C3 CYBERSECURITY CLUB CONGO &

# Les 1ères UNIVERSITES DE LA CYBERSECURITE AU CONGO

du **11** au **23** Novembre 2024
au **Palais des Congrès** - BRAZZAVILLE

**FORMATION "CLASSE MAKOLA"**

**TITRE : SENSIBILISATION ET FORMATION SUR LA CYBERSECURITE - INTELLIGENCE ARTIFICIELLE**

**SYLLABUS FCL-M**



## 1. Introduction

### 1.1 Objectifs

L'objectif principal des Universités de la Cybersécurité est de sensibiliser à la problématique de la cybercriminalité et d'initier aux principaux enjeux de la cybersécurité ainsi qu'à l'utilisation des technologies de pointe innovantes.

La formation permettra de :



- Développer la culture de sécurité des Systèmes d'Informations en entreprise.
- Former des acteurs de sécurité des Systèmes d'Informations de haut niveau susceptibles d'intervenir efficacement dans les différents problèmes de sécurité pour la protection des infrastructures TIC.
- Comprendre les enjeux de la cybercriminalité
- Maîtriser les compétences techniques
- Connaître les mesures de prévention
- Bâtir une cyberstratégie d'une organisation
- Former des professionnels spécialisés dans la détection, l'investigation et la prévention des crimes informatiques
- Instruire les acteurs sécurité à l'utilisation de l'intelligence artificielle pour la cybersécurité.

### 1.2 Prérequis pour les apprenants

Cette formation est ouverte à tous. Néanmoins l'expérience professionnelle fera la différence.

De plus, les connaissances de base suivantes faciliteront la compréhension des étudiants, mais ne sont pas impératives :

– Connaissances de base sur les systèmes d'information (biens, fonctionnement, le modèle OSI, le protocole TCP/IP, etc.) ;
– Connaissances de base sur le fonctionnement technique des réseaux, des systèmes d'exploitation et des applications.

### 1.3 Cibles privilégiées

– Les agents des institutions techniques/stratégiques de la République
– Les agents des forces de sécurité et de défense (la gendarmerie, la police, les services de renseignements, l'armée, ...)
– Les professionnels publics et privés
– Les enseignants-chercheurs

## 2. Animateurs

1. **Christian Makaya, PhD** (Animateur Principal)
   - Expert et Leader en Intelligence Artificielle, Cybersécurité et Réseaux Intelligents
   - Directeur Scientifique, HP inc., Palo Alto, Californie, USA
   - PhD en Génie Informatique
2. **Marius Gabin ETA** (Assistant)
   - Expert en Transmission des Données et Sécurité de l'Information
   - Consultant en Cybersécurité
   - Enseignant Chercheur en TIC et Maths Appliquées à l'Université Marien Ngouabi
   - Président du CyberSecurity Club Congo, Brazzaville (Congo)
3. **Colonel Alain EKONDZI** (Assistant)
   - Docteur en Informatique
   - Enseignant-Chercheur, Université Marien Ngouabi, Brazzaville (Congo)
   - Directeur du Centre de Formation de l'Informatique (CFI) du Centre d'Informatique et de Recherche de l'Armée et de la Sécurité (CIRAS).
4. **Vivien Armel EYANGOLO** (Assistant)
   - Instructeur Cisco certifié CCNP Entreprise |Certifié CyberOps.
   - Doctorant en Cybersécurité à Bircham International University.
   - Responsable de service du centre de calcul au CFI-CIRAS-

## 3. Programme de la formation

Cette formation est constituée de 4 modules indépendants étalés sur 4 jours.



| | |
|---|---|
| **Module 1** | **Cyberfraude et Cyber enquête** |
| **Durée** | *7 Heures* |
| **Objectifs** | *Dans ce tutoriel nous allons couvrir les techniques et méthodologies pour faire des investigations relatives à des crimes commis via Internet et de lutte contre ces types de méfaits. Un aperçu de la sécurisation des données pour la répression des cybercrimes y sera aussi abordé.* |
| | |
| **Module 2** | **Stratégie opérationnelle de la cybersécurité** |
| **Durée** | *7 Heures* |
| **Objectifs** | *Les thématiques abordées pour ce tutoriel seront autour de : cyberstratégie d'une organisation, rôle et responsabilités d'une équipe de cybersécurité, gestion de cybermenaces et cybercrises, plan de continuité et de reprise des affaires, collecte des preuves lors d'un cyberincident.* |
| | |
| **Module 3** | **Détection et réponses aux intrusions** |
| **Durée** | *7 Heures +* |
| **Objectifs** | *Les thématiques abordées pour ce tutoriel seront autour de : Détections des intrusions, analyse du flux de trafic, collecte et analyse des évènements, architecture, confinement, phases d'une cyberattaque, ingénierie sociale, hameçonnage, planification des tests d'intrusion* |

| | |
|---|---|
| **Module 4** | **L'intelligence artificielle pour la cybersécurité** |
| **Durée** | *7 Heures +* |
| **Objectifs** | *Après avoir présenté l'IA d'une façon générale, nous allons voir comment l'IA révolutionne la cybersécurité en analysant d'énormes volumes de données afin d'accélérer les temps de réponses et renforcer la gestion opérationnelle et la sécurité des systèmes.* |

## 4. Durée

4 jours
7 Heures/jour

## 5. Coût de la formation

Négociable à la demande.