

Understanding Cisco Cybersecurity Operations Fundamentals

Réf. CBROPS · Cisco · Cybersécurité · **Formation certifiante**

DURÉE	NIVEAU	MODALITÉS	VOUCHER EXAMEN
5 jours	Fondamental	Présentiel · Live · Intra	Inclus

Présentation

Formation d'entrée dans le monde des opérations de sécurité, CBROPS couvre les concepts, la surveillance, l'analyse des hôtes et des intrusions réseau, ainsi que les politiques et procédures d'un SOC. Elle prépare l'examen 200-201 de la certification Cisco Certified CyberOps Associate, porte d'entrée idéale vers les métiers d'analyste SOC.

Objectifs pédagogiques

- Maîtriser les concepts fondamentaux de la cybersécurité et du SOC
- Analyser la surveillance de sécurité et les différents types de données réseau
- Réaliser l'analyse basée sur l'hôte (endpoints, journaux)
- Analyser les intrusions réseau (paquets, IDS/IPS, protocoles)
- Appliquer les politiques et procédures de réponse à incident
- Comprendre les concepts cryptographiques appliqués à la surveillance

Programme détaillé

1. Module 1 — Concepts de sécurité • Confidentialité, intégrité, disponibilité • Défense en profondeur • Modèles d'attaque et surface d'attaque • Gestion des risques et des vulnérabilités
2. Module 2 — Surveillance de la sécurité • Types de données : full packet capture, NetFlow, logs • Techniques d'évasion • Impact du chiffrement TLS sur la visibilité • Sources de données du SOC
3. Module 3 — Analyse basée sur l'hôte • Rôles des endpoints • Journaux Windows et Linux • Analyse des malwares et sandboxing • Investigation sur poste

4. Module 4 — Analyse des intrusions réseau

- Analyse de paquets (Wireshark)
- IDS/IPS et signatures
- Corrélation d'événements
- Gestion des faux positifs

5. Module 5 — Politiques et procédures de sécurité

- Cycle de réponse à incident (NIST)
- Rôle du CSIRT
- Chaîne de possession
- Cyber Kill Chain et Diamond Model

Prérequis

Connaissances de base des réseaux TCP/IP et des systèmes d'exploitation (Windows et Linux) ; une familiarité avec les fondamentaux de sécurité est un plus.

Public visé

Futurs analystes SOC de niveau 1, techniciens sécurité, étudiants et professionnels IT en reconversion vers la cybersécurité.

Ce qui est inclus

- Support de cours officiel Cisco (Digital Learning)
- Travaux pratiques d'analyse SOC et d'investigation
- Voucher d'examen de certification 200-201
- Attestation de réussite Advancia Training
- Pauses-café, déjeuner et accès à un formateur expert certifié Cisco

Certification

Prépare à l'examen 200-201 CBROPS (environ 120 minutes, QCM), examen unique de la certification Cisco Certified CyberOps Associate. Advancia Training est centre d'examen agréé Pearson VUE : vous passez votre certification dans nos locaux.

1 900 DT HT / participant — tarif inter-entreprise · financement CNFCPP possible