Understanding Cisco Cybersecurity Operations Fundamentals

Durée: 180 Jours **Réf de cours: CBROPS** **Version: 1.0** **Méthodes d'apprentissage: E-learning**

Résumé:

Cette formation permet aux participants d'acquérir les compétences et connaissances nécessaires pour comprendre les dispositifs d'infrastructure de réseau, les opérations et les vulnérabilités de la suite de protocoles TCP/IP (Transmission Control Protocol/Internet Protocol). Les participants apprendront les concepts de sécurité, les opérations et les attaques courantes des applications réseau, les systèmes d'exploitation Windows et Linux, et les types de données utilisées pour enquêter sur les incidents de sécurité. A l'issue de la formation, ils disposeront des connaissances de base nécessaires pour exercer la fonction d'analyste en cybersécurité de niveau associé dans un centre d'opérations de sécurité centré sur les menaces, afin de renforcer le protocole réseau, de protéger vos appareils et d'accroître l'efficacité opérationnelle.
La formation est une combinaison d'études dirigées par un instructeur et d'études à son propre rythme - 5 jours en classe et environ 1 jour d'auto-apprentissage. Le contenu de l'auto-apprentissage sera fourni dans le cadre du didacticiel numérique que les participants recevront au début de la formation et devrait faire partie de votre préparation à l'examen.
Mise à jour : 21.11.2023

Public visé:

Cette formation est destinée à un analyste de cybersécurité de niveau associé qui travaille dans des centres d'opérations de sécurité.

Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
- Expliquer le fonctionnement d'un SOC et décrire les différents types de services qui sont effectués du point de vue d'un analyste SOC de niveau 1.
- Expliquer les outils de surveillance de la sécurité du réseau (NSM) dont dispose l'analyste de la sécurité du réseau.
- Expliquer les données dont dispose l'analyste de la sécurité des réseaux.
- Décrire les concepts de base et les utilisations de la cryptographie.
- Décrire les failles de sécurité du protocole TCP/IP et la manière dont elles peuvent être utilisées pour attaquer les réseaux et les hôtes.
- Comprendre les technologies courantes de sécurité des points d'extrémité.
- Comprendre la chaîne d'exécution et les modèles de diamant pour les enquêtes sur les incidents, ainsi que l'utilisation de kits d'exploitation par les acteurs de la menace.
- Identifier les ressources pour la chasse aux cybermenaces.
- Expliquer la nécessité de la normalisation des données d'événements et de la corrélation des événements.
- Identifier les vecteurs d'attaque courants.

Pré-requis:

Les participants doivent remplir les conditions suivantes :

- Familiarité avec les réseaux Ethernet et TCP/IP
- Connaissance pratique des systèmes d'exploitation Windows et Linux
- Connaissance des 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

Contenu:

Définir le centre d'opérations de sécurité

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

Explorer les catégories de types de données

Comprendre les concepts de base de la cryptographie

Comprendre les attaques TCP/IP courantes

Comprendre les technologies de sécurité des points finaux

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

Identifier les ressources pour la chasse aux cybermenaces

Comprendre la corrélation et la normalisation des événements

Identifier les vecteurs d'attaque courants

Identifier les activités malveillantes

Identifier les schémas de comportement suspect

Mener des enquêtes sur les incidents de sécurité

Utilisation d'un modèle de carnet de route pour organiser la surveillance de la sécurité

Comprendre les mesures SOC

Comprendre le flux de travail et l'automatisation du SOC

Décrire la réponse aux incidents

Comprendre l'utilisation de VERIS

Comprendre les bases du système d'exploitation Windows

Comprendre les bases du système d'exploitation Linux

Ateliers

- 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

Méthodes pédagogiques :

Support de cours officiel remis aux participants