Préparation à la certification CISSP (Certified Information Systems Security Professional)

Durée : 5 jours Référence : CISSP

Cette formation présente les concepts de sécurité utiles à l'obtention de la certification CISSP. Elle vous préparera au passage de l'examen en couvrant l'ensemble du Common Body of Knowledge (CBK) du (ISC) ².

Contenu

- Sécurité du SI et le CBK de l'(ISC) ²
- Gestion de la sécurité et sécurité des opérations
- Architecture, modèles de sécurité et contrôle d'accès
- Cryptographie et sécurité des développements
- Sécurité des télécoms et des réseaux
- Continuité des activités, loi et éthique et sécurité physique

Participants

Responsable de la sécurité des SI, Chef de projet en sécurité.

Pré-requis

Connaissance des réseaux, des systèmes d'exploitation, de la sécurité de l'information.

Programme

Sécurité du SI et le CBK de l'(ISC) ²

- La sécurité des SI.
- La certification CISSP.
- Présentation du périmètre couvert par le CBK.

Gestion de la sécurité et sécurité des opérations

- Pratiques de gestion de la sécurité : rédaction de politiques, directives, procédures et standards en sécurité, programme de sensibilisation à la sécurité, pratiques de management, gestion des risques.

- Sécurité des opérations : mesures préventives, de détection et correctives, rôles et responsabilités des acteurs, meilleures pratiques, sécurité lors de l'embauche du personnel.

Architecture, modèles de sécurité et contrôle d'accès

- Architecture et modèles de sécurité : architecture de système, modèles théoriques de sécurité de l'information, méthodes d'évaluation de systèmes, modes de sécurité opérationnels.
- Systèmes et méthodologies de contrôle d'accès : catégories et types de contrôles d'accès, accès aux données, accès aux systèmes, systèmes de prévention des intrusions (IPS) et de détection d'intrusions (IDS), journaux d'audit, menaces et attaques reliés au contrôle des accès.

Cryptographie et sécurité des développements

- Cryptographie : concepts, cryptographie symétrique et asymétrique, fonctions de hachage, infrastructure à clef publique.
- Sécurité des développements d'applications et de systèmes : bases de données, entrepôts de données, cycle de développement, programmation orienté objet, systèmes experts, intelligence artificielle.

Sécurité des télécoms et des réseaux

- Sécurité des réseaux et télécoms : notions de base, modèle TCP/IP, équipement réseaux et de sécurité, protocoles de sécurité, attaques sur les réseaux, sauvegardes des données, technologies sans fils, VPN...

Continuité des activités, loi et éthique et sécurité physique

- Continuité des opérations et plan de reprise en cas de désastre : plan de continuité des activités, plan de rétablissement après sinistre, mesures d'urgence, programme de formation et de sensibilisation, communication de crise, exercices et tests.
- Loi, investigations et éthique : droit civil, criminel et administratif, propriété intellectuelle, cadre juridique en matière d'investigation, règles d'admissibilité des preuves.
- Sécurité physique : menaces et vulnérabilités liées à l'environnement d'un lieu, périmètre de sécurité, exigences d'aménagement, surveillance des lieux, protection du personnel.