CISSP, sécurité des SI, préparation à la certification

-Réference: **SII-364** -Prix: **0 €/P** -Durée: **5 Jours (35 Heures)**

Les objectifs de la formation

- Connaître le Common Body of Knowledge de la sécurité IT.
- Développer une vision globale des enjeux de sécurité IT.
- Approfondir les connaissances des huit domaines du CISSP.
- Se préparer à l'examen de certification du CISSP.

A qui s'adesse cette formation ?

POUR QUI :

- Responsables de la sécurité des SI ou toute autre personne jouant un rôle dans la politique de sécurité des SI.

PRÉREQUIS :

- Connaissances de base sur les réseaux et les systèmes d'exploitation ainsi qu'en sécurité de l'information.
- Connaissances de base des normes en audit et en continuité des affaires.

Programme

- **Sécurité du SI et le CBK de l'(ISC)²**
  - La sécurité des Systèmes d'Information.
  - Le pourquoi de la certification CISSP.
  - Présentation du périmètre couvert par le CBK.
- **Gestion de la sécurité et sécurité des opérations**
  - Pratiques de gestion de la sécurité. La rédaction de politiques, directives, procédures et standards en sécurité.
  - Le programme de sensibilisation à la sécurité, pratiques de management, gestion des risques, etc.
  - Sécurité des opérations : mesures préventives, de détection et correctives, rôles et responsabilités des acteurs.
  - Les meilleures pratiques, la sécurité lors de l'embauche du personnel, etc.
- **Architecture, modèles de sécurité et contrôle d'accès**
  - Architecture et modèles de sécurité : architecture de système, modèles théoriques de sécurité de l'information.

Programme

- Les méthodes d'évaluation de systèmes, modes de sécurité opérationnels, etc.
- Systèmes et méthodologies de contrôle d'accès. Les catégories et types de contrôles d'accès.
- Accès aux données et 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, etc.

- **Cryptographie et sécurité des développements**
  - Cryptographie. Les concepts, cryptographie symétrique et asymétrique.
  - Les fonctions de hachage, infrastructure à clé publique, etc.
  - Sécurité des développements d'applications et de systèmes. Les bases de données, entrepôts de données.
  - Le cycle de développement, programmation orientée objet, systèmes experts, intelligence artificielle, etc.

- **Sécurité des télécoms et des réseaux**
  - Sécurité des réseaux et télécoms. Les notions de base, modèle TCP/IP, équipements réseaux et de sécurité.
  - Les protocoles de sécurité, les attaques sur les réseaux, sauvegardes des données, technologies sans fil, VPN...

- **Continuité des activités, loi, éthique et sécurité physique**
  - Continuité des opérations et plan de reprise en cas de désastre.
  - Le plan de continuité des activités, le plan de rétablissement après sinistre.
  - Les 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.
  - Le cadre juridique en matière d'investigation, règles d'admissibilité des preuves, etc.
  - La sécurité physique. Les menaces et vulnérabilités liées à l'environnement d'un lieu, périmètre de sécurité.
  - Les exigences d'aménagement, surveillance des lieux, protection du personnel, etc.

(+212) 5 22 27 99 01

(+212) 6 60 10 42 56

Contact@skills-group.com

Nous sommes à votre disposition :
De Lun - Ven 09h00-18h00 et Sam 09H00 – 13H00

Angle bd Abdelmoumen et rue Soumaya, Résidence Shehrazade 3, 7éme étage N° 30
Casablanca 20340, Maroc