Understanding Cisco Cybersecurity Operations Fundamentals

Durée: 5 Jours **Réf de cours: CBROPS** **Version: 1.2**

Résumé:

Le cours **Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)** est conçu pour former les analystes en cybersécurité de niveau débutant à travailler dans un centre d'opérations de sécurité (SOC). Il prépare également à la certification **Cisco Certified CyberOps Associate**..
Veuillez noter que ce cours 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 vous recevrez au début du cours et devrait faire partie de votre préparation à l'examen.

Ce cours vaut 30 crédits de formation continue (CE) pour la recertification.
Mise à jour : 25.06.2025

Public visé:

Ce cours est destiné à un analyste en cybersécurité de niveau associé travaillant dans un centre d'opérations de sécurité (SOC).

Objectifs pédagogiques:

- A l'issue de cette formation, les participants seront en mesure de :
- Comprendre le fonctionnement d'un SOC et les rôles d'un analyste de niveau 1.
- Identifier les vecteurs d'attaque courants, les activités malveillantes et les comportements suspects.
- Utiliser les outils de surveillance de la sécurité réseau (NSM).
- Analyser les incidents de sécurité et utiliser un playbook SOC.
- Comprendre les systèmes d'exploitation Windows et Linux.
- Appliquer les concepts de cryptographie, de sécurité cloud et de normalisation des événements

Pré-requis:

Les participants doivent remplir les conditions préalables suivantes :

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

Après cette formation, nous vous conseillons le(s) module(s) suivant(s):

- CBRCOR - Performing CyberOps Using Cisco Security Technologies
- CBRTHD - Conducting Threat Hunting and Defending using Cisco Technologies for CyberOps

Contenu:

Fondamentaux du SOC

- Rôles
- Outils
- Automatisation
- Indicateurs de performance

Systèmes d’exploitation

- Architecture
- Commandes
- Services et sécurité sous Windows et Linux.

Technologies de sécurité des terminaux

- Antivirus
- Pare-feu
- Sandboxing
- Détection comportementale.

Attaques TCP/IP

- Spoofing
- DoS/DDoS
- Attaques ARP
- Vulnérabilités ICMP/TCP/UDP.

Cryptographie

- Hachage
- Chiffrement
- Intégrité des données.

Sécurité cloud

- Modèles de déploiement
- IAM
- Conformité.

Analyse d’incidents

- Kill chain
- Modèles de diamant
- Chasse aux menaces.

Corrélation et normalisation des événements

- Collecte et analyse de journaux
- PCAPs
- Alertes.

Travaux pratiques

- Analyse de trafic
- Investigation d’attaques
- Utilisation de Security Onion

Méthodes pédagogiques :

Les participants réalisent un test d'évaluation des connaissances en amont et en aval de la formation pour valider les connaissances acquises pendant la formation.
Un support de cours officiel sera remis aux stagiaires au format électronique.

Pour profiter pleinement du support électronique dès le 1er jour, nous invitons les participants à se munir d'un PC ou d'une tablette, qu’ils pourront connecter en WiFi dans nos locaux de Rueil, Lyon ou nos agences en régions.

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.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s’auto-évaluer sur l’atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d’inscription :

• Vous pouvez vous inscrire sur l’une de nos sessions planifiées en inter-entreprises jusqu’à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d’info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement