Sécurité : Certified Information Systems Security Professional (CISSP)

Référence : **SECCISSP** Durée : **5 jours** Certification : **CISSP**

CONNAISSANCES PREALABLES

• 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

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

CERTIFICATION PREPAREE

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

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Management de la sécurité

METHODE D'EVALUATION 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

CONTENU DU COURS

Fonctionnement de la sécurité

- Changer les contrôles
- Gérer la configuration

Estimer la vulnérabilité

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

Cryptographie

- Historique

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

Architecture et conception de la sécurité
- Processeurs
- Mémoires
- Systèmes d'exploitation
- Modèles
- TCSEC, ITSEC

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

Sécurisation des applications
- SDLC
- Sécurité des bases de données
- AI

Malware

Administration de la continuité de l'exploitation et prévision des cas d'urgence
- Stratégie
- BIA
- Sauvegardes des données

Tests

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

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

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.*