# FICHE TECHNIQUE DE FORMATION
# Introduction à la Cybersécurité

## Objectifs de la Formation:

Comprendre les concepts fondamentaux de la cybersécurité.

Développer des compétences pour identifier et gérer les menaces de cybersécurité.

Maîtriser les principes et les pratiques de base pour sécuriser les systèmes et les données.

## Public Cible:

Responsables IT, administrateurs réseau, développeurs, toute personne souhaitant comprendre les bases de la cybersécurité.

## Prérequis:

Connaissances de base en informatique.

## Méthodologie Pédagogique:

Exposés théoriques, démonstrations pratiques, ateliers interactifs, études de cas.

## Programme de la Formation:

### 1. Introduction à la Cybersécurité

Concepts de Base : Comprendre les principes fondamentaux de la cybersécurité.

Menaces et Attaques : Identification des principales menaces et types d'attaques.

### 2. Mesures de Sécurité

Politiques de Sécurité : Développement de politiques de sécurité de l'information.

Contrôles de Sécurité : Présentation des contrôles de sécurité techniques et organisationnels.

### 3. Sécurisation des Systèmes et Réseaux

Protection des Systèmes : Techniques pour protéger les systèmes d'information.

Sécurisation des Réseaux : Stratégies pour sécuriser les réseaux informatiques.

## 4. Gestion des Identités et des Accès

Gestion des Identités : Techniques pour gérer les identités et les accès.

Authentification et Autorisation : Présentation des méthodes d'authentification et d'autorisation.

## 5. Cryptographie de Base

Concepts de Cryptographie : Introduction aux concepts de cryptographie.

Applications Pratiques : Utilisation de la cryptographie pour sécuriser les données.

## 6. Surveillance et Détection

Outils de Surveillance : Introduction aux outils de surveillance de la sécurité.

Détection des Intrusions : Techniques pour détecter les intrusions et les activités suspectes.

## 7. Réponse aux Incidents

Plan de Réponse aux Incidents : Élaboration d'un plan de réponse aux incidents de sécurité.

Gestion des Incidents : Techniques pour gérer les incidents de cybersécurité.

## 8. Applications Pratiques

Ateliers de Sécurisation : Exercices pratiques pour sécuriser les systèmes et les réseaux.

Simulations de Réponse aux Incidents : Jeux de rôle pour pratiquer la réponse aux incidents.

## 9. Normes et Régulations

Introduction aux Normes : Présentation des normes et régulations en cybersécurité.

Conformité Réglementaire : Techniques pour assurer la conformité avec les régulations.

## 10. Évaluation Finale