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

Mis à jour le 11/04/2024

S'inscrire

Formation Cisco CyberOps Associate™ : Préparation à la Certification

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

2 jours (14 heures)

Présentation

La certification Cisco CyberOps Associate™ attestera de votre expertise avancée en tant qu'analyste senior. Cette certification validera vos compétences.

Avec notre formation Cisco CyberOps™ vous aurez une meilleure compréhension des opérations de cybersécurité. Renforcez votre expertise pour assurer une protection proactive, sécuriser vos appareils, et exceller dans votre rôle d'analyste senior.

L'examen est composé de plusieurs modules dont les dispositifs, les opérations et les vulnérabilités de l'infrastructure réseau basée sur TCP/IP. Vous permettant de vous armer pour relever les défis de la sécurité informatique.

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

Vous serez ainsi en mesure de fortifier les protocoles réseau, sécuriser vos appareils et optimiser l'efficacité opérationnelle.

Objectifs

- Comprendre les principes fondamentaux de la cybersécurité
- Maîtriser les concepts de sécurité
- Acquérir une expertise dans la surveillance de la sécurité
- Se préparer à la certification Cisco CyberOps Associate™

Public visé

- Analyste 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

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

Programme de la formation Cisco CyberOps Associate™

Introduction à la Cybersécurité et les concepts de base

- CIA (Confidentiality, Integrity, Availabiliy)
- Security Deployments
  - Network, endpoint, et application security systems
  - Agentless et agent-based protections
  - Legacy antivirus, antimalware
  - SIEM, SOAR, log management
  - Cloud security deployments

Les fondamentaux de la sécurité et Access Control

- **Security Concepts**
  - Risk
  - Threat
  - Vulnerability
  - Exploit
- Access Control Models
  - Discretionary, mandatory, nondiscretionary access control
  - Authentication, authorization, accounting

Data Visibility et Loss Prevention

- Data Visibility Challenges
  - Network, host, cloud visibility
- Data Loss Prevention
  - Identification des pertes de données à partir des profils de trafic

Security Monitoring

- Type de données
  - TCP dump
  - NetFlow
  - Firewalls
  - Application control
- Utilisation des données dans le security monitoring
  - Full packet capture, session data, transaction data, statistical data, metadata, alert data

Cyberattaques courantes

- Network Attacks
- Web Application Attacks
- Social Engineering Attacks
- Endpoint-based Attacks
- Evasion et Obfuscation Techniques
- Impact of Certificates on Security

Analyse des intrusions

- Extraction des fichiers depuis TCP streams
- Identification key elements
- Protocol headers
- Artifact elements

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.