Annexe 2 : Les programmes de formation de l'Appel à consultation N°4/2021

Système, Réseau et Sécurité

L'objectif de cette formation **certifiante** est de démontrer une compréhension des principes et des pratiques d'administration de système d'exploitation, des réseaux informatiques et de la sécurité informatique. Cette formation doit aboutir à un niveau professionnel mesurable de compétence opérationnelle dans ces domaines et **doit inclure au minimum** le programme ci-dessous :

I. Concepts de base des systèmes d'exploitation (5 jours)

1. Le système d'exploitation
2. Rôles, typologie, évolution
3. Architecture et composants de base
4. Virtualisation et conteneurisation

II. Administration du système d'exploitation : Niveau I (5 jours)

1. La ligne de commande
2. Le système de fichier : gestion et traitement
3. Installation et configuration de composants et de services
4. Gestion des processus
5. Gestion des utilisateurs et des groupes
6. Journalisation et résolution des problèmes
7. Prise de commande à distance

III. Administration du système d'exploitation : Niveau II (10 jours)

1. Optimisation des performances
2. Contrôle d'accès et sécurisation du système
3. Gestion de la connectivité réseau
4. Gestion avancée du stockage
5. Installation et contrôle des systèmes
6. Introduction aux conteneurs
7.

IV. Concepts de base des réseaux informatiques (5 jours)

1. Les réseaux de transmission de données
2. Typologie des réseaux
3. Terminologie et notion fondamentales

V. Administration du réseaux informatiques : Niveau I (5 jours)

1. Couches et protocoles
2. Réseaux locaux
3. Configuration : terminaux, commutateurs et routeurs
4. Adressage IPv4 et IPv6
5. Diagnostique et bonnes pratiques

VI. Administration du réseaux informatiques : Niveau II (10 jours)

1. VLAN : Configuration et routage
2. Commutation avancée
3. Adressage dynamique
4. Routage statique
5. Sécurité, diagnostique et bonnes pratiques

VII. Concepts de base de la sécurité informatique (5 jours)

1. Terminologie et notion fondamentales
2. Typologie des menaces, des vulnérabilités
3. Exemple d'attaques

VIII. Cybersécurité : Niveau I (10 jours)

1. Environnement sécurisé
2. Analyse sécuritaire système d'exploitation et réseau
3. Les outils de surveillance, d'alerte et de protection
4. Analyse d'attaques
5. Cryptographie

Analyste Test & Validation

L'objectif de cette formation **certifiante** est de démontrer une compréhension des principes et des pratiques de base des tests logiciels. Cette formation doit aboutir à un niveau professionnel de compétence dans les principes et les pratiques des tests logiciels dans le domaine IT et doit **inclure au minimum** le programme ci-dessous :

I. Concepts de base

1. La production du logiciel
2. Le processus du test
3. La typologie des tests
4. Les techniques d'élaboration d'un test
5. Élaboration d'un rapport de test

II. Élaboration d'un cas de test

1. Boite noire
2. Boite blanche

III. Exécution d'un cas de test

1. Environnement de test
2. Exécution du test
3. Détection des anomalies
4. Enregistrement et reproduction des résultats

IV. Type et outils de tests

1. Test unitaire
2. Test REST
3. Test simulé
4. Automatisation des tests

V. Tests de la sécurité applicative

1. Authentification et Autorisation

VI. Tests de performance

1. Indicateurs de performance
2. Monitoring
3. Analyse