Email: info@isisec.net Tel: 25380845 / 60502222 Site Web: www.isisec.net

ISISEC

CALENDRIER ET COUT DES FOEMATIONS

INTITULE DE LA FORMATION	COUT (FCFA)		PERIODE
	PARTICULIER	ENTREPRISE	
CCNA V7	300 000	600 000	DU 01 AOUT AU 30 NOV 2022
CYBERSECURITY ESSENTIAL	150 000	300 000	DU 18 AOUT AU 17 SEPT 2022
			DU 22 SEPT AU 22 OCT 2022
CYBERSECURITY OPS	300 000	600 000	DU 12 AOUT AU 04 NOV 2022

FORMATION CCNAv7.0

DESCRIPTION DU COURS

Le programme **CCNAv7** donne accès au métier de technicien réseau et permet de débuter une carrière dans l'informatique. La formation comporte trois modules : Introduction aux réseaux ; Commutation, routage et réseaux sans fil ; Réseaux d'entreprises, Sécurité et l'automatisation. Cette formation prépare à la certification CCNA (code de l'examen : 200-301).

OBJECTIFS

- Développez des connaissances pratiques sur les applications, les protocoles et les services de routage, de commutation et de réseau
- Étudiez avec un instructeur en classe et accédez à du contenu spécialisé en ligne à tout moment.

- Mettez en pratique ce que vous apprenez en utilisant de vrais équipements et l'outil de simulation de configurations réseau Cisco Packet Tracer.
- Recevez des commentaires immédiats sur votre travail en répondant aux questionnaires et aux tests intégrés.
- Préparez-vous pour le marché du travail avec des présentations et des projets collaboratifs
- Rejoignez la communauté internationale Cisco Networking Academy.

PRE-REQUIS

Connaissance de base des réseaux informatiques

DÉROULEMENT DE LA FORMATION

- **Période : Du 01 Aout 2022 au 30 Novembre 2022**
- **Durée :**
  - ✓ **4 Mois**
  - ✓ **3 jours / Semaine**
  - ✓ **3H / Jour (Lun, Mar, Mer)**
  - ✓ **Session de Soir : 18h00 – 21h00**
  - ✓ **Volume horaire total : Au moins 300 H**
  - ✓ **Volume Horaire présentiel : Au moins 180 H**
- **Langue :**
  - ✓ **Cours avec instructeur : FRANÇAIS**
  - ✓ **Support du cours et examens sur la plateforme : FRANÇAIS**

CONTENU

MODULE 1 : CCNA 1 v7.0 : INTRODUCTION AUX RÉSEAUX

CHAPITRE 1 : CONNECTIVITE ET COMMUNICATION D'UN RESEAU DE BASE

- Le résautage de nos jours
- Configuration de base des commutateurs et périphériques finaux
- Protocoles et modèles

CHAPITRE 2 : CONCEPTS ETHERNET

- Couche physique
- Systèmes de nombres
- Couche de liaison de données
- Commutation Ethernet

CHAPITRE 3 : COMMUNICATION ENTRE RESEAUX

- Couche réseau
- Résolution d'adresse
- Configuration de base du routeur

CHAPITRE 4 : ADRESSAGE IP

- Adressage IPv4
- Adressage IPv6
- Protocole ICMP

CHAPITRE 5 : COMMUNICATION DES APPLICATIONS

- Couche transport
- Couche application

CHAPITRE 6 : CONCEPTION ET SECURISATION D'UN PETIT RESEAU

- Fondamentaux de la sécurité réseau
- Concevoir un petit réseau

MODULE 2 : CCNA 2 V7.0 : COMMUTATION, ROUTAGE ET RÉSEAUX SANS FIL

CHAPITRE 1 : CONCEPTS DE COMMUTATION, VLANS ET ROUTAGE INTER-VLANS

- Configuration de base du commutateur
- Concepts de commutation
- VLANs
- Routage inter-VLAN

CHAPITRE 2 : RÉSEAUX REDONDANTS

- Protocole STP
- EtherChannel

CHAPITRE 3 : RÉSEAUX FIABLES ET DISPONIBLES

- DHCPv4
- Concepts SLAAC et DHCPv6
- Concepts FHRP

CHAPITRE 4 : SÉCURITÉ DE COUCHE 2 ET RÉSEAUX LOCAUX SANS FIL

- Concepts de sécurité LAN
- Configuration de la sécurité du commutateur
- Concepts de réseaux locaux sans fil
- Configuration de réseaux locaux sans fil

CHAPITRE 5 : CONCEPTS DE ROUTAGE ET CONFIGURATION

- Concepts de routage
- Routage statique IP
- Dépanner les routes statique et par défaut

MODULE 3 : CCNA 3 V7.0 : RÉSEAUTAGE D'ENTREPRISE, SÉCURITÉ ET AUTOMATISATION

CHAPITRE 1 : CONCEPTS OSPF ET CONFIGURATION

- Concepts OSPFv2 à zone unique
- Configuration OSPFv2 à zone unique

CHAPITRE 2 : SÉCURITÉ RÉSEAU

- Concepts de sécurité réseau
- Concepts ACL
- Configuration des ACL pour IPv4

CHAPITRE 3 : CONCEPTS WAN

- NAT pour IPv4
- Concepts WAN
- Concepts VPN et IPSec

CHAPITRE 4 : OPTIMISER, SURVEILLER ET DÉPANNER LES RÉSEAUX

- Concepts de qualité de service (**QoS**)
- Gestion réseau
- Conception réseau
- Dépannage réseau (**Network Troubleshooting**)

CHAPITRE 5 : TECHNOLOGIES DES RÉSEAUX ÉMERGENTS

- Virtualisation réseau
- Automatisation réseau

Coût de la formation :

- **Particulier :** **300 000 FCFA (100 000 FCFA par module)**
- **Entreprise :** 600 000 **FCFA**

Pour tout autre renseignement, veuillez contacter le 6**0502222/70399911/25380845** ou par mail à **info@isisec.net**.

CYBERSECURITY ESSENTIALS

DESCRIPTION DU COURS

Le cours Cybersecurity Essentials développe une compréhension de base de la cybersécurité et explique en quoi elle est liée à la sécurité de l'information et du réseau. Le cours présente aux participants les caractéristiques des délits informatiques, les principes de sécurité ainsi que les technologies et les procédures pour protéger les réseaux. Grâce à des contenus interactifs et multimédias, à des activités pratiques et à des études de cas du secteur, les étudiants créent des compétences techniques et commerciales pour poursuivre des carrières dans la cybersécurité.

- Découvrez les procédures pour mettre en œuvre la confidentialité, l'intégrité, la disponibilité et les contrôles de sécurité sur des réseaux, des serveurs et des applications.
- Apprenez les principes de sécurité et comment développer des politiques de sécurité conformes aux lois de la cybersécurité.
- Appliquez des compétences par la pratique, en utilisant les TP et les activités de Cisco Packet Tracer.
- Recevez des commentaires immédiats sur votre travail en répondant aux questionnaires et aux tests intégrés

DÉROULEMENT DE LA FORMATION

- **Période : 1ere session: Du 18 Aout au 17 Sept 2022**
  2eme session : Du 22 Sept au 22 Oct 2022
- **Durée**
  - ✓ **1 Mois**
  - ✓ **2 jours / Semaine (Jeudi et Samedi)**
  - ✓ **Cours du Soir : Jeudi 18h00 – 21h00**
    Samedi 15H00 – 18H00

- **Langue**
  - **Cours avec instructeur : FRANCAIS**
  - **Support sur la plateforme CISCO : FRANCAIS**
  - **Tests et examens sur la plateforme CISCO : FRANCAIS**

CONTENU

CHAPITRE 1 : UN UNIVERS DE MAGICIENS, DE HEROS ET DE CRIMINELS

- Le monde de la cybersécurité
- Cybercriminels contre professionnels de la cybersécurité
- Menaces envers le royaume
- Les forces obscures de la cybersécurité
- Augmenter le nombre de héros

CHAPITRE 2 : LE CUBE MAGIQUE DE LA CYBER SECURITE

- Le cube magique de la cyber sécurité
- LA TRIADE CID
- Les états des données
- Les mesures de cyber sécurité
- Le cadre de gestion de la sécurité IT

CHAPITRE 3 : MALWARES ET CODES MALVEILLANTS

- Malwares et codes malveillants
- La supercherie
- Les attaques

CHAPITRE 4 : L'ART DE PROTEGER DES SECRETS

- La cryptographie
- Le contrôle d'accès
- La dissimulation des données

CHAPITRE 5 : L'ART D'ASSURER L'INTÉGRITÉ

- Les types de contrôles de l'intégrité des données
- Les signatures numériques
- Les certificats
- Protection de l'intégrité des bases de données

CHAPITRE 6 : LE ROYAUME DES CINQ NEUF

- La haute disponibilité
- Les mesures pour améliorer la disponibilité
- Gestion des incidents
- Reprise après sinistre

CHAPITRE 7 : FORTIFIER LE ROYAUME

- Protéger les systèmes et les périphériques
- Le renforcement du serveur
- Le renforcement du réseau
- Sécurité physique

CHAPITRE 8 : DEVENIR SPECIALISTE DE LA CYBERSECURITE

- Les domaines de la cybersécurité
- Comprendre le serment lié à l'adhésion
- Étape suivante

MATÉRIELS DE TRAVAUX PRATIQUE :

Matériels **CISCO**

Coût de la formation :

- **Particulier :** 150.000 F cfa
- **Entreprise :** 300.000 F cfa

Pour tout autre renseignement, veuillez contacter le **25380845 / 60502222** ou par mail à info@isisec.net.

Une attestation est délivrée à la fin de la formation en cas de validation.

Email: info@isisec.net Tel: 25380845 / 60502222 Site Web: www.isisec.net

CYBERSECURITY OPERATIONS

(CyberOps Associate)

DESCRIPTION DU COURS

Les organisations d'aujourd'hui sont mises au défi de détecter rapidement les violations de la cybersécurité et de répondre efficacement aux incidents de sécurité. Des équipes de personnes dans les centres d'opérations de sécurité (SOC) surveillent de près les systèmes de sécurité, protégeant leurs organisations en détectant et en réagissant aux menaces de cybersécurité. Cyber Ops Associate prépare les candidats à débuter une carrière en travaillant avec des analystes de cybersécurité de niveau associé au sein des centres d'opérations de sécurité.

PRE-REQUIS

- Connaissance de base des systèmes d'exploitation informatiques, tels que Windows et Linux.

DÉROULEMENT DE LA FORMATION

- **Période : Du 12 Aout Au 04 Nov 2022**
- **Durée**

  - ✓ **2 jours / Semaine (Vendredi et Samedi)**
  - ✓ **3H / Jour**
  - ✓ **Cours du Soir : 18h00 – 21h00**
  - ✓ **Volume Horaire presentiel: Au moins 70 H**
  - ✓ **Volume Horaire total: Au moins 240 H**

CONTENU

CHAPITRE 1 : LE DANGER

- ❖ Histoires de guerre
- ❖ Acteurs de la menace
- ❖ Impact de la menace

CHAPITRE 2 : DES COMBATTANTS DANS LA GUERRE CONTRE LA CYBERCRIMINALITE

- ❖ Le centre des opérations de sécurité moderne
- ❖ Devenir un défenseur

CHAPITRE 3 : SYSTÈME D'EXPLOITATION WINDOWS

- ❖ Historique de Windows
- ❖ Architecture et opérations Windows
- ❖ Configuration et surveillance Windows
- ❖ Sécurité Windows

Email: info@isisec.net Tel: 25380845 / 60502222 Site Web: www.isisec.net

CHAPITRE 4: SYSTEME D'EXPLOITATION LINUX

- Bases de Linux
- Travailler dans le shell Linux
- Serveurs et clients Linux
- Administration de base du serveur
- Le système de fichiers Linux
- Travailler dans l'interface graphique Linux
- Travailler sur un hôte Linux

CHAPITRE 5 : PROTOCOLES RESEAUX

- Processus de communication réseau
- Protocoles de communication
- Encapsulation de données

CHAPITRE 6 : ETHERNET ET PROTOCOLE IP

- Ethernet
- IPv4
- Principes de base de l'adressage IP
- Types d'adresses IPv4
- La passerelle par défaut
- IPv6

CHAPITRE 7 : VERIFICATION DE LA CONNECTIVITE

- ICMP
- Utilitaires Ping et Traceroute

CHAPITRE 8 : PROTOCOLE DE RESOLUTION D'ADRESSE

- MAC et IP

- ARP
- Problèmes ARP

CHAPITRE 9 : LA COUCHE TRANSPORT

- Caractéristiques de la couche de transport
- Etablissement de session de couche de transport
- Fiabilité de la couche de transport

CHAPITRE10 : SERVICES RESEAUX

- DHCP
- DNS
- NAT
- Services de transfert et de partage de fichiers
- Email
- HTTP

CHAPITRE 11 : LES APPAREILS DE COMMUNICATION RESEAU

- Périphériques réseau
- Communications sans fil

CHAPITRE 12 : L'INFRASTRUCTURE DE SECURITE DU RESEAU

- Topologies de réseau
- Dispositif de sécurité
- Services de sécurité

CHAPITRE 13 : LES HACKERS ET LEURS OUTILS

- Qui attaque notre réseau ?
- Outils d'acteur de menace

CHAPITRE 14 : LES ATTAQUES ET LES MENACES FREQUENTES

- Malware
- Attaques de réseau courantes - Reconnaissance, accès et ingénierie sociale
- Attaques réseau - déni de service, débordements de tampon et évasion

CHAPITRE 15 : MONITORING DU RESEAU ET LES OUTILS

- Introduction à la surveillance du réseau
- Introduction aux outils de surveillance du réseau

CHAPITRE 16 : ATTAQUER LA FONDATION

- Détails du PDU IP
- Vulnérabilités IP
- Vulnérabilités TCP et UDP

CHAPITRE 17 : ATTAQUER CE QUE NOUS FAISONS

- Services IP
- Services aux entreprises

CHAPITRE 18 : COMPRENDRE LES MECANISMES DE DEFENSE

- Defense en profondeur
- Politiques, réglementations et normes de sécurité

CHAPITRE 19 : CONTRÔLE D'ACCÈS

- Concepts de contrôle d'accès
- Utilisation et fonctionnement AAA

CHAPITRE 20 : THREAT INTELLIGENCE

- Sources d'informations
- Services Threat Intelligence

CHAPITRE 21 : LA CRYPTOGRAPHIE

- Intégrité et authenticité
- Confidentialité
- Cryptographie à clé publique
- Autorités et système de confiance PKI
- Applications et impacts de la cryptographie

CHAPITRE 22 : PROTECTION DES TERMINAUX

- Protection antimalware
- Prévention des intrusions basée sur l'hôte
- Sécurité des applications

CHAPITRE 23 : ÉVALUATION DE LA VULNERABILITE DES TERMINAUX

- Profilage de réseau et de serveur
- Système commun de notation des vulnérabilités (CVSS)
- Gestion sécurisée des appareils
- Systèmes de gestion de la sécurité de l'information

CHAPITRE 24 : LES TECHNOLOGIES ET LES PROTOCOLES

- Surveillance des protocoles communs
- Technologies de sécurité

CHAPITRE 25 : DONNEES DE SECURITE RESEAU

- Types de données de sécurité
- Journaux des terminaux
- Journaux réseau

CHAPITRE 26 : ÉVALUATION DES ALERTES

- Source d'alertes
- Vue d'ensemble de l'évaluation des alertes

CHAPITRE 27 : UTILISATION DES DONNEES DE SECURITE DU RESEAU

- Une plateforme de données commune
- Investigation sur les données du réseau
- Amélioration du travail de l'analyste en cybersécurité

CHAPITRE 28 : DIGITAL FORENSICS ET ANALYSE ET REPONSE AUX INCIDENTS

- Gestion des preuves et attribution d'attaque
- La chaîne Cyber Kill
- Le modèle diamant de l'analyse des intrusions
- Réponse aux incidents

Coût de la formation :

- **Particulier :** 300.000 F cfa
- **Entreprise :** 600.000 F cfa

Modalité de paiement particulier

INTITULE de la Formation	Modalité
CCNA CyberSecurity Operations	▪ Premier versement : **100.000 F cfa** ▪ Deuxième : **100.000 F cfa** ▪ Troisième : **100.000 F cfa**

NB : les paiements des tranches se feront à la fin de chaque mois

Pour tout autre renseignement veuillez contacter le ***25380845 / 60502222*** ou par mail à **info@isisec.net**.

Une attestation est délivrée à la fin de la formation en cas de validation.