UCAC (FORMATION CONTINUE)
Université Catholique d'Afrique Centrale

PANESS
PARTENAIRE

EXECUTIVE MASTER CYBERSECURITE ET INTELLIGENCE ARTIFICIELLE



PANESS

Douala:

(+237) 697.076.997

Village COGEFAR (entrée mini cité)

Yaoundé:

(+237) 659.30.94.00

Yaoundé , Montée Cradat - Immeuble IHTM-Université

paness.ucac@panessgroup.com

UCAC Formation continue:

(+237) 677.27.72.03

Yaoundé , Campus d'Ekounou

Partenaires techniques:

PIST Université · IHTM Université · SUP'RH Casablanca Maroc

PRÉSENTATION

La massification et la sophistication des cyberattaques qui utilisent aujourd'hui de nouvelles approches d'automatisation ou d'apprentissage en s'appuyant, notamment, sur des techniques de Machine Learning imposent de nouvelles approches et de nouvelles compétences de la part des experts de la cybersécurité.

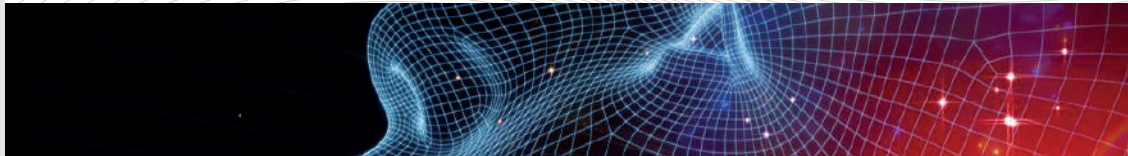
Le Mastère Cybersécurité et intelligence artificielle répond à ces nouveaux dangers en formant des experts capables de mettre en place les dernières avancées en matière d'Intelligence Artificielle et de Machine Learning au service de la cybersécurité pour mieux protéger les organisations contre les cybermenaces.



OBJECTIFS DE LA FORMATION

Ce programme vise à former des experts capables de comprendre et de répondre aux menaces de sécurité complexes en utilisant la puissance de l'IA, tout en sécurisant les systèmes d'IA eux-mêmes.

- Apprendre à identifier et à mitiger les vulnérabilités dans les modèles d'apprentissage automatique (Machine Learning
- IA pour la Cybersécurité : Utiliser l'IA (en particulier le Machine Learning et le Deep Learning) pour améliorer les outils de cybersécurité, comme la détection d'anomalies, la classification des logiciels malveillants, la prévention des intrusions et l'automatisation de la réponse aux incidents.
- Audit et Conformité : Maîtriser les cadres réglementaires (comme le RGPD) et les normes de sécurité.
- Compétences Techniques : Maîtrise des langages de programmation clés (Python pour l'IA, C/C++ pour la sécurité bas niveau), des infrastructures de cloud computing, des réseaux, et des systèmes d'exploitation.



COMPÉTENCES ACQUISES

- Maîtriser les techniques d'apprentissage automatique (Machine Learning, Deep Learning) pour la détection proactive des anomalies, la classification des menaces et l'analyse des comportements suspects.
- Savoir traiter et analyser de très grands volumes de données de sécurité (logs, alertes SIEM) pour identifier des modèles d'attaques complexes.
- Utiliser l'IA pour surveiller en temps réel, détecter les menaces émergentes et mener des activités de renseignement sur les cybermenaces (Cyber Threat Intelligence).
- Comprendre les vulnérabilités propres aux modèles d'IA (attaques par empoisonnement, évasion) et savoir comment sécuriser les systèmes d'apprentissage automatique.
- Appliquer les principes de l'IA et de l'automatisation dans les pipelines de développement (DevSecOps) pour garantir la sécurité dès la conception.
- Mener et piloter des projets de sécurisation complexes.
- Agir en respectant les règles déontologiques strictes de la cybersécurité et du maniement des données.
- Maintenir une connaissance à jour des dernières cybermenaces et des avancées en IA
- Former et sensibiliser les équipes et la direction aux enjeux de la cybersécurité.

DÉBOUCHÉS DE LA FORMATION

- Ingénieur Cybersécurité
- Analyste SOC / CERT
- Consultant en sécurité des systèmes d'information
- Data Scientist spécialisé sécurité
- Ingénieur IA et sécurité
- Architecte Sécurité Cloud
- Responsable sécurité informatique (RSSI)
- Expert en détection d'intrusion basée IA

PROGRAMME

- UE1 Outils de programmation I
- UE2 Outils mathématiques
- UE3 Matériels et réseaux
- UE4 Langue et droit
- UE5 Privacy et creativity
- UE6 Learning
- UE7 Traitement langage
- UE 8 Sécurité système
- UE9 Approfondissement data
- UE10 Développement web
- UE10 Cybersécurite
- UE10 Sécurité
- UE11 Mangement et marketing

CONDITIONS D'ADMISSION

- Bac + 3 informatique
- Expérience professionnelle (2 ans minimum dans le domaine)

CONSTITUTION DU DOSSIER

- Copies certifiées conformes acte de naissance, CNI, Diplôme (Bac +3 minimum) ;
- Attestation de travail;
- CV ;
- Lettre de motivation ;
- 4 photos 4×4 ;
- 35 000 FCFA frais de dossier ;





CORPS ENSEIGNANT

- Un corps enseignant compétent, polyvalent et diversifié, composé d'enseignants de l'UCAC et d'enseignants internationaux ;
- Des enseignants associés de l'UCAC issus des entreprises, de cabinets de cybersecurité, du monde universitaire ;
- Experts internationaux expérimentés et spécialisés
  1. Bonde Lossan, PhD (Systèmes embarquées, Université de Lille/AUA, Kenya)
  2. Pagna Jules, PhD (Cybersécurité, Bradford University/BNP Paribas, GB)
  3. Ainam Jean Paul, PhD (Intelligence Artificielle, Polytechnic University/Meta, USA)
  4. Moulema Paul, PhD (Programmation avancée, Andrews University, USA)
  5. Ngueleo, Lucien PhD(c) (Machine learning, Universite de Lille 1,France) ;
- Des conférenciers de renommée internationale et professeurs visiteurs des écoles internationales partenaires de l'UCAC.

Date limite de dépôt des dossiers : 13 FÉVRIER 2026
Rentrée académique formation Continue : 23 FÉVRIER 2026

Durée de la formation	**2ANS (18 MOIS)**
Coût de la formation	**1 225 000FCFA / AN**

Modalités de Paiement au démarrage de chaque semestre 625 000 FCFA