Comprendre les principes fondamentaux des opérations de cybersécurité de Cisco (CBROPS)

Description

Comprendre les principes fondamentaux des opérations de cybersécurité de Cisco

Le cours « Comprendre les principes fondamentaux des opérations de cybersécurité de Cisco (CBROPS) » est conçu pour vous fournir les compétences essentielles en matière de sécurité réseau. En vous plongeant dans l'analyse des menaces, vous apprendrez à identifier, enquêter et répondre efficacement aux cyberattaques. Grâce à des exercices pratiques et à une formation complète, vous maîtriserez les outils et les concepts clés pour garantir la sécurité des infrastructures critiques.

Destiné aux analystes en cybersécurité travaillant dans un centre d'opérations de sécurité (SOC), ce cours vous donnera toutes les bases nécessaires pour comprendre et gérer les cybermenaces. Vous découvrirez également les techniques d'analyse des incidents, les méthodes de corrélation d'événements, et les processus de normalisation des données. Ce cours est une étape essentielle pour ceux qui souhaitent se spécialiser dans le domaine de la cybersécurité et passer la certification Cisco Certified CyberOps Associate.

Contenu du cours
Module 1 : Définir le centre d'opérations de sécurité

- Comprendre les rôles et responsabilités d'un SOC
- Identifier les types de SOC

Module 2 : Comprendre les outils de surveillance de l'infrastructure et de la sécurité du réseau

- Utiliser les outils de NSM
- Analyser les données réseau

Module 3 : Explorer les catégories de types de données

- Classer les types de données utilisées dans un SOC

Module 4 : Comprendre les concepts de base de la cryptographie

- Utiliser les techniques de cryptographie

Module 5 : Comprendre les attaques TCP/IP courantes

- Identifier les failles de sécurité

Module 6 : Comprendre les technologies de sécurité des points finaux

- Protéger les terminaux

Module 7 : Comprendre l'analyse des incidents dans un SOC centré sur les menaces

- Analyser les incidents de sécurité

Module 8 : Identifier les ressources pour la chasse aux cybermenaces

- Chasser les menaces cybernétiques

Module 9 : Comprendre la corrélation et la normalisation des événements

- Corréler et normaliser les données de sécurité

Module 10 : Identifier les vecteurs d'attaque courants

- Comprendre les schémas de comportement des cyberattaques

Module 11 : Mener des enquêtes sur les incidents de sécurité

- Explorer les Playbooks SOC

Module 12 : Comprendre les bases du système d'exploitation Windows et Linux

- Explorer les systèmes Windows et Linux dans un SOC

Lab / Exercices

- Configurer l'environnement initial du laboratoire de collaboration
- Utiliser les outils NSM pour analyser les catégories de données
- Explorer les technologies cryptographiques
- Explorer les attaques TCP/IP
- Explorer la sécurité des points finaux
- Étudier la méthodologie des pirates
- Chasse au trafic malveillant
- Corréler les journaux d'événements, les PCAP et les alertes d'une attaque
- Enquêter sur les attaques par navigateur
- Analyser les activités DNS suspectes
- Explorer les données de sécurité à des fins d'analyse
- Enquêter sur les activités suspectes à l'aide de Security Onion
- Enquêter sur les menaces persistantes avancées
- Explorer les Playbooks SOC
- Explorer le système d'exploitation Windows
- Explorer le système d'exploitation Linux

Documentation

- Support de cours numérique inclus

Profils des participants

- Analystes en cybersécurité
- Techniciens en réseaux et sécurité
- Administrateurs systèmes
- Professionnels IT souhaitant se spécialiser en cybersécurité

Connaissances Préalables

- Connaissances en réseaux TCP/IP
- Compétences en systèmes d'exploitation Windows et Linux
- Notions de sécurité réseau
- Connaissance des outils de surveillance réseau

Objectifs

- Définir le rôle d'un SOC
- Utiliser les outils de surveillance des réseaux
- Analyser les données réseau pour détecter les menaces
- Comprendre les bases de la cryptographie
- Identifier et corréler les événements de sécurité
- Mener des enquêtes sur les cyberattaques

Description
Formation Comprendre les principes fondamentaux des opérations de cybersécurité de Cisco (CBROPS)
Niveau
Intermédiaire
Prix de l'inscription en Présentiel (CHF)
4350
Prix de l'inscription en Virtuel (CHF)
4350
Durée (Nombre de Jours)
5
Reference
CBROPS