Cybersecurité

Understanding Cisco Cybersecurity Operations Fundamentals

CBROPS

Version : 1.0
5 Jours

Objectifs

A l'issue de ce cours, le stagiaire sera en mesure d'atteindre ses objectifs :

- Expliquer le fonctionnement d'un centre d'opérations de sécurité (SOC) et décrire les différents types de services qui sont fournis du point de vue d'un analyste SOC de niveau 1.
- Expliquer les outils de surveillance de la sécurité des réseaux (NSM) qui sont à la disposition de l'analyste de la sécurité des réseaux.
- Expliquer les données qui sont à la disposition de l'analyste de la sécurité des réseaux.
- Décrire les concepts de base et les utilisations de la cryptographie.
- Décrire les failles de sécurité dans le protocole TCP/IP et comment elles peuvent être utilisées pour attaquer les réseaux et les hôtes.
- Comprendre les technologies courantes de sécurité des terminaux.
- Comprendre la chaîne d'élimination et les modèles en 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 normaliser les données d'événements et de corréler les événements.
- Identifier les vecteurs d'attaque courants.
- Identifier les activités malveillantes.
- Identifier les modèles de comportements suspects.
- Mener des enquêtes sur les incidents de sécurité.
- Expliquer l'utilisation d'un playbook typique dans le SOC.
- Expliquer l'utilisation des métriques SOC pour mesurer l'efficacité du SOC.
- Expliquer l'utilisation d'un système de gestion des flux de travail et de l'automatisation pour améliorer l'efficacité du SOC.
- Décrire un plan type de réponse aux incidents et les fonctions d'une équipe type de réponse aux incidents de sécurité informatique (CSIRT).
- Expliquer l'utilisation de Vocabulary for Event Recording and Incident Sharing (VERIS) pour documenter les incidents de sécurité dans un format standard.

Pour plus d'informations : info@learneo.com ou 01 53 20 37 00

Public Concerné

- Étudiants poursuivant un diplôme technique
- Professionnels actuels de l'informatique
- Diplômés récents de l'enseignement supérieur avec un diplôme technique

Pré-requis

Avant de suivre ce cours, le stagiaire doit posséder les compétences et les connaissances 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.

Le cours Cisco suivant peut vous aider à acquérir les connaissances nécessaires à la préparation de ce cours : Mise en œuvre et administration des solutions Cisco (CCNA®)

Plan du cours détaillé

- Définir le centre des opérations de sécurité
- Comprendre l'infrastructure réseau et les outils de surveillance 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 d'extrémité
- 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 modèles de comportement suspect
- Mener des enquêtes sur les incidents de sécurité
- Utiliser un modèle de manuel pour organiser la surveillance de la sécurité
- Comprendre les mesures du 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

Laboratoire

- Utilisez les outils NSM pour analyser les catégories de données
- Explorer les technologies cryptographiques
- Explorer les attaques TCP/IP
- Explorer la sécurité des points de terminaison
- Étudier la méthodologie des pirates
- Traquer le trafic malveillant
- Corréler les journaux d'événements, les captures de paquets (PCAP) et les alertes d'une attaque
- Étudier les attaques basées sur les navigateurs
- Analyser l'activité suspecte du système de nom de domaine (DNS)
- Explorer les données de sécurité à des fins d'analyse
- Étudier 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