+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 29/06/2024

S'inscrire

Formation et préparation à la Certification OSCC™ (SEC-100)

ALL-IN-ONE : EXAMEN INCLUS AU TARIF AVEC LE COURS SEC-100

3 jours (21 heures)

PRÉSENTATION

La toute nouvelle certification OffSec CyberCore Certified (OSCC SEC-100), sortie le 25 juin 2024, atteste de vos compétences fondamentales en cybersécurité et en exploitation offensive.

Avec notre formation et notre programme, vous développerez des compétences pratiques et théoriques essentielles, visant à renforcer votre expertise dans les techniques offensives et défensives, ainsi que dans la sécurité cloud.

Notre formation couvre des aspects cruciaux tels que la mise en réseau, les meilleures pratiques défensives, la sécurité cloud et la cryptographie. Avec un équilibre parfait entre théorie approfondie et travaux pratiques en laboratoire, ce cours vous offre une préparation complète dans les disciplines essentielles de la cybersécurité.

Chaque module met à l'épreuve vos connaissances et compétences dans des domaines spécifiques de la cybersécurité et de l'exploitation offensive.

La formation OSCC™ est constamment mise à jour pour refléter les dernières tendances et évolutions dans le domaine de la sécurité informatique d'OffSec.

OBJECTIFS

- Comprendre les concepts de base de la mise en réseau et de la sécurité
- Apprendre les techniques offensives et les meilleures pratiques défensives
- Se familiariser avec les architectures de sécurité cloud
- Étudier la cryptographie, les systèmes d'exploitation et les processus de test d'intrusion
- Acquérir une vue d'ensemble des techniques offensives et des tactiques défensives

PUBLIC VISÉ

- **Administrateurs système**
- Techniciens réseau
- Consultants en sécurité
- Chercheurs en sécurité
- Analyste SOC

Pré-requis

- Connaissances de base en informatique
- Familiarité avec les systèmes d’exploitation Windows et Linux

Pré-requis techniques

- **Kali Linux** --> Téléchargeable ici
- Un ordinateur capable de faire fonctionner trois machines virtuelles avec facilité
- VMware Workstation 15 ou supérieur
- Processeur 64 bits avec un minimum de 2 cœurs et prise en charge de NX, SMEP, VT-d/IOMMU et VT-x/EPT
- Au moins 100 Go de disque dur disponible
- Au moins 8 Go de RAM
- Le seul système d'exploitation hôte pris en charge est Windows 10 / 11

Note : Ambient IT n’est pas propriétaire de OSCC™, cette certification appartient à OffSec ® Services LLC.

PROGRAMME DE NOTRE FORMATION CERTIFICATION OSCC™

Introduction à la CyberSécurité

- Introduction générale au cours
- Importance de la cybersécurité aujourd'hui
- Compréhension des menaces et des vulnérabilités
- Rôles de cybersécurité
- Résumé des compétences préalables nécessaires
- Présentation du programme de la formation
- Objectifs d'apprentissage
- Méthodologie de la formation

Techniques fondamentales

- Concepts de base et introduction à AWS
- Introduction aux systèmes d'exploitation Linux
- Commandes de base et gestion des fichiers
- Introduction aux systèmes d'exploitation Windows
- Gestion des utilisateurs et des fichiers

Scripts et réseau

- Introduction à la programmation en Python
- Scripts de base pour l'automatisation des tâches
- Introduction à PowerShell pour l'administration Windows
- Scripts de base pour la gestion du système
- Concepts de base du réseau
- Modèle OSI et protocoles courants

Réseau et Cryptographie

- Conception et gestion des réseaux d'entreprise
- Introduction et configuration de pare-feu
- Principes de la cryptographie
- Algorithmes courants et leur utilisation

Tests d'intrusion et attaques

- Étapes et méthodologies du test d'intrusion
- Techniques de collecte d'informations
- Utilisation de Nmap pour la reconnaissance réseau
- Types courants d'attaques web
- Techniques de prévention et de détection
- Méthodes d'attaque sur les terminaux
- Stratégies de défense

Privilèges et Défense

- Techniques d'élévation des privilèges
- Contre-mesures
- Techniques pour contourner les systèmes de défense
- Meilleures pratiques pour la détection
- Attaques spécifiques aux environnements cloud
- Stratégies de défense cloud

Gestion et Analyse

- Gestion d'un Security Operations Center
- Rôles et responsabilités
- Identification et gestion des vulnérabilités

- Outils et techniques
- Techniques d'analyse de malware
- Prévention et réponse

Ingénierie sociale et Sécurité Wi-Fi

- Comprendre et détecter les attaques d'ingénierie sociale
- Méthodes de prévention
- Types d'attaques et leurs impacts
- Stratégies de défense
- Menaces et contre-mesures pour les réseaux sans fil

Sécurité des systèmes et gestion de carrière

- Sécurité des systèmes embarqués et de contrôle industriel
- Concepts fondamentaux de validation des entrées
- Conception de systèmes fiables
- Concepts de base et bonnes pratiques
- Introduction aux tests d'assurance qualité
- Identification et évaluation des risques
- Prise de décisions sécuritaires pour l'entreprise

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.