UNDERSTANDING CISCO CYBERSECURITY OPERATIONS FUNDAMENTALS

Cette formation Cisco CyberOps : Comprendre les fondamentaux des opérations de cybersécurité Cisco vous apporte une compréhension des différents types d'infrastructure, opérations et vulnérabilités à l'œuvre sur les réseaux Cisco et sur les transmissions TCP/IP. Elle aborde les concepts fondamentaux relatifs à la sécurité, aux opérations et attaques sur les applications réseaux, aux systèmes d'exploitation Windows et Linux, ainsi que sur les types de données utilisées pour analyser les incidents de sécurité.

Grace à cette formation Cisco CyberOps, vous serez à même de remplir le rôle d'analyste en cybersécurité en centre d'opérations de sécurité pour renforcer vos protocoles réseau, protéger vos appareils et augmenter l'efficacité opérationnelle. Ce cours vous prépare également à la certification Cisco Certified CyberOps Associate.

CURSUS:
CISCO

CODE DE LA FORMATION:
CS-SC-CYBROPS

ÉDITEUR OU CONSTRUCTEUR:
CISCO

DURÉE:
5 JOURS

PRÉREQUIS:

Pour suivre ce cours Cisco Cyber Operations dans de bonnes conditions, les participants doivent avoir suivi la formation Cisco CCNA : Mettre en œuvre et administrer des solutions (CCNA) ou posséder les connaissances équivalentes. Vous devez également comprendre le fonctionnement des réseaux Ethernet et TCP/IP, ainsi qu'avoir une maîtrise des systèmes d'exploitation Windows & Linux.

PUBLIC:

Cette formation Cisco CyberOps s'adresse aux analystes en cybersécurité de niveau Associate œuvrant dans des centres d'opérations en sécurité.

OBJECTIFS:

Après avoir suivi ce cours Cisco CyberOps, vous devriez être en mesure de :

- Expliquer comment un SOC opère and décrire les différents types de services réalisés par un analyste SOC de niveau 1
- Expliquer les outils de Network Security Monitoring (NMS) disponible pour un analyste de sécurité réseau.
- Expliquer les données disponibles à un analyste de sécurité réseau.
- Décrire les concepts de base de la cryptographie.
- Décrire les failles de sécurité dans le protocole TCP/IP et comment elles peuvent être exploitées pour attaquer les réseaux et les hôtes
- Comprendre les technologies de sécurité pour les endpoints
- Comprendre le kill chain et les diamond modeles pour les enquêtes sur les incidents, et l'utilisation de kits d'exploit par les acteurs de la menace
- Identifier les ressources pour se prémunir contre les cybermenaces
- Expliquer le besoin de la normalisation et la corrélation des évènements
- Identifier les attaques vectors courant
- Identifier les activités malveillantes
- Identifier les patterns des comportements suspicieux

- Mener des enquêtes sur les incidents de sécurité
- Expliquer l'utilisation d'un playbook typique dans un SOC
- Expliquer l'utilisation des métriques SOC pour mesurer l'efficacité du SOC
- Expliquer l'utilisation d'un système de gestion du workflow et d'automatisation pour améliorer l'efficacité du SOC
- Décrire un plan de réponse aux incidents et les fonctions d'un CSIRT typique
- Expliquer l'utilisation de VERIS pour documenter les incidents de sécurité dans un format standard
- Décrire les fonctionnalités et fonctionnalités du système d'exploitation Windows
- Décrire les caractéristiques et fonctionnalités du système d'exploitation Linux

CONTENU:

- Définition du centre d'opérations de sécurité
- Comprendre l'infrastructure réseau et les outils de surveillance de la sécurité 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 terminaux
- Comprendre l'analyse des incidents dans un Threat-Centric SOC
- Identifier les ressources pour se prémunir contre les cybermenaces
- Comprendre la corrélation et la normalisation des événements
- Identification des vecteurs d'attaque communs
- Identifier les activités malveillantes
- Identifier les modèles de comportement suspect
- Mener des enquêtes sur les incidents de sécurité
- Utilisation d'un modèle de Playbook pour organiser la surveillance de la sécurité
- Comprendre les métriques SOC
- Comprendre le workflow et l'automatisation 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