Understanding Cisco Cybersecurity Operations Fundamentals

Durée: 5 Jours Réf de cours: CBROPS Version: 1.1 Méthodes d'apprentissage: Classe à distance

Résumé:

Le cours « Understanding Cisco Cybersecurity Operations Fundamentals » (CBROPS) vous enseigne les concepts de sécurité, les opérations et les attaques courantes des réseaux et des applications, ainsi que les types de données nécessaires pour enquêter sur les incidents de sécurité.
Cette formation vous apprend à surveiller les alertes et les brèches, et à comprendre et suivre les procédures établies pour répondre aux alertes converties en incidents. Grâce à une combinaison de cours magistraux, de laboratoires pratiques et d'auto-apprentissage, vous apprendrez les compétences, les concepts et les technologies essentiels pour être un membre actif d'un centre d'opérations de cybersécurité (SOC), y compris la compréhension de l'infrastructure informatique, des opérations et des vulnérabilités.
Ce cours vous prépare à la certification Cisco Certified Cybersecurity Associate.
Ce cours est une combinaison de formation dispensée par un formateur et d'auto-apprentissage - 5 jours en classe et environ 1 jour d'auto-apprentissage. Le contenu de l'auto-apprentissage sera fourni dans le cadre du matériel de cours numérique que vous recevrez au début du cours et fera partie de votre préparation à l'examen.
Mis à jour 20/02/2025

Classe à Distance - site Client

Cette formation peut être suivie à distance en synchrone depuis n'importe quel site pourvu d'une connexion internet (2 Mb/s en symétrique recommandés). Le programme (théorie et pratique) suit le même déroulé pédagogique qu'en présentiel. La solution technologique adoptée permet aux apprenants à distance de suivre les présentations faites au tableau, de voir et d'entendre l'instructeur et les participants en temps réel, mais également d'échanger avec eux.

Public visé:

Cette formation est destinée à un analyste de cybersécurité de niveau débutant à intermédiaire qui travaille dans des centres d'opérations de sécurité (SOC).

Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
- Expliquer le fonctionnement d'un centre d'opérations de sécurité (SOC) et décrire les différents types de services qui sont assurés par un analyste SOC de niveau 1.
- Expliquer les outils de surveillance de la sécurité du réseau (NSM) dont dispose un analyste sécurité réseau.
- Expliquer les données dont dispose l'analyste sécurité réseau.
- 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.
- Identifier les activités malveillantes et 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 du "Vocabulary for Event Recording and Incident Sharing" (VERIS) pour documenter les incidents de sécurité dans un format standard.

Pré-requis:

Les participants doivent posséder les connaissances suivantes :

- Être familiarisé avec les réseaux Ethernet et TCP/IP.
- Avoir une connaissance pratique des systèmes d'exploitation Windows et Linux
- Être familiarisé avec les 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 un Centre d'opérations de sécurité (SOC)

Comprendre l'infrastructure du 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 postes de travail

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

Identifier les moyens de traquer les 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 de Playbooks pour l'organisation de 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 (autoformation)

Comprendre les bases du système d'exploitation Windows (autoformation)

Comprendre les bases du système d'exploitation Linux (autoformation)

Ateliers

- TP 1 : Utiliser les outils NSM pour analyser les catégories de données
- TP 2 : Explorer les technologies cryptographiques
- TP 3 : Explorer les attaques TCP/IP
- TP 4 : Explorer la sécurité des points finaux
- TP 5 : Étudier la méthodologie des pirates informatiques
- TP 6 : Traquer le trafic malveillant
- TP 7 : Corréler les logs d'événements, les PCAP et les alertes d'une attaque
- TP 8 : Enquêter sur les attaques par navigateur
- TP 9 : Analyser les activités DNS suspectes
- TP 10 : Explorer les données de sécurité à des fins d'analyse
- TP 11 : Enquêter sur une activité suspecte à l'aide de Security Onion
- TP 12 : Enquêter sur les menaces persistantes avancées
- TP 13 : Explorer les Playbooks SOC
- TP 14 : Explorer le système d'exploitation Windows
- TP 15 : Explorer le système d'exploitation Linux

Méthodes pédagogiques :

Support de cours officiel remis aux participants

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.