Understanding Cisco Cybersecurity Operations Fundamentals

Durée: 180 Jours **Réf de cours: CBROPS** **Version: 1.2** **Méthodes d'apprentissage: E-learning**

Résumé:

Le cours **Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)** est conçu pour former les analystes en cybersécurité de niveau débutant à travailler dans un centre d'opérations de sécurité (SOC). Il prépare également à la certification **Cisco Certified CyberOps Associate**..
Apprentissage en ligne
Contenu interactif à son propre rythme qui offre une flexibilité en termes de rythme, de lieu et de temps pour répondre aux besoins des individus et des organisations. Ces ressources comprennent également des livres en ligne, des podcasts et vodcasts éducatifs, ainsi que l'apprentissage par vidéo.

Ce cours vaut 30 crédits de formation continue (CE) pour la recertification.
Mise à jour : 25.06.2025

Public visé:

Ce cours est destiné à un analyste en cybersécurité de niveau associé travaillant dans un centre d'opérations de sécurité (SOC).

Objectifs pédagogiques:

- A l'issue de cette formation, les participants seront en mesure de :
- Comprendre le fonctionnement d'un SOC et les rôles d'un analyste de niveau 1.
- Identifier les vecteurs d'attaque courants, les activités malveillantes et les comportements suspects.
- Utiliser les outils de surveillance de la sécurité réseau (NSM).
- Analyser les incidents de sécurité et utiliser un playbook SOC.
- Comprendre les systèmes d'exploitation Windows et Linux.
- Appliquer les concepts de cryptographie, de sécurité cloud et de normalisation des événements

Pré-requis:

Les participants doivent remplir les conditions préalables suivantes :

- Familiarité avec les réseaux Ethernet et TCP/IP
- Connaissance pratique des systèmes d'exploitation Windows et Linux
- Familiarité avec les concepts de base de la sécurité des réseaux
- CCNA - Mettre en oeuvre et administrer des solutions réseaux Cisco

Test et certification

Recommandé comme préparation aux examens suivants :

200-201 - CBROPS Comprendre les principes fondamentaux des opérations de cybersécurité de Cisco

Après cette formation, nous vous conseillons le(s) module(s) suivant(s):

- CBRCOR - Performing CyberOps Using Cisco Security Technologies
- CBRTHD - Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps

Contenu:

Fondamentaux du SOC

- Rôles
- Outils
- Automatisation
- Indicateurs de performance

Systèmes d’exploitation

- Architecture
- Commandes
- Services et sécurité sous Windows et Linux.

Technologies de sécurité des terminaux

- Antivirus
- Pare-feu
- Sandboxing
- Détection comportementale.

Attaques TCP/IP

- Spoofing
- DoS/DDoS
- Attaques ARP
- Vulnérabilités ICMP/TCP/UDP.

Cryptographie

- Hachage
- Chiffrement
- Intégrité des données.

Sécurité cloud

- Modèles de déploiement
- IAM
- Conformité.

Analyse d’incidents

- Kill chain
- Modèles de diamant
- Chasse aux menaces.

Corrélation et normalisation des événements

- Collecte et analyse de journaux
- PCAPs
- Alertes.

Travaux pratiques

- Analyse de trafic
- Investigation d’attaques
- Utilisation de Security Onion

Méthodes pédagogiques :

Les participants réalisent un test d'évaluation des connaissances en amont et en aval de la formation pour valider les connaissances acquises pendant la formation.
Un support de cours officiel sera remis aux stagiaires au format électronique.

Pour profiter pleinement du support électronique dès le 1er jour, nous invitons les participants à se munir d'un PC ou d'une tablette, qu’ils pourront connecter en WiFi dans nos locaux de Rueil, Lyon ou nos agences en régions.