

**CISCO**

## 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 débiter 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.

## DEROULEMENT DE LA FORMATION

🚩 Période : **Du 17 Septembre Au 16 Décembre 2021**

🚩 Durée

- ✓ 3 Mois
- ✓ 2 jours / Semaine (Vendredi et Samedi)
- ✓ 3H / Jour
- ✓ Cours du Soir : 18h30 – 21h30

## 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 : SYSTEME D'EXPLOITATION WINDOWS

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

### 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

### CHAPITRE 10 : 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 évacion

### 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

- ❖ Défense en profondeur
- ❖ Politiques, réglementations et normes de sécurité

## CHAPITRE 19 : CONTROLE D'ACCES

- ❖ 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
CyberSecurity Operations	<ul style="list-style-type: none"><li>▪ Premier versement : <b>100.000 F cfa</b></li><li>▪ Deuxième : <b>100.000 F cfa</b></li><li>▪ Troisième : <b>100.000 F cfa</b></li></ul>

***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](mailto:info@isisec.net).

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