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

Mis à jour le 19/12/2024

S'inscrire

Formation Certification SSCP

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

4 jours (28 heures)

Présentation

Notre formation de certification SSCP vous enseignera la maîtrise des systèmes de sécurité. Approfondissez vos connaissances et vos compétences dans la mise en œuvre de plan de cybersécurité dans les systèmes .

Durant notre formation SSCP, vous réviserez tous les chapitres présents à l'examen. En effet, nous couvrons les 6 domaines du SSCP Systems Security Certified Practitioner de l'ISC2 :

L’examen évalue des sujets tels que la connaissance des concepts et pratiques de sécurité, les Modèles de contrôle d'accès, DAC, MAC, RBAC, ABAC, et Cryptographie, sécurité des systèmes. Une large gamme de thèmes sera abordée pour garantir une préparation complète et approfondie.

Cette certification renforcera grandement votre attractivité auprès des employeurs si vous désirez un emploi dans le domaine de la cybersécurité.

Objectifs

- Acquérir les connaissances nécessaires à la réussite de l’examen SSCP
- Maîtriser les connaissances en sécurité des systèmes
- Comprendre les besoins en sécurité dans un environnement cloud
- Acquérir les connaissances nécessaires pour conseiller une organisation sur les meilleures pratiques en cybersécurité

Public visé

- Administrateur système
- Ingénieur sécurité
- Analyste Cybersécurité
- Administrateur réseau
- Consultant en cybersécurité

Pré-requis

- Une expérience recommandée de 2 ans en administration système/sécurité
- Connaissances solides en sécurité informatique
- Compréhension de l’anglais technique

Note : Ambient IT n’est pas propriétaire de SSCP, cette certification appartient à ISC2, INC.

Programme de la Préparation à la Certification SSCP

Concepts et pratiques de sécurité

- Principes fondamentaux de la sécurité et de l'information
  - Confidentialité, intégrité, disponibilité
  - Non-répudiation et authenticité
- Couches de sécurité et périmètres
- Contrôles de sécurité préventifs, détectifs, correctifs
- Cadres normatifs et réglementaires comme ISO 27001, NIST, RGPD
- Concepts de sécurité, contrôle d’accès physique, protection des équipements et des installations.

Gestion de l'accès

- Introduction au concept de gestion des accès et à son importance
- Modèle de contrôle d'accès, DAC, MAC, RBAC, ABAC
- Gestion des identités et des accès IAM
- Authentification, autorisation, journalisation, mise en œuvre et gestion
- Pratiques sécurisées pour la gestion des comptes utilisateurs
- Technologies d'authentification avec authentification multifacteurs, authentification unique, certificats numériques.

Identification, gestion des risques et des menaces

- Sensibilisation aux risques, identification des menaces, vulnérabilités et impacts
- Méthodologies d'évaluation des risques
  - Qualitative
  - Quantitative
  - Hybride
- Analyse des menaces, intelligence sur les menaces, rapports et interprétation
- Techniques de surveillance, SIEM, IDS et IPS
- Gestion des risques, de réduction, transfert, acceptation ou évitement

- Tableaux de bord pour le suivi des indicateurs de sécurité
- Étude de cas : analyse d'une cyberattaque et retour d'expérience

Cryptographie, sécurité des systèmes

- Vue sur les types de système on-premise, cloud, hybrides
- Sécurisation des systèmes d'exploitation par durcissement, mises à jour, gestion des privilèges
- Sécurisation des bases de données avec gestion des accès et contrôle des modifications
- fondamentaux de la cryptographie clés publiques, privées, PKI
- Cryptographie appliquée hachage, signatures numériques, algorithmes modernes comme AES, RSA, SHA

Sécurité des réseaux et des communications

- Concepts de réseaux modèles OSI et TCP/IP
- Protocoles sécurisés SSL/TLS, IPsec, VPN
- Cryptographie de chiffrement symétrique/asymétrique, certificats numériques
- Sécurisation des infrastructures réseau pare-feu, routeurs, switches
- Défenses contre les attaques réseau DDoS, attaques par déni de service, MITM
- Pratiques sécurisées pour les réseaux sans fil

Reprise après sinistre et continuité des activités

- Plans de secours : création, documentation et validation par des tests réguliers
- Sauvegardes et restaurations : stratégies et meilleures pratiques
- Gestion des crises : communication et coordination pendant un incident
- Étude de cas : simulation de reprise après sinistre

Stratégies et astuces pour réussir l'examen

FAQ – QUESTIONS / RÉPONSES

En quelle langue la formation SSCP vous est enseignée ?

La formation est en français.

En quelle langue se déroule l'examen ?

L'examen se déroule en anglais.

L’examen est-il compris dans le prix de la formation ?

Oui, le prix de la certification est inclus au coût de la formation

Comment se déroule l'examen pour la certification SSCP ?

L'examen consiste en un QCM composé de 125 questions sur les domaines suivants :

- Concepts et pratiques de sécurité
- Contrôles d'accès
- Identification, surveillance et analyse des risques
- Réponse aux incidents et récupération
- Cryptographie
- Sécurité des réseaux et des communications
- Sécurité des systèmes et des applications

Cet examen dure 3 heures et est en anglais.

Pour réussir cet examen, il faut au minimum obtenir 700 points sur 1000 points.

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.