CYBERSÉCURITÉ

Préparation à la certification CISSP ®

5 jours (35h00) | SEC002 | Num form : form-28 | Perfectionnement / Avancé

INFORMATIQUE / SÉCURITÉ IT / CYBERSÉCURITÉ

À l'issue de ce stage vous serez capable de :

- Connaître les différents domaines du CBK défini par L'(ISC)².
- Gestion des accès et des identités
- Évaluation de la sécurité et des tests
- Sécurité des Opérations
- Engineering de la sécurité et cryptographie
- Sécurité des réseaux et des communications

Niveau requis :

- Justifier de cinq ans d'expérience professionnelle minimum dans au moins 2 des 8 domaines du CBK®

Public concerné :

- Consultants IT,
- Managers
- Administrateurs réseaux
- Ingénieurs sécurité
- Responsable sécurité

Programme :

SÉCURITÉ DES INFORMATIONS ET GESTION DES RISQUES

- Les concepts de confidentialité, intégrité et disponibilité

- Les principes de gouvernance de la sécurité
- La conformité
- Les questions légales et réglementaires concernant la sécurité de l'information dans un contexte global
- L'éthique professionnelle
- La politique de sécurité, les standards, les procédures et les guidelines
- Les exigences de continuité d'activité
- Les politiques de sécurité du personnel
- Les concepts de management des risques
- Le modèle de menace
- Les considérations de risque de sécurité dans la stratégie d'acquisition
- La sensibilisation, la formation et l'éducation à la sécurité de l'information

LA SÉCURITÉ DES ASSETS

- Classification de l'information et support des assets
- Le maintien de la propriété
- Protéger la confidentialité
- Assurer la rétention appropriée
- Les mesures de sécurité des données
- Les exigences de manipulation

INGÉNIERIE DE LA SÉCURITÉ

- Les processus d'engineering et les principes de conception sécurisée
- Comprendre les concepts fondamentaux des modèles de sécurité
- Les mesures et contre-mesures
- Les possibilités de sécurités offertes par les systèmes d'information
- Les vulnérabilités de sécurité des architectures, des conceptions, des solutions
- Evaluer et réduire les vulnérabilités de sécurité des systèmes web, mobiles et des systèmes embarqués
- La cryptographie
- Les principes de sécurité au site et à la conception de l'installation
- La sécurité physique

SÉCURITÉ DES TÉLÉCOMMUNICATIONS ET DES RÉSEAUX

- Les principes de conception sécurisée à l'architectures réseau
- Sécuriser les composants réseau
- Concevoir et établir des canaux de communication sécurisés
- Prévenir ou limiter les attaques réseau

LA GESTION DES IDENTITÉS ET DES ACCÈS

- Contrôle d'accès physique et logique aux assets

- Gérer l'identification et l'authentification des personnes et des équipements
- L'identité en tant que service
- Les services d'identité tiers
- Les mécanismes d'autorisation
- Les attaques au contrôle d'accès
- Le cycle de vie des identités et du provisionnement des accès

ÉVALUATION DE LA SÉCURITÉ ET TESTS

- Les stratégies d'évaluation et de test de sécurité
- Tests de mesures de sécurité
- Les données des processus de sécurité
- Les résultats des tests
- Les audits internes ou third-party

CONTINUITÉ DES OPÉRATIONS ET PLAN DE REPRISE

- Les investigations
- Les exigences des types d'investigations
- Les activités de monitoring et de logging
- Le provisionnement des ressources
- Les concepts fondamentaux de sécurité des opérations
- Les techniques de protection de ressources
- La gestion de incidents
- Opérer et maintenir des mesures de sécurité préventives
- La gestion des patchs et vulnérabilités
- Les processus de gestion des changements
- Les stratégies de reprise
- Les stratégies de reprise après sinistre
- Les plans de reprise après sinistre
- Le Plan de Continuité d'Activité
- La gestion de la sécurité physique
- Les problèmes de sécurité du personnel

LA SÉCURITÉ DU DÉVELOPPEMENT LOGICIEL

- La sécurité dans le cycle de vie de développement logiciel
- Les mesures de sécurité dans les environnements de développement
- L'efficacité de la sécurité du logiciel
- Evaluer l'impact de la sécurité d'un logiciel acquis