Les fondamentaux des opérations de cybersécurité de Cisco (CBROPS 200-201)

Date et durée

Code formation : CBROPS
Durée : 5 jours
Nombre d'heures : 35 heures

Formation avec préparation à la certification

CyberOps Associate®

Description

Les menaces informatiques deviennent de plus en plus complexes, sournoises et récurrentes. Ainsi, il est essentiel pour toute entreprise de pouvoir compter sur des **spécialistes de la cybersécurité**. Que ce soit **avant, pendant ou après une attaque**, ils doivent être en mesure de répondre à toutes ces situations. C'est la raison pour laquelle les professionnels CyberOps sont de plus en plus demandés.
En suivant cette **formation Cisco CyberOps Associate**, vous comprendrez les concepts de sécurité, les procédures opérationnelles et les menaces courantes qui pèsent sur les réseaux et les applications. Vous vous familiariserez avec les types de données nécessaires pour **enquêter sur les incidents de sécurité**. Elle vous permettra aussi de maitriser la surveillance des alertes et des intrusions, ainsi que de comprendre et de **suivre les protocoles** établis pour répondre aux alertes qui se transforment en incidents.
À la fin de ce **programme accompagné de labs**, vous serez également préparé pour le passage de l'examen Cisco 200-201 CBROPS. Cet examen vous permettra de décrocher le titre de **Cisco Certified CyberOps Associate** et d'accéder à un rôle d'analyste des opérations de cybersécurité dans un centre d'opérations de cybersécurité (SOC).

Objectifs

A l'issue de la **formation Cisco CBROPS**, vous atteindrez les objectifs suivants :

- comprendre et décrire les concepts de sécurité ;
- comprendre et décrire les opérations liées au processus de surveillance de la sécurité ;
- comprendre et décrire les opérations d'une analyse basée sur l'hôte ;
- comprendre et décrire es opérations d'une analyse des intrusions réseau ;
- connaître les procédures de mise en œuvre des politiques et des procédures de sécurité ;
- être bien préparer pour le passage de l'examen Cisco 200-201 CBROPS.

Points forts

Un formateur expert et certifié Cisco, des support de cours officiel avec des labs et une préparation à la certification Cisco Certified CyberOps Associate.

Modalités d'évaluation

Travaux Pratiques

Pré-requis

Suivre la **formation Cisco CBROPS** nécessite les prérequis suivants :

- avoir une bonne connaissance des réseaux Ethernet et du protocole TCP/IP ;
- avoir des connaissances pratiques sur les systèmes d'exploitation Windows et Linux ;
- avoir une bonne connaissance des concepts de base de la sécurité des réseaux.

Pour acquérir ses connaissances, la formation Cisco suivante est recommandée :

Les formations ci-dessous sont recommandées.

Implémentation et administration des solutions Cisco (CCNA 200-301)

Public

Cette formation s'adresse aux publics suivants :

- tout professionnel de l'informatique qui souhaite acquérir des connaissances en matière d'opérations de cybersécurité avec les technologies Cisco, ou qui veulent décrocher le titre de Cisco Certified CyberOps Associate.

Cette formation s'adresse aux profils suivants

Analyste cybersécurité
Administrateur réseaux - télécoms
Administrateur système
Auditeur interne / externe

Programme

Domaine 1 : les concepts de sécurité

- Présentation du concept de triade de la CIA (confidentialité, intégrité, disponibilité).
- Comparaison entre plusieurs types de déploiement de sécurité.
- Explication des termes relatifs à la sécurité.
- Comparaison entre différents concepts de sécurité.
- Présentation des principes de la stratégie de défense en profondeur.
- Comparaison entre plusieurs modèles de contrôle d'accès.
- Explication des termes employés dans la norme de sécurité CVSS.
- Identification des défis liés à la visibilité des données (réseau, hôte et Cloud) au moment de la détection.
- Identification des pertes de données potentielles en fonction des profils de trafic fournis.
- Interprétation de la méthode du 5-tuple afin d'isoler un hôte compromis dans un ensemble groupé de journaux.
- Comparaison entre la détection basée sur des règles et la détection comportementale ou statistique.

Domaine 2 : la surveillance de la sécurité

- Comparaison entre une surface d'attaque et une surface de vulnérabilité.
- Identification des types de données fournies par ces technologies.
- Explication de l'utilisation de ces types de données dans la surveillance de la sécurité.
- Présentation des attaques réseau (attaques basées sur le protocole, attaques par déni de service, attaques par déni de service distribué et attaques de type Man in the middle).
- Présentation des attaques contre les applications web (attaques par injection SQL, attaques par injection de commandes, attaques par scripts intersites, etc.).

- Présentation d'une attaque d'ingénierie sociale.
- Explication des attaques basées sur les points de terminaison (débordements de mémoire tampon, commande et contrôle, logiciels malveillants et ransomwares).
- Présentation des techniques de contournement et d'obscurcissement (tunneling, cryptage et proxy).
- Explication des impacts des certificats sur la sécurité incluant la PKI, la traversée des réseaux publics et privés, l'asymétrie et la symétrie).
- Identification des composants des certificats dans un scénario particulier.

Domaine 3 : l'analyse basée sur l'hôte

- Présentation des technologies de point de terminaison en matière de surveillance de la sécurité.
- Identification des composants sur Windows et Linux dans une situation spécifique.
- Explication du rôle de l'attribution dans une investigation.
- Identification des types de preuves apportées sur la base des journaux fournis.
- Comparaison d'images de disques modifiées et non modifiées
- Interprétation des journaux du système d'exploitation, de l'application ou de la ligne de commande pour identifier un évènement.
- Interprétation du rapport de sortie d'un outil d'analyse de logiciels malveillants comme la chambre de détonation ou le bac à sable).

Domaine 4 : l'analyse des intrusions dans le réseau

- Mettre en correspondance les évènements fournis et les technologies sources.
- Comparaison de l'impact et de l'absence d'impact pour ces éléments.
- Comparaison de l'inspection approfondie des paquets avec le filtrage des paquets et le fonctionnement d'un pare-feu dynamique.
- Comparaison de l'interrogation du trafic en ligne avec les écoutes ou la surveillance du trafic.
- Comparaison des caractéristiques des données obtenues à partir des écoutes ou de la surveillance du trafic et des données transactionnelles (NetFlow) dans le cadre de l'analyse.
- Extraction de fichiers à partir d'un flux TCP lorsque vous recevez un fichier PCAP et Wireshark.
- Identification des éléments clés d'une intrusion à partir d'un fichier PCAP spécifique.
- Interprétation des champs d'entête de protocole dans le cadre de l'analyse des intrusions.
- Interprétation des éléments d'artéfact communs d'un évènement afin d'identifier une alerte.
- Interprétation des expressions régulières de base.

Domaine 5 : les politiques et les procédures de sécurité

- Présentation des différents concepts de gestion.
- Description des éléments d'un plan de réponse aux incidents selon la norme NIST.SP800-61.
- Application du processus de gestion des incidents pour un évènement.
- Identification des éléments avec les étapes d'analyse basées sur le NIST.SP800-61.
- Identification des parties prenantes de l'organisation en fonction des catégories de la RI du NIST (CMMC et NIST.SP800-61).
- Présentation des différents concepts définis dans le manuel NIST.SP800-86.
- Identification des éléments utilisés pour le profilage du réseau et des serveurs.
- Identification des données protégées dans un réseau.
- Classification des événements d'intrusion dans les catégories décrites dans le modèle de sécurité, notamment le modèle Cyber Kill Chain et le modèle Diamond d'intrusion.
- Description de la relation entre les métriques SOC et l'analyse de la portée (temps de détection, temps de confinement, temps de réponse et temps de contrôle).

Programme des laboratoires :

- 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 informatiques.
- Chasse au trafic malveillant.
- Corréler les journaux d'événements, les captures de paquets (PCAP) et les alertes d'une attaque.
- Étudier les attaques par navigateur.
- Analyser les activités suspectes du système de noms de domaine (DNS).
- 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 et Linux.