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 MONT NABEMBA"

THÈME : LA CYBERSÉCURITÉ APPLIQUÉE À LA TÉLÉPHONIE MOBILE

SYLLABUS FCMN

Formateur : **Docteur Roch Corneille NGOUBOU**
Administrateur Général du Centre d'Encadrement, Technique, Universitaire et Professionnel (CETUP).
Enseignant des Universités (UMNG, UDSN, CFI-CIRAS).
Site web : www.cetup.pro
Directeur des Services Informatiques et de la Prospective au FONEA

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.

Les modules composant cette formation sont conçus pour fournir une compréhension complète des risques numériques dans le contexte des MSC et développer des compétences pratiques pour évaluer ces risques de manière méthodologique.

1.2 Prérequis pour les apprenants

Les connaissances de base suivantes faciliteront la compréhension des apprenants inscris à cette formation :

i. L'architecture fonctionnelle d'un réseau de communication en particulier le reseau de telephonie mobile
ii. Les systèmes d'informations et leurs architectures fonctionnelles
iii. Connaissances de base sur le fonctionnement technique des réseaux, des systèmes d'exploitation et des applications.
iv. Connaissances sur les protocoles de communication (le modèle OSI, le protocole TCP/IP, etc.)

1.3 Cibles privilégiées

i. Les jeunes diplômés
ii. Les jeunes étudiants
iii. Les professionnels de la téléphonie mobile ou de la télécommunication

2. Programme de la formation

Cette formation est constituée de 3 modules indépendants étalés sur 3 jours.

1. Définition des Concepts Clés

1.1. MSC en Téléphonie Mobile

- **Définition et Fonctionnement** : Introduction aux MSC (Mobile Switching Centers) et leur rôle dans le réseau de téléphonie mobile.
- **Architecture et Composants** : Analyse des composants principaux du MSC, leur fonctionnement et leur intégration dans le réseau.

1.2. Risque Numérique

- **Définition** : Qu'est-ce que le risque numérique ?
- **Identification des Risques** : Comment les risques numériques peuvent impacter les MSC.

1.3. Aléa Numérique

- **Définition** : Qu'est-ce qu'un aléa numérique ?
- **Types d'Aléas** : Analyse des différents types d'aléas numériques et leur impact sur les MSC.

1.4. Vulnérabilité

- **Définition** : Comprendre la vulnérabilité dans le contexte numérique.
- **Identification des Vulnérabilités** : Comment identifier les vulnérabilités spécifiques aux MSC.

1.5. Enjeu Connexe

- **Définition** : Qu'est-ce qu'un enjeu dans le contexte des MSC ?
- **Analyse des Enjeux** : Identification et évaluation des enjeux liés aux MSC.

1.6. Croisement entre Aléa Numérique, Vulnérabilité et Enjeu

- **Méthodologie de Croisement** : Approche méthodologique pour croiser les aléas numériques, les vulnérabilités et les enjeux dans le contexte des MSC.

2. Formulaire d'Identification des Aléas Numériques

2.1. Objectif du Formulaire

- **Identification des Aléas** : Créer un formulaire pour identifier les aléas numériques affectant le MSC d'un opérateur de téléphonie mobile.

2.2. Contenu du Formulaire

- **Détails du MSC** : Informations sur le MSC spécifique.
- **Type d'Aléa** : Catégorisation des aléas numériques.
- **Impact Potentiel** : Évaluation de l'impact potentiel de chaque aléa.

3. Formulaire d'Identification des Vulnérabilités et Enjeux

3.1. Objectif du Formulaire

- **Identification des Vulnérabilités** : Développer un formulaire pour identifier les vulnérabilités et enjeux liés au MSC.

3.2. Contenu du Formulaire

- **Détails du MSC** : Informations sur le MSC spécifique.
- **Type de Vulnérabilité** : Classification des vulnérabilités.
- **Enjeux Connexes** : Analyse des enjeux connexes à chaque vulnérabilité.

4. Modèle Conceptuel des Données

4.1. Intégration des Identifications

- **Conceptualisation des Données** : Développer un modèle conceptuel intégrant les aléas numériques, les vulnérabilités, et les enjeux.

4.2. Croisement des Composantes

- **Approche Méthodologique** : Méthodologie pour croiser aléa numérique, vulnérabilité, et enjeu.
- **Calcul du Risque** : Méthodes pour calculer le risque basé sur le croisement des trois composantes.

5. Indicateurs d'Évaluation du Risque et Variables Composites

5.1. Indicateurs d'Évaluation du Risque

- **Définition des Indicateurs** : Développer des indicateurs pour évaluer le risque numérique.
- **Variables Composites** : Identification et utilisation des variables composites connexes.

5.2. Simulation par Tableur

- **Matrice d'Évaluation des Impact** : Créer une matrice pour évaluer les impacts.
- **Matrice d'Évaluation des Risques** : Créer une matrice pour évaluer les risques numériques.
- **Exercice Pratique** : Utiliser un tableur pour simuler l'évaluation des risques en croisant aléa et vulnérabilité.

3. Durée

La durée de cette formation est de 3 jours, soit un module par jour :

7 Heures/jour

4. Coût de la formation

Nous comptons sur le sponsoring pour que cette formation soit totalement gratuite pour tous les candidats qui seront sélectionnés. Le sponsoring est sensé prendre en ligne de compte les frais pédagogiques, les frais de documentation, les frais du matériel de formation et les frais de déjeuner pendant la formation.