CAMPUS CYBER

Campus Cyber - IA

01. ORCHESTRATION ECOSYSTEME.

+ **ESPACE D'ÉCHANGES ENTRE PAIRS** SÉCURISÉ.

+ **LIEU DE LA GOUVERNANCE** TOUT AU LONG DU CYCLE DE VIE DES PRODUCTIONS.

+ **TIERS DE CONFIANCE** POUR LA PRODUCTION, DIFFUSION ET L'EXPLOITATION DES LIVRABLES.



02. INNOVATION - CAMPUS CYBER.

+ EXPLORER

+ PRODUIRE

+ PARTAGER

Explorer des sujets complexes[1]

Identifier et anticiper les futures évolutions de marché de la cyber.

Explorer par la réduction des risques grâce à la mutualisation.

Mettre en œuvre des projets exploratoires[2]

En vue de productions de livrables et de briques technologiques : prototypages, preuves de concepts.

Générer des effets de levier pour et par l'écosystème par le partage des communs[3]

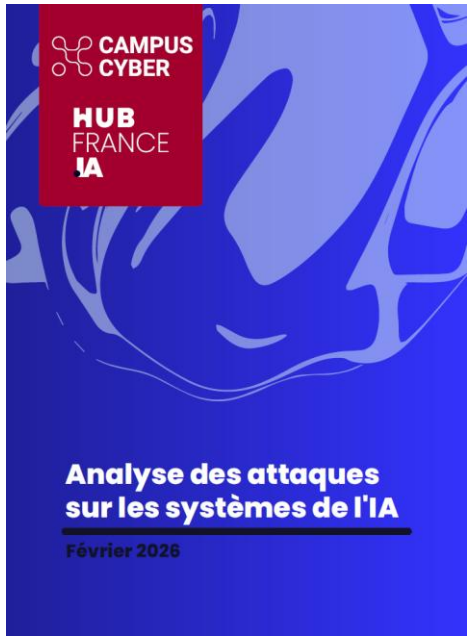
Propager les points de vue et les orientations de l'écosystème français.

Encourager le développement de standards.

Accroître l'interopérabilité des solutions françaises.

03. GROUPES DE TRAVAIL IA X CYBERSECURITE – LES DERNIERS LIVRABLES.

LIVRE BLANC – ANALYSE DES ATTAQUES SUR UN SYSTÈME D'IA.



GROUPE DE TRAVAIL MUTUALISE CAMPUS CYBER X HUB FRANCE IA

Un référentiel commun pour comprendre, qualifier et cartographier les risques liés aux attaques sur les systèmes d'IA avec des fiches pratiques par scénario d'attaque.

V4 à sortir fin 2026

GUIDE D'IMPLEMENTATION DES RECOMMANDATIONS POUR UN SYSTÈME D'IA GENERATIVE.



GROUPE DE TRAVAIL CAMPUS CYBER

Co-lead HeadMind Partners et BNP Paribas

Traduire les principes de sécurité recommandés par l'ANSSI en actions concrètes, mesures et méthodes pour implémenter les recommandations du guide. Ce document aborde l'ensemble des recommandations du guide de l'ANSSI.

04. GROUPES DE TRAVAIL – TRAVAUX EN COURS.

GROUPE DE TRAVAIL CAMPUS CYBER EN COURS– SECURISATION DE L'IA

Partage sur l'état de déploiement / difficultés / recommandations et besoins au sein des organisations.

- Identifier les problématiques les plus critiques pour les 6 prochains mois

5 thématiques de travail :

1. Contrôle des outils et des actions
2. Identity and Access Management (IAM)
3. Sécurité des objectifs et des prompts
4. Cloisonnement du runtime et de la mémoire
5. Surveillance des comportements et Human in/over the loop



05. NOTE D'ANALYSE - MYTHOS ET AUTRES MODELES-FRONTIERE.

Regard croisé de plusieurs catégories d'acteurs mobilisés par le Campus Cyber (DSI, RSSI, spécialistes en intelligence sur la menace cyber, en gestion de crise, en pentesting et en audit, conseil en transformation numérique…), a un triple objet :

- synthétiser les éléments d'analyse rassemblés à date au sein de l'écosystème du Campus Cyber
- identifier les principales implications des progrès de l'IA en cyber, au-delà du seul cas Mythos, pour les utilisateurs finaux comme pour les offreurs de solutions
- amorcer la structuration d'une réponse collective, au carrefour des deux communautés cyber et IA

Suivi d'un cycle de **Matinales de l'IA.**

06. IA & CYBER : IDENTIFIER LES PROCHAINS CHANTIERS COLLECTIFS.

L'IA constitue un axe stratégique du Campus Cyber dans la feuille de route 2026–2028.

Identification des sujets à lancer avant fin 2026, avec un premier focus sur la sécurisation des agents IA.

- Workshop pour identifier les enjeux communs rencontrés par les acteurs de l'écosystème
- Qualifier les besoins opérationnels et le partage / démo de cas d'usage prioritaires
- Évaluer les possibilités de mutualisation au sein de l'écosystème
- Constituer les communautés de travail permettant de faire avancer ces sujets collectivement

Contacts :

nicolas.sastre@campuscyber.fr Directeur Pole Innovation et International
juliette.farcy@campuscyber.fr Programmes Innovation

CAMPUS CYBER

CAMPUS CYBER ©