PROGRAMME DE TRANSFERT AU CAMPUS CYBER

La Cyber au rendez-vous de l'IA de confiance
20 Juin 2023 - Auditorium du Campus Cyber

Session du matin

Accueil café : 8h00

9h00 - 9h20 : Introduction

- *Florent Kirchner, Coordinateur de la stratégie nationale pour la cybersécurité*
- *Guillaume Avrin, Coordinateur de la stratégie nationale pour l'intelligence artificielle*

9h20 - 10h00 : Keynotes

Keynote 1 : L'IA pour la Cybersécurité

- *David Bizeul, Resp. Scientifique, Sekoia*
- *Gildas Jeantet, Resp. Data, Sekoia*

Keynote 2 : La Sécurité de l'IA

- *Teddy Furon, Directeur de Recherche, Inria*

10h00 - 10h50 : Table Ronde-1 | Focus recherche
Etat de l'art de la recherche, focus sur quelques thématiques en IA & Cyber
Animée par Cédric Auliac, Resp. Programme IA, CEA

- *Cédric Gouy-Pailler, Resp. de Laboratoire, CEA*
- *Jean-Yves Marion, Directeur du Loria/CNRS*
- *Luc Chausson, Resp. Département Certification des technologies de l'Information, LNE*
- *Pierre-Francois Gimenez, Chercheur, Inria-CentraleSupélec*
- *Reda Yaich, Resp. Cybersécurité et Réseaux, IRT SystemX*

10h50 - 11h00 : Questions/Réponses

11h00 - 11h50 : Table Ronde | Focus Réglementaire
Quelles sont les réglementations en vigueur en Cybersécurité et Intelligence artificielle ?
Animée par Cécile Théard Jallu, Cabinet De Gaulle Fleurance

- *Agnes Delaborde, Resp. Département Evaluation IA et Cybersécurité, LNE*
- *Brunessen Bertrand, Professeure de Droit, Université de Rennes, CNRS*
- *Félicien Vallet, Chef du Service IA, CNIL*
- *Isabelle Landreau, Docteur en Droit, Group DPO, Idemia*

11h50 - 12h00 : Questions table ronde

12h00 - 12h15 : Présentation appels à projets Transfert du PTCC

- *Michel Mauny, Coordonnateur des projets de recherche et de transfert, PTCC*

12h15 - 13h30 : Networking/Cocktail

La Cyber au rendez-vous de l'IA de confiance
20 Juin 2023 - Auditorium du Campus Cyber

Session de l'après-midi

13h30 - 14h00 : Cybersécurité pour l'IA de confiance

- *Keynote 3 : Protecting ownership rights of ML models using watermarking in the light of adversarial attacks*
- *Katarzyna Kapusta, Ingénieur R&D en Cybersécurité, Thales*

14h00 - 14h30 : Présentation d'une solution de détection de la menace

- *Utilisation de l'IA pour de la détection de menaces ransomware via l'analyse du trafic SMB*
- *Jérôme Plumecoq, Resp. Team ML, Gatewatcher*

14h30 - 15h00 : Pitchs de startup Cyberbooster

- *Eny Sauvertre Co-founder, Brain Security*
- *Arthur Duchet-Suchaux, Co-founder, Knock-Knock*
- *Georges-Bastien Michel, CEO, Reversense*

15h00 - 15h20 : Présentation de l'outil PRECRIME (EN VISIO)

- *Luigi Lenguito, CEO, Bfore.ai*

15h20 - 15h40 : Présentation de la plateforme CYLVIA

- *Thomas Czernichow, Directeur technique science des données, ALEIA*

15h40 - 16h00 : Présentation du projet ANR Picture (EN VISIO)

- *Sécurité physique et intrinsèque des réseaux de neurones embarqués*
- *Pierre-Alain Moellic, ingénieur de recherche en Sécurité de l'Intelligence artificielle, CEA*

16h00 - 16h30 : Publication scientifique

- *Keynote 4 : Modèle d'attaque IA contre la crypto-postquantique*
- *Francois Charton, Ingénieur de recherche Meta-AI*

16h30 - 17h20 : Présentations de sujets de thèses

- *Confiance et incertitude dans les modèles de neurones profonds*
  Grégor Jouet, Doctorant, Institut For Future Technologies, MIPTIS

- *Auto-configuration des algorithmes d'apprentissage pour la détection d'intrusion*
  Omar Anser, Doctorant, Inria

- *Utilisation du ML pour les attaques par canaux auxiliaires*
  Sana Boussam, Doctorante, Inria/Thales

- *In-network autonomous defense systems*

Wafik Zahwa, Doctorant, Inria/Numeryx (EN VISIO)

- *Exploring the Scope of Machine Learning using Homomorphic Encryption in IoT/Cloud*
  Yulliwas Ameur, Doctorant CNAM Paris

17h20 - 17h30 : Mot de clôture

- *Françoise Préteux, Directrice déléguée à la recherche et au développement économique, IMT*