CISCO

CCNA CYBERSECURITY OPERATIONS

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. CCNA Cyber Ops 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.

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

DEROULEMENT DE LA FORMATION

- **Période : Du 24 Mai au 20 Juillet 2019**
- **Durée**
  - ✓ **2 Mois**
  - ✓ **2 jours / Semaine (Vendredi et Samedi)**
  - ✓ **3H / Jour**
  - ✓ **6H / Semaine**
  - ✓ **Cours du Soir : 18h30 – 21h30**
- **Langue**
  - **Cours avec instructeur : FRANCAIS**
  - **Support sur la plateforme CISCO : FRANCAIS**
  - **Tests et examens sur la plateforme CISCO : FRANCAIS**

CONTENU

CHAPITRE 1 : CYBERSECURITE ET CENTRE OPERATIONNEL DE SECURITE

- ❖ Le danger
- ❖ Des combattants dans la guerre contre la cybercriminalité

CHAPITRE 2 : SYSTEME D'EXPLOITATION WINDOWS

- ❖ Vue d'ensemble de Windows
- ❖ Administration de Windows

CHAPITRE 3 : SYSTEME D'EXPLOITATION LINUX

- ❖ Vue d'ensemble de Linux
- ❖ Administration de Linux
- ❖ Hôtes Linux

CHAPITRE 4 : PROTOCOLES ET SERVICES RESEAU

- Protocoles réseau
- Ethernet et protocole IP
- Vérification de la connectivité
- Protocole de résolution d'adresse

CHAPITRE 5 : L'INFRASTRUCTURE DE RESEAU

- Les appareils de communication réseau
- L'infrastructure de sécurité du réseau
- Les représentations du réseau

CHAPITRE 6 : PRINCIPES DE SECURITE DU RESEAU

- Les hackers et leurs outils
- Les attaques et les menaces fréquentes

CHAPITRE 7 : TOUT SAVOIR SUR LES ATTAQUES RESEAU

- Les hackers et leurs outils
- Attaques ciblant les fondements du réseau
- Attaques ciblant les activités

CHAPITRE 8 : PROTECTION DU RESEAU

- Comprendre les mécanismes de défense
- Le contrôle d'accès
- La Threat Intelligence

CHAPITRE 9 : LA CRYPTOGRAPHIE ET L'INFRASTRUCTURE A CLE PUBLIQUE

- La cryptographie
- L'infrastructure à clé publique

CHAPITRE 10 : ANALYSE ET SECURITE DES TERMINAUX

- Protection des terminaux
- Profilage du réseau et du serveur

CHAPITRE 11 : SURVEILLANCE DE LA SECURITE

- Les technologies et les protocoles
- Les fichiers journaux

CHAPITRE 12 : ANALYSE DES DONNEES RELATIVES AUX INTRUSIONS

- Évaluation des alertes
- Utilisation des données de sécurité du réseau
- Investigation numérique

CHAPITRE 13 : LA GESTION DES INCIDENTS

- Modèles de gestion des incidents
- Équipes CSIRT et NIST 800-61r2

TRAVAUX PRATIQUES

TP1 : Tout savoir sur les attaques

TP2 : Identifier les processus en cours d'exécution

TP3 : Découvrir les processus, les threads, les handles et le Registre Windows

TP4: Utiliser Windows PowerShell

TP5: Utilisation outils avancés de Windows

TP6 : Serveurs Linux

TP7 : Utilisation de Wireshark

TP8 : Découvrir NMAP

TP9 : Attaquer une base de données mySQL

TP10 : Consulter les journaux du serveur

TP11 : Règles Snort et de pare-feu

TP12 : Extraire un fichier exécutable d'une capture PCAP

TP13 : Interpréter les données HTTP et DNS pour isoler le cybercriminel

TP14 : Isoler un hôte compromis en utilisant un quintuplé

TP15 : Gestion des incidents

ETUDES DE CAS

Études de cas relatives à la cybersécurité

MATERIELS DE TRAVAUX PRATIQUE :

Matériels **CISCO**

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** ▪ Deuxième : **100.000 F** ▪ Troisième : **100.000 F**

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.

Personne responsable :

MOUMOUNI ABOU Mahaman Laoual
62 10 68 67
77 09 30 55 (**Whatsapp**)