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 ÎLE-MBAMOU"**

**TITRE : SENSIBILISATION ET DE FORMATION SOUTENUE SUR LA CYBERSÉCURITÉ**

**SYLLABUS FC-ÎM**



## 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.

Les modules composants cette formation :

- Donnent des réponses aux besoins de sécurisation des réseaux et des systèmes informatiques et les applications.
- Aident à développer la culture de sécurité des Systèmes d'Informations en entreprise.
- Permettent de former des acteurs de sécurité des Systèmes d'Informations de haut niveau susceptibles d'intervenir efficacement dans les différents problèmes de sécurité.
- Mettent à la disposition des acteurs de sécurité une formation de qualité sur la cybersécurité dans le but de supporter les activités de l'entreprise avec les outils cybers.



### 1.2 Prérequis pour les étudiants

La formation est ouverte à tous. Néanmoins, les connaissances de base suivantes faciliteront la compréhension des apprenants, 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, …).

## 2. Animateurs

1. **Stanislas NYOKAS** (Animateur principal)
   - Expert et Leader en Cybersécurité
   - Enquêteur Expert en Cybercriminalité
   - Docteur en Mathématiques pures
   - PDG iTM Systems, Londres (Angleterre) [www.itmsystems.net]

2. **Afshin NAEINI**
   - Consultant Technique Senior en criminalistique numérique, iTM Systems, Londres (Angleterre)
3. **Marius Gabin ETA**
   - 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. Programme de la formation

Cette formation est constituée de 10 modules indépendants étalés sur 10 jours.

| | |
|---|---|
| **1er jour** | |
| **Module 1** | ***Formation de sensibilisation à la cybersécurité*** |
| **Durée** | *7 Heures* |
| **Objectifs** | *– Comprendre les notions de base sur la Cybersécurité*<br>*– Comprendre les motivations et le besoin de sécurité des Systèmes d'informations*<br>*– Connaitre les définitions et la typologie des menaces*<br>*– Connaitre la portée et les objectifs de la sécurité informatique.* |
| | |
| **2ème jour** | |
| **Module 2** | ***Fondements de la cybersécurité*** |
| **Durée** | *7 Heures* |
| **Objectifs** | *Ce module de formation se focalise sur les connaissances cyber qu'il faut développer. Il est très pratique, car il démontre la mise en place d'une machine cyber sécurisée pour aider à pratiquer l'art à domicile. Ce cours permet d'apprendre et de comprendre les attaques afin de se protéger concrètement.* |
| | |
| **3ème jour** | |
| **Module 3** | ***Cybersécurité pour les professionnels de l'informatique*** |
| **Durée** | *7 Heures* |
| **Objectifs** | *L'équipe de sécurité d'une entreprise doit être impliquée dans les tests pour voir si le réseau d'une organisation est vulnérable aux attaques extérieures. Celà est essentiel pour renforcer la sécurité du réseau, et c'est l'une des compétences les plus recherchées par tout professionnel de la sécurité informatique.* |
| | |
| **Module 4** | ***Cybersécurité pour les infrastructures critiques*** |
| **Durée** | *7 heures* |
| **Objectifs** | *Ce cours donne des notions très importantes sur la sécurité des infrastructures critiques et les enjeux. Il fait un tour d'horizon de la cybersécurité des infrastructures critiques, recensement des vulnérabilités et classification, menaces et risques, architecture de cybersécurité d'un système utilisé dans les infrastructures critiques.* |
| | |
| **5ème jour** | |
| **Module 5** | ***Cybersécurité avec les nuages (cloud computing)*** |
| **Durée** | *7 heures* |
| **Objectifs** | - *Permettre d'acquérir les connaissances et les compétences nécessaires pour supporter et gérer un Cloud Computing*<br>- *Apprendre les concepts de sécurité cloud nécessaires pour atténuer les menaces sur une entreprise* |

| 6ème jour | |
|---|---|
| **Module 6** | ***Cybersécurité - Énumération du piratage éthique*** |
| **Durée** | *7 heures* |
| **Objectifs** | *Le processus de collecte d'informations sur les ordinateurs et les personnes auxquelles ils appartiennent. Dans ce cours, il sera exposé les concepts, les outils et les techniques derrière l'empreinte : trouver des sites Web connexes, déterminer les informations sur le système d'exploitation et l'emplacement, identifier les utilisateurs via les médias sociaux et les services financiers, suivre les e-mails, etc.* |
| | |
| **7ème jour** | |
| **Module 7** | ***Cybersécurité - Piratage éthique évitant ACL, IDS, HIDS, Pare-feu*** |
| **Durée** | *7 heures* |
| **Objectifs** | *Le piratage éthique - tester pour voir si le réseau d'une organisation est vulnérable aux attaques extérieures - est une compétence recherchée par de nombreux professionnels de la sécurité informatique. Dans ce cours, un expert en cybersécurité vous prépare à faire vos premiers pas dans le test des défenses des clients.* |
| | |
| **8ème jour** | |
| **Module 8** | ***Cybersécurité - Piratage éthique avant l'attaque du périmètre*** |
| **Durée** | *7 heures* |
| **Objectifs** | *Après l'empreinte et la reconnaissance, la numérisation est la deuxième phase de collecte d'informations que les pirates utilisent pour dimensionner un réseau. Les analyses de réseau sont également un outil clé dans l'arsenal des pirates éthiques, qui s'efforcent de prévenir les attaques contre l'infrastructure et les données d'une organisation.* |
| | |
| **9ème jour** | |
| **Module 9** | ***Cybersécurité - Processus d'analyse des logiciels malveillants*** |
| **Durée** | *7 heures* |
| **Objectifs** | *Dans ce cours vous découvrirez les concepts clés associés à l'analyse des programmes malveillants. Vous apprendrez comment les acteurs malveillants attaquent les organisations, les utilisateurs et les terminaux et comment vous pouvez commencer à analyser les artefacts associés à ces attaques.* |
| | |
| **10ème jour** | |
| **Module 10** | ***Cybersécurité - Ethical Hacking, Hacking des serveurs web et applications web*** |
| **Durée** | *7 heures* |
| **Objectifs** | *- Pendant cette formation le participant aura une meilleure compréhension des faiblesses et vulnérabilité des systèmes*<br>*- Aider les organisations à renforcer les contrôles de sécurité de ses systèmes afin de minimiser le risque d'incident.* |



## 4. Durée

10 jours
7 Heures/jour

## 5. Coût de la formation

*Négociable à la demande*