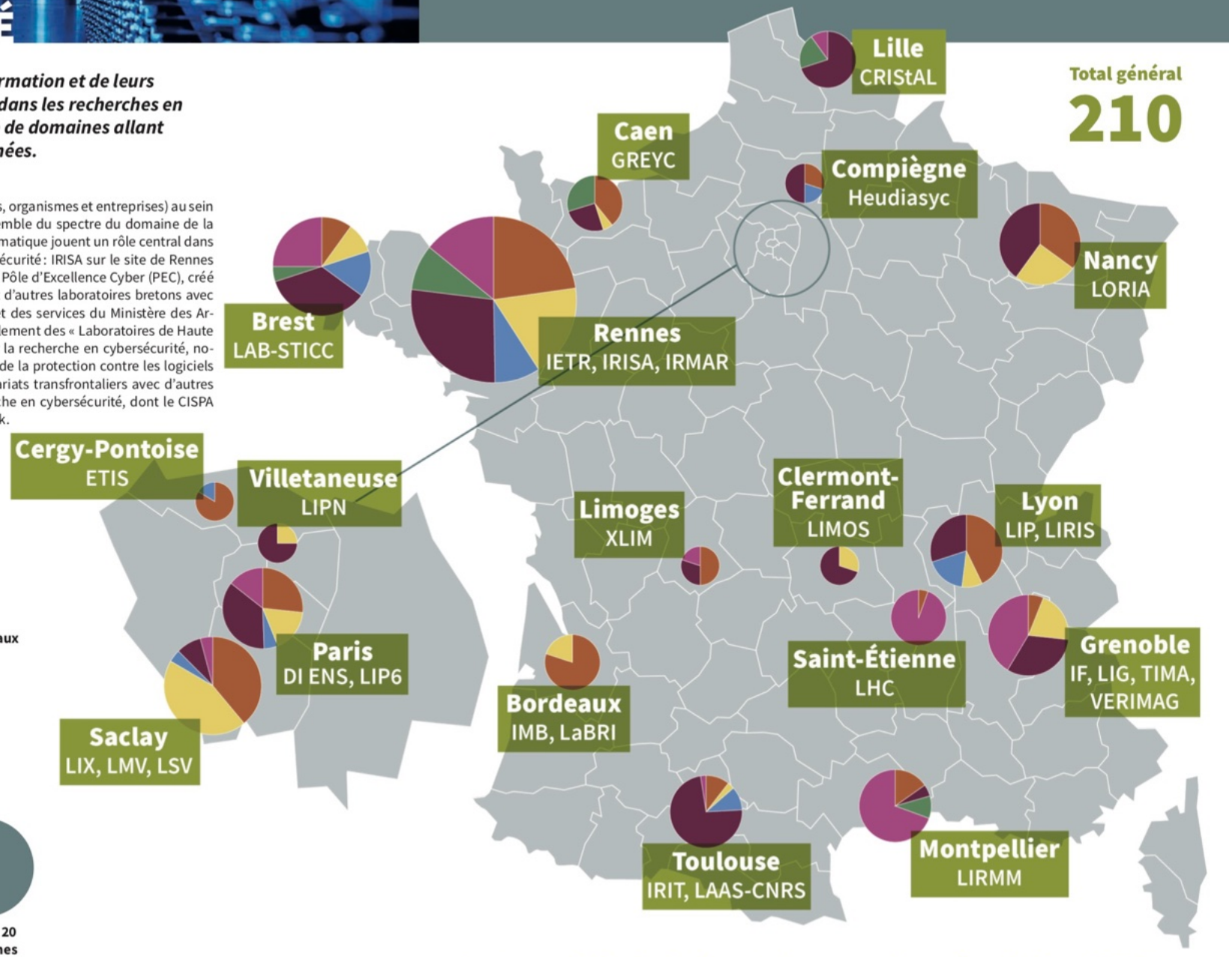
La cybersécurité : Contexte

- **Recrudescence de la cybercriminalité**
  - Objets connectés, infrastructures et systèmes critiques, données personnelles, réseaux sociaux, intelligence économique…
- **Une priorité des programmes européens (H2020, Horizon Europe, …)**
  - Centre européen de compétences industrielles, technologiques et de recherche en cybersécurité et réseau des centres nationaux de coordination
- **Plusieurs initiatives en France**
  - Appel de Paris pour la confiance et la sécurité dans le cyberspace (2018)
  - Comité stratégique de Filière (CSF) « industrie de sécurité »
  - PEPR dédié à la cybersécurité – PIA4
  - Campus Cyber
- **Région Occitanie**
  - Plusieurs outils pour soutenir la filière (Cyber'Occ, EDIH Occitanie, CERT/CSIRT, …)

LES LABORATOIRES EN CYBERSÉCURITÉ

À travers l'Institut des sciences de l'information et de leurs interactions (INS2I), le CNRS est investi dans les recherches en cybersécurité et couvre un large spectre de domaines allant de la cryptologie à la protection de données.

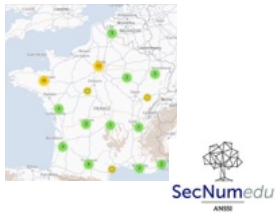
Le CNRS mène, avec ses partenaires (universités, écoles, organismes et entreprises) au sein des unités mixtes de recherche, des travaux sur l'ensemble du spectre du domaine de la cybersécurité. Deux laboratoires de recherche en informatique jouent un rôle central dans les deux pôles identifiés au niveau national en cybersécurité : IRISA sur le site de Rennes et LORIA sur celui de Nancy. Le site rennais accueille le Pôle d'Excellence Cyber (PEC), créé en 2016, qui structure les partenariats entre l'IRISA et d'autres laboratoires bretons avec des acteurs industriels français de la filière sécurité et des services du Ministère des Armées. Les sites de Rennes et de Nancy accueillent également des « Laboratoires de Haute Sécurité » (LHS) qui constituent des plateformes pour la recherche en cybersécurité, notamment sur le thème de la détection d'intrusions et de la protection contre les logiciels malveillants. Le site de Nancy développe des partenariats transfrontaliers avec d'autres centres d'excellence européens en matière de recherche en cybersécurité, dont le CISPA (*Helmholtz Center for Information Security*) à Sarrebruck.



Cartographie des laboratoires en cybersécurité au CNRS

La cybersécurité en Occitanie

> Une Recherche et Formation d'excellence



> **Sciences du numérique et SHS**

> **Université de Toulouse**

- Licence Pro. Réseaux Informatique, Mobilité, Sécurité – IUT de Blagnac UT2J – **SecNumEdu**
- Bachelor Universitaire de Technologie (BUT) – Cybersécurité et IoT – IUT de Blagnac UT2J
- UT3: 3 parcours dans 2 master sciences numérique, Réseaux et Télecom (Parcours IDP, SSIR, STRI) - Master ISSD (Ingénierie, Sécurité, Sûreté et Défense)
- Formation ingénieur TLS-SEC et Mastère spe "securité Informatique (ENSEEIHT, ENAC, INSA) –**SecNumEdu**
- UT1C: 2 masters sciences sociales sur enjeux stratégiques liées au numérique et menaces cyber

> **Université de Montpellier**

- Licence Pro. Réseaux et Télecom- Parcours Cybersécurité – IUT de Béziers –**SecNumEdu**
- BUT – parcours déploiement d'applications communicantes et sécurisées
- Fac. des sciences – Master Informatique –crypto
- Sécurité matérielle (2 formations Bac + 5 , 1 MASTERE à Polytech Montpellier, école doctorale I2S)

> **Une offre riche en Formation Continue**

> **Plus de 150 personnes (chercheurs, enseignants-chercheurs, ingénieurs de recherche, doctorants, post-doctorants)**

La cybersécurité en Occitanie

> Un écosystème industriel riche

- Airbus, Airbus DS, Activus, Algodone, APSYS, BoostAerospace, BPCE, Capgemini, CNES, Continental, CGI, CS, Cyblex Technologies, Digital Security, IMS Networks, iTrust, Modis, Orange, OCD, Pierre Fabre, Renault Software Labs, Rockwell Collins, Scassi, SecLab Cybersecurity, Sogeti, Sopra-Steria, Thales Avionics, Thales CS, Thales Alenia Space, Thales DIS, Vitesco, Ninjalab, Netheos, Objectif Libre, Lyra Networks, iBP, Great-X, Pradeo, Ziwit, …

> Des acteurs et clusters dynamiques

CYBER'OCC

Ambitions – Thèmes pluri-disciplinaires

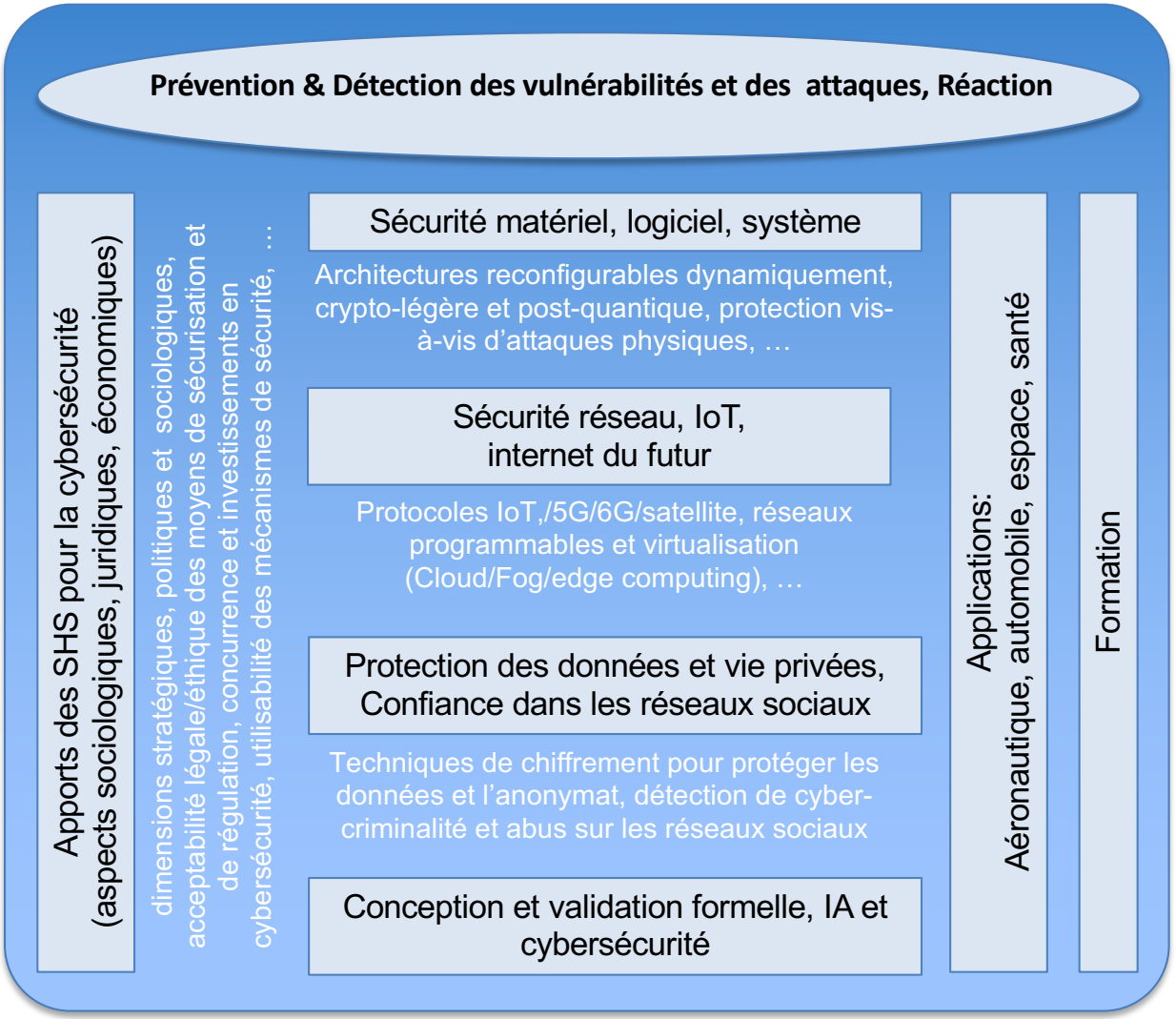
Fédérer les forces en cybersécurité en Occitanie et assurer une meilleure visibilité nationale et internationale du site (groupes de travail, animation scientifique, projets …)

Renforcer les moyens humains par le co-financement d'allocations doctorales/ Post-docs

Soutenir des actions de formation et de sensibilisation à la cybersécurité (modules FC courte duréee, école thématique cyber sécurité, conf. annuelle THcon, défi cyber collèges-lycées)

Développer les collaborations industrielles (Thèses co-financées, projets collaboratifs, synergie avec les clusters Cyber'OCC, …)

Renforcer nos collaborations internationales (chercheurs invités, séminaires, projets)



Plan d'actions et budget initial

Action	Nombre	PU (k€)	Total
Thèses (50%)	10	61,1	611
Post Doc – (12 ou 18mois)	180 mois		865
Projets exploratoires (max 15k€/projet)		15	150
Accueil chercheurs invités	8 mois	5,5	44
Actions de formation, sensibilisation, animation scientifique, rayonnement • Ingénierie pédagogique • Journées annuelles du projet • école thématique cybersécurité • Soutien conférences (THcon, …) • Séminaires invités, comité scientifique			180
CDD IE «Chef de projet »	4 ans	37,6	150
Total			**2000**

> des évolutions depuis la mise en place

Gouvernance

- **Bureau**
  - Assure le fonctionnement au jour le jour
  - Composition: 6 chercheurs (LAAS, LIRMM, IRIT, SHS) + Chef de projet
- **Comité exécutif**
  - en charge de la stratégie, mise en place du programme de travail annuel, appels d'offres, sélection, opportunités de collaborations/projets
  - 17 membres : 11 chercheurs (représentant les différentes disciplines), 1 représentant de Cyber'OCC, 1 représentant de l'ANSSI, 2 industriels, 1 représentant de la Région, Chef de projet
  - Fréquence: 4 fois/an minimum et autant que nécessaire
- **Comité de pilotage**
  - Valider les différentes actions mises en place
  - Représentants des tutelles (CNRS, UM, …) et de la Région Occitanie
  - Fréquence: en début du projet et ensuite 1 fois/an

Thèses lancées en 2022

- **Céline Bellanger**
  - Sujet : Cybersécurité pour les systèmes embarqués à base d'IA
  - Direction: Pierre-Loïc Garroche (ENAC) et Matthieu Martel (Uni. Perpignan)
  - Co-financement **:** ENAC
- **Van Tien Nguyen**
  - Sujet : Auto-protection des environnements nomades
  - Direction: E. Alata, D. Dragomirescu (LAAS-CNRS); G. Doyen, NAVAS, Renzo E. (IMT Atlantique)
  - Co-financement : IMT Atlantique
- **Gabin Noblet**
  - Sujet : Utilisation de réseaux de neurones "adversariaux" pour générer des données d'intrusion réseau réalistes
  - Direction: P. Owezarski (LAAS-CNRS), W. Ritchie (Cyblex Technologies)
  - Co-financement : Cyblex
- **Skandalis Maximos**
  - Sujet : Apprentissage profond et méthodes formelles pour la détection automatique d'énoncés contradictoires - application à la détection de désinformations
  - Direction : Richard MOOT, Christian RETORE, Simon ROBILLARD (LIRMM)
  - Co-financement : AID
- **Antony Dalmière**
  - Sujet : Social Engineering
  - Direction: V. Nicomette (LAAS-CNRS), P. Marchand (Lerass, UT2J)
  - Co-financement : UT3

Thèses : Pré-sélection Appel Avril 2023

- **Tran Phan Quoc BAO**
  - Sujet : Regular-Singular D-Modules in Positive Characteristic – (*crypto*)
  - Direction: Joao Pedro dos Santos (IMAG)
- **Ziling LIAO**
  - Sujet : ARSENE: Susceptibilité des mémoires embarquées volatiles et non-volatiles aux injections de fautes : modèles et durcissement – (*sécurité matériel*)
  - Direction: Florent Bruguier, Philippe Maurine (LIRMM)
- **Marianne PRUDET**
  - Sujet : Biométrie et systèmes d'intelligence artificielle : pour un cadre juridique fiable et protecteur des droits et libertés fondamentaux (*SHS*)
  - Direction: Jessica Eynard (Institut de Droit Privé)
- **Marie-Eve SAMSON**
  - Sujet : L'équilibre des pouvoirs dans le complexe militaro-industriel spatial en France - (*SHS*)
  - Direction : Lukas RASS-MASSON (Institut de Droit Privé)
- **Damien THEVENIAUT**
  - Sujet : A Framework for Considering Human Factors in Collaborative Decision Making for Secure Architecture Design (HCODES) - (*processus de conception pour la sécurité- facteurs humains*)
  - Direction: Brahim Hamid (IRIT), Jason Jaskolka (Carlton Uni, Canada)
- **Javier Camino TREVINO**
  - Sujet : KeyGen: Génération de clés secrètes à partir de sources d'aléa commun (*crypto-couches basses*)
  - Direction: Meryem Benammar et Damien Roque (ISAE)

Appels Post-Doc

- **Leslie Nardari**
  - Sujet : L'usurpation d'identité : propositions pour une lutte efficace
  - Direction: Jessica Eynard (Institut de Droit Privé)
  - Septembre 2022 – Février 2023 (intégration école de la magistrature)

- **Appel en cours :**
  - date limite 14 mai 2023
  - Financement : 18 mois max.

Projets Scientifiques : Appel 14 Oct. 2022

- **SecIIV**
  - Sujet : Security Objectives Threatened by Implicit Interactions Vulnerabilities
  - Brahim Hamid (IRIT), Jason Jaskolka (Carlton Univ., Canada)
  - Durée: 24 mois — Montant : 15 k€
- **CAP**
  - Sujet : Revisiting Constraint Acquisition Through the Lens of Program Specification Synthesis
  - Nadjib Lazaar (LIRMM), Sébastien Bardin, Arnaud Goetlib, Grégoire Menguy (CEA Paris Saclay)
  - Durée: 24 mois — Montant : 15 k€
- **SSbD**
  - Sujet : Seamless Security by design
  - Nan Messe (IRIT), Jamal El Hachem (IRISA), Avi Shaked (University of Oxford, UK), Mehdi Mirakhorli (Rochester Institute of Technology (RIT), US.)
  - Durée: 24 mois — Montant : 10 k€

- **Prochain Appel 2023: 14 mai 2023**

Soutien de manifestations scientifiques

> Trois dates de soumission dans l'année

- 30 septembre — 31 janvier — 31 mai

> Soutien

- Montant : 2000 € max
- Cas particuliers selon l'envergure et la nature des événements

> Charte ICO en cours d'élaboration

- Égalité, mixité, diversité
- Réduire l'empreinte environnementale
- …

Soutien de manifestations scientifiques

- **THCon – Toulouse Hacking Convention, co-organisé par l'ICO**
  - 14-15 avril, 2022, Toulouse
  - 20-21 avril, 2023, Toulouse

- **Workshop on Trusted Computing and the Internet of Things (TcIoT)**
  - 10 novembre, 2022, IRIT, Toulouse
  - Organisateur: Mohamed Kandi (IRIT)

- **Colloque Collectivités Territoriales et Cybersécurité**
  - 8 décembre 2022, Université Toulouse Capitole
  - Organisateur : Giorgia Macilotti (IDETCOM)

Soutien de manifestations scientifiques

- **JC2: Journées Nationales du GT Codage et Cryptographie (C2) du GDR « Informatique et Mathématique » et le GDR « Sécurité Informatique »**
  - 15-20 octobre, 2023, Najac, Aveyron
  - Cible les jeunes chercheurs, doctorants, post-doctorants
  - Organisateurs: Jean-Christophe Deneuville (ENAC), Emmanuel Hallouin (Toulouse 2), Jérôme Lacan (Isae Supaero), Philippe Moustrou (Toulouse 2) Marc Perret (Toulouse 2)

Autres opportunités : Groupes de travail

- GT : Formation
  - Animateurs: Abdelmalek Benzekri, Florent Bruguier, V. Nicomette, Girogia Macilotti
- GT : SHS et cybersécurité
  - Animateurs: TBD

- GT : Sécurité matériel, logiciel, système
  - Animateurs: TBD
- GT 2: Sécurité réseau, IoT
  - Animateurs: TBD
- GT : Sécurité des données, réseaux sociaux
  - Animateurs: TBD
- GT : Approches formelles, IA
  - Animateurs: TBD
- GT : Santé …

GT Formation - Réponse AMI CMA

> AMI “Compétences et métiers d’avenir”

- Anticiper et contribuer à satisfaire les besoins en emploi ou en compétences
- Accélérer la mise en œuvre de formations répondant aux besoins
- Toucher tous les publics, quel que soit le statut (scolaires, étudiants, apprentis, salariés, demandeurs d’emploi, indépendants, libéraux, entrepreneurs...)
- Veiller à avoir un spectre large en matière de formation : de bac-3 au bac+8,
- formation tout au long de la vie
- S’appuyer sur des dispositifs existants, les mettre en réseau ou inventer des solutions nouvelles
- Repérer les bonnes pratiques locales, nationales ou internationales et favoriser leur essaimage

Appel CMA Cybersécurité

- **Budget de 140 M€ - 4 objectifs:**
  - Formation initiale de spécialistes
  - Sensibilisation de non spécialistes en formation initiale
  - Formation continue
  - Sensibilisation dans le secondaire
- **Objectif : doubler le nombre d'emplois dans la filière d'ici 2025 : 37 000 emplois supplémentaires**
- **Constat de la région Occitanie (Cité de l'Economie et des Métiers de Demain, avec CyberOcc) :**
  - Besoin de sensibilisation, et de renforcement de la formation initiale et continue
  - Volumétrie d'emploi importante (-+ 3000 emplois à horizon 3 ans).
- **Proposition coordonnée par l'ICO, portée par l'UT**
- **Échéance** : au fil de l'eau, on cible un dépôt en mai

Ambition de la proposition ICO (1)

- Sensibiliser à la cybersécurité (formation initiale)
  - Les étudiants du supérieur en Occitanie (niveau L, M), quelque soit le diplôme
  - Les doctorants, quelle que soit la thématique de recherche
  - Les élèves du secondaire (lycée, collège)
- Sensibiliser à la cybersécurité (formation continue)
  - Des managers
  - Des cadres
  - Des techniciens
  - Des acteurs de collectivités territoriales
- Former des experts (formation de spécialistes)
  - Modules “avancés”, à destination d’étudiants de niveau BUT3/L ou M
  - Niveau doctorat/postdoc pour aider à former les non spécialistes
- Partenaires contactés
  - écoles/universités en Occitanie
  - écoles doctorales en Occitanie
  - industriels
  - institutionnels (rectorat, région, ANSSI, gendarmerie, Réserve Cyber Citoyenne...)

Ambition de la proposition ICO (2)

- 5 Axes proposés
  - Conception des modules d'enseignement formation initiale
  - Conception des modules de formation continue
  - Formation des formateurs
  - Mise en place de plateformes pédagogiques
  - Promotion de la formation et des métiers

Partenaires déclarés (3)

- Universités/écoles/ EPIC
  - UT Capitole, Sciences Po
  - UT2J
  - UT3
  - UM (Polytech Montpellier, IUT Nîmes, IUT Montpellier, UFR STAPS, Fac de Droit..)
  - ISIS
  - ENAC
  - INSA
  - INP/N7
  - ISAE
  - CEA
- Industriels
  - Airbus, …
  - Lettres de soutien : Thales, Continental, …
- Institutionnels
  - Région, Rectorats

Contact et participation à l'ICO

- **Si vous souhaitez**
  - contribuer aux activités de l'ICO, en recherche, formation ou innovation, participer aux groupes de travail
  - co-financer des thèses, proposer des stages, …
  - partager vos besoins en formation continue
  - monter des projets collaboratifs avec les partenaires de l'ICO (ANR, Europe, …)
  - co-organiser/soutenir des événements en cybersécurité (scientifiques, sensibilisation, innovation/dév-éco, …)
  - faire partie du club des partenaires industriels de l'ICO
  - vous inscrire sur les listes de diffusion de l'ICO
  - proposer des initiatives
  - …

contactez par email: bureau@ico-occitanie.fr

Communication

- Logo

- Page web
  - http:// www.ico-occitanie.fr

- Liste de diffusion: diffusion-ico-occitanie@laas.fr
  - Pour vous inscrire à cette liste, envoyer un email à: sympa@laas.fr
    avec comme objet : subscribe diffusion-ico-occitanie

- Comptes Linkedin, Twitter : à mettre en place