EduGroupe
Accompagner pour réussir

Sécurité : Certified Information Systems Security Professional (CISSP)

Référence : **SECCISSP** Durée : **5 jours (35 heures)** Certification : **CISSP**

Connaissances préalables

- 1-Avoir une expérience dans l'administration des systèmes, une bonne compréhension des systèmes Unix, Linux et Windows
- 2-Connaître les concepts de base de la sécurité
- 3-Avoir des connaissances de base en langue anglaise car le support de cours est en langue anglaise

Profil des stagiaires

- Consultants, Managers, Administrateurs réseaux et Ingénieurs sécurité

Objectifs

- Fonctionnement de la sécurité, Contrôle d'accès, Cryptographie
- Modèles et architectures de la sécurité
- Sécurisation des télécommunications et des réseaux
- Sécurité des applications, Plan de continuité d'activité
- Cadre légal, investigation et éthique, Sécurité physique
- Sécurité des informations et gestion des risques
- Préparer, Réviser et Acquérir les trucs et astuces pour réussir l'examen officiel CISSP.

Certification préparée

L'examen CISSP - Certified Information Systems Security Professional délivré par l'(ISC)² s'adresse aux professionnels experts de la sécurité informatique. La certification CISSP permet d'étalonner son niveau de compétences tant au niveau des connaissances techniques qu'au niveau analyse des risques et audit des systèmes dans une optique gouvernance des systèmes d'informations. Pour en savoir plus sur l('ISC)² et la certification CISSP cliquez ici

Méthodes pédagogiques

- La formation est constituée d'apports théoriques, d'exercices pratiques et de réflexions
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- Mise à disposition d'un poste de travail par participant

Formateur

- Consultant-Formateur expert Management de la sécurité

Méthodes d'évaluation des acquis

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

EduGroupe
Accompagner pour réussir

Contenu du cours

1. Fonctionnement de la sécurité

- Changer les contrôles
- Gérer la configuration

2. Estimer la vulnérabilité

-

3. Contrôle des accès

- AAA
- Méthodes d'authentification (types 1, 2 et 3)
- Autorisations : - DAC, RBAC, MAC
- Autorisations : - DAC, RBAC, MAC
- Gestion centralisée, décentralisée ou hybride
- Vulnérabilités

4. Cryptographie

- Historique

5. Différents type de cryptographie (SSL, S/MIME, PKI, etc.)

-

6. Architecture et conception de la sécurité

- Processeurs
- Mémoires
- Systèmes d'exploitation
- Modèles
- TCSEC, ITSEC

7. Sécurisation des télécommunications et des réseaux

- Modèles OSI/ DoD, TCP/IP
- Ethernet
- Périphériques (routeurs, switchs)
- Pare-feu
- Périphériques
- Technologies WAN
- Voix
- IPsec

8. Sécurisation des applications

- SDLC
- Sécurité des bases de données
- AI

9. Malware

-

10. Administration de la continuité de l'exploitation et prévision des cas d'urgence

- Stratégie
- BIA
- Sauvegardes des données

11. Tests

-

12. Lois, enquêtes et éthique

- Propriété intellectuelle
- Réponse aux incidents
- Lois : HIPAA, GLB, SOX

13. Sécurisation physique

- CPTED
- Protection contre le feu
- Sécurité électrique
- HVAC
- Périmètres de sécurité
- Contrôle d'accès physique
- Détection d'intrusion

14. Sécurisation des informations et gestion des risques

- CIA
- Rôles et responsabilités
- Taxonomie – Classification de l'information
- Gestion des risques
- DSLC (Security Development LifeCycle)
- Certification et accréditation
- Stratégies, procédures, standards
- Transfert des connaissances

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.