

Mis à jour le 02/02/2024

S'inscrire

Formation Cisco CyberOps Professional™ : Préparation à la Certification

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

2 jours (14 heures)

Présentation

L'acquisition de la certification Cisco CyberOps Professional™ témoigne de votre expertise avancée en tant qu'analyste principal au sein d'un centre d'opérations de sécurité (SOC). Intervenant dans des situations d'incident, de sécurité cloud, et d'autres responsabilités liées à la sécurité défensive active.

Notre formation Cisco CyberOps Professional™ vous permettra d'avoir une meilleure compréhension des [opérations de cybersécurité](#).

L'examen est composé de [plusieurs modules](#) dont l'automatisation de tâche de sécurité à l'aide de scripts, la gestion de données dans des formats courants. Mais aussi sur l'utilisation d'APIs pour l'automatisation des opérations de sécurité.

Vous apprendrez à recommander des techniques analytiques, à évaluer la posture de sécurité des actifs et à effectuer des [analyses de malware](#).

Durant notre formation de préparation à l'examen, nous aborderons tous les points présents en vous donnant les astuces.

Ce programme de formation vous permettra aussi d'avoir une perspective approfondie sur la gestion des incidents, la surveillance et les analyses de comportements d'utilisateurs.

Objectifs

- Comprendre l'utilisation des playbooks et des outils nécessaires

- Appliquer les playbooks pour des scénarios courants en cybersécurité
- Maîtriser les normes de conformité industrielles et la gestion des risques
- Utiliser les techniques d'analyse de données et améliorer les contrôles de sécurité
- Automatiser des tâches opérationnelles de sécurité avec des concepts avancés

Public visé

- Analyste senior en cybersécurité
- Analyste SOC

Pré-requis

- Avoir obtenu une certification CCNA ou connaître les principes de base des réseaux et la construction de réseaux locaux
- Comprendre le fonctionnement des réseaux Ethernet et TCP/IP
- Avoir une maîtrise des systèmes d'exploitation Windows & Linux
- 3 à 5 ans d'expérience de mise en place de solutions réseaux est conseillé

Note : Ambient IT n'est pas propriétaire de Cisco Certifications™, cette certification appartient à Cisco, Inc.

Programme de la formation Cisco CyberOps Professional™

Fondamentaux de la CyberSécurité

- Compréhension des playbooks et des outils nécessaires
- Application des playbooks pour des scénarios courants
- Connaissance des normes de conformité industrielles
- Gestion des risques et cyber-assurance
- Analyse de la sécurité dans des environnements cloud

Techniques de sécurité opérationnelle

- Recommandations en techniques d'analyse de données
- Évaluation et amélioration des contrôles de sécurité
- Recommandations pour la sécurisation des systèmes
- Utilisation de la menace et de l'analyse dans la prévention de la perte de données

Processus d'investigation et d'analyse

- Analyse des modèles de menace
- Enquête sur les types courants de cas et d'attaques
- Processus complet d'analyse de logiciels malveillants

- Investigations d'intrusions et de pertes de données
- Triage des vulnérabilités et analyses de risques

Automatisation et orchestration

- Concepts et mécanismes d'orchestration et d'automatisation
- Interprétation et modification de scripts (Python)
- Automatisation des tâches opérationnelles de sécurité
- Reconnaissance des formats de données et opportunités d'automatisation
- Utilisation de Bash, CI/CD, et principes d'Infrastructure as Code

Pratiques avancées de sécurité

- Mise en œuvre de techniques avancées de détection et de réponse
- Évaluation des métriques de sécurité opérationnelle
- Analyse avancée des comportements d'utilisateurs et d'entités
- Utilisation d'outils d'analyse réseau et de détection d'intrusions
- Exploration des implications de SecDevOps et des pratiques avancées de sécurité

Stratégie et méthodes pour réussir l'examen

Examen blanc

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.