Exécuter les CyberOps en utilisant les technologies de sécurité de Cisco (CBRCOR)

Description

Une formation clé pour maîtriser la sécurité des CyberOps

La formation **“Exécuter les CyberOps en utilisant les technologies de sécurité de Cisco (CBRCOR)”** vous offre une opportunité unique d’approfondir vos connaissances en cybersécurité. À travers ce cours, vous apprendrez à gérer et à automatiser les opérations de sécurité dans un environnement SOC. Cette formation vous prépare à l’examen **CBRCOR** et vous donne accès aux dernières technologies de sécurité de Cisco. Avec des scénarios pratiques, vous serez formé pour devenir un véritable expert en réponse aux incidents et en gestion des cybermenaces.

Une expertise adaptée à votre carrière en cybersécurité

Grâce à cette formation, vous développerez les compétences nécessaires pour analyser des menaces complexes et proposer des solutions adaptées aux environnements d’entreprise modernes. En mettant l’accent sur les outils tels que Cisco Firepower et Cisco SecureX, cette formation vous permet de mieux comprendre et réagir face aux cyberattaques. Un programme complet qui vous aidera à exceller en tant qu’analyste SOC. N’attendez plus, et faites le pas vers un futur prometteur en cybersécurité.

Reference
CBRCOR
Contenu du cours
Module 1 : Gestion des risques et opérations SOC

- Comprendre les processus analytiques et les playbooks
- Analyser les captures de paquets et l'analyse du trafic
- Évaluer les risques de sécurité et les menaces dans un SOC

Module 2 : Analyse des logs des terminaux et appliances

- Comprendre les responsabilités de sécurité dans le cloud
- Analyser les journaux des terminaux et des appliances
- Surveiller les actifs de l'environnement d'entreprise

Module 3 : Threat Tuning et renseignement sur les menaces

- Implémenter le Threat Tuning dans un environnement SOC
- Pratiques avancées de recherche et de renseignement sur les menaces
- Comprendre et utiliser les API pour la cybersécurité

Module 4 : Sécurité SOC et rapports analytiques

- Analyser la sécurité d'un réseau et produire des rapports
- Notions de base sur les logiciels malveillants (Malware Forensics)
- Effectuer une chasse proactive aux menaces

Module 5 : Enquête sur les incidents et réponse

- Investiguer des incidents en utilisant les outils SIEM et SOAR
- Répondre aux incidents en suivant les bonnes pratiques SOC
- Déterminer les indicateurs de compromission (IOC) et les indicateurs d'attaque (IOA)

Lab / Exercices

- Explorer l'orchestration Cisco SecureX
- Explorer les Playbooks Splunk Phantom
- Examiner les captures de paquets de Cisco Firepower et l'analyse PCAP
- Valider une attaque et déterminer la réponse à l'incident
- Soumettre un fichier malveillant à Cisco Threat Grid pour analyse
- Explorer la politique de contrôle d'accès de Cisco Firepower NGFW et les règles Snort
- Suivre les TTP d'une attaque réussie en utilisant un TIP
- Interroger Cisco Umbrella à l'aide du client API Postman
- Corriger un script d'API Python
- Créer des scripts de base Bash
- Reverse Engineering d'un logiciel malveillant

Documentation

- Support de cours numérique inclus

Examen

- Cette formation prépare à l'examen de base 350-201 CBRCOR

Profils des participants

- Ingénieur en cybersécurité
- Investigateur en cybersécurité
- Gestionnaire d’incidents
- Analyste SOC niveau débutant
- Ingénieur réseau avec expérience en sécurité

Connaissances Préalables

- Connaissance de base des environnements UNIX/Linux
- Familiarité avec Splunk et ses fonctions de recherche
- Connaissance des langages de scripts tels que Python ou JavaScript
- Compréhension des concepts de cybersécurité
- Expérience dans l’analyse de logs et de journaux réseau

Objectifs

- Configurer les outils et plateformes SOC
- Utiliser des playbooks pour la réponse aux incidents
- Analyser les menaces avec Cisco Firepower
- Comprendre les modèles de déploiement SecDevOps
- Appliquer l'automatisation avec Cisco SecureX
- Interpréter et analyser les logs réseau

Description
Exécuter les CyberOps en utilisant les technologies de sécurité de Cisco (CBRCOR)
Niveau
Intermédiaire
Prix de l'inscription en Présentiel (CHF)
4350
Prix de l'inscription en Virtuel (CHF)
4350
Durée (Nombre de Jours)
5