4

4. Session de préparation approfondie à la certification CISSP

OBJECTIFS DE LA FORMATION

L' objectif de cette formation est de :

- Approfondir les domaines de la sécurité déjà connus
- Acquérir des connaissances plus poussées dans des domaines moins connus
- Acquérir le vocabulaire commun relatif au CISSP®
- Mieux comprendre les questions de l'examen
- Discuter des meilleures pratiques avec vos collègues
- Acquérir des aptitudes en gestion de la sécurité et des risques
- Développer une vision globale et pas seulement technologique des besoins en sécurité de l'entreprise

La durée de la formation est de 5 jours.

CONTENU DE LA FORMATION

Séance 1 : Sécurité et Gestion des Risques (Sécurité, Risques, Conformité, Lois, Règlementations, Continuité d'Activité)

Les différents points qui seront traités sont les suivants :

1. Comprendre et appliquer les concepts de la C.I.A ;
2. Déployer les Principes de Gouvernance de la Sécurité ;
3. Assurer la Conformité ;
4. Comprendre les difficultés légales et règlementaires de la sécurité informatique dans un contexte global ;
5. Comprendre l'éthique professionnelle ;
6. Développer et implémenter les politiques de sécurité, les procédures, les guidelines et les standards ;
7. Comprendre les Exigences de la Continuité d'activité ;
8. Concevoir la sécurité des ressources humaines ;
9. Comprendre et appliquer les principes de la gestion des risques ;
10. Comprendre et appliquer la modélisation des menaces ;
11. Introduire le concept d'analyse des risques dans les processus d'acquisition ;
12. Etablir et gérer la formation, la sensibilisation et l'éducation sur la sécurité.

4. Session de préparation approfondie à la certification CISSP

Section 2 : La protection des biens

Les différents points qui seront traités sont les suivants :

1. Classifier les informations et les biens (sensitivité, criticité) ;
2. Déterminer et maintenir le propriétaire d'un bien ;
3. Assurer la confidentialité ;
4. Maintenir une politique de rétention appropriée ;
5. Déterminer les contrôles de la sécurité des données ;
6. Etablir les exigences pour le maintien du bien.

Section 3 : L'ingénierie de la sécurité

Les différents points qui seront traités sont les suivants :

1. Implémenter et gérer les processus d'ingénierie en utilisation une approche conceptuelle sécurisée ;
2. Comprendre les concepts fondamentaux des modèles de sécurité ;
3. Sélectionner les contrôles et les contremesures en se basant sur les modèles d'évaluation de la sécurité des systèmes ;
4. Comprendre les fonctionnalités de sécurité d'un système informatique ;
5. Analyser et éliminer les vulnérabilités d'une architecture de sécurité (Web, Mobile, Système embarqué, etc) ;
6. Déployer la cryptographie ;
7. Concevoir et implémenter les principes de la sécurité physique.

Section 4 : Sécurité des réseaux et des Communications

Les différents points qui seront traités sont les suivants :

1. Déployer une architecture réseau avec une conception sécurisée ;
2. Sécuriser les composantes d'un réseau ;
3. Concevoir et établir des canaux sécurisés de communication ;
4. Prévenir et gérer les attaques réseaux .

4. Session de préparation approfondie à la certification CISSP

Section 5 : Gestion des accès et des identités

Les différents points qui seront traités sont les suivants :

1. Contrôler les accès logiques et physiques aux biens ;
2. Gérer l'identification et l'authentification des personnes et des équipements ;
3. Intégrer le iAAS (identity as a Service) ;
4. Intégrer les solutions tierces de gestion des identités ;
5. I mplémenter et gérer les mécanismes d'autorisation ;
6. Prévenir et gérer les attaques sur les mécanismes de contrôle d'accès ;
7. Gérer les identités et le cycle de provisionning.

Section 6 : Tests et analyses de la sécurité

Les différents points qui seront traités sont les suivants :

1. Concevoir et valider les stratégies de tests ;
2. Réaliser les contrôles de sécurité ;
3. Collecter des données sur le processus de sécurité ;
4. Analyser et répertorier les outputs des tests ;
5. Réaliser des audits tierce-partie.

4. Session de préparation approfondie à la certification CISSP

Section 7 : Les opérations de sécurité

Les différents points qui seront traités sont les suivants :

1. Comprendre et renforcer les investigations ;
2. Comprendre les exigences des différents types d'investigation ;
3. Assurer les activités de monitoring et de journalisation ;
4. Sécuriser le provisionning des ressources ;
5. Comprendre et déployer les principes de base des opérations de sécurité ;
6. Déployer les techniques de protection des ressources ;
7. Concevoir la gestion des incidents ;
8. Concevoir et maintenir les mesures préventives ;
9. Implémenter la gestion des patches et des vulnérabilités ;
10. Implémenter le processus de gestion des changements ;
11. Concevoir les mesures curatives ;
12. Concevoir et tester les plans de secours ;
13. Concevoir et tester les plans de continuité d'activité ;
14. Implémenter et gérer la sécurité physique ;
15. Assurer la sécurité du personnel.

Section 8 : Sécurité de développement des logiciels

Les différents points qui seront traités sont les suivants :

1. Comprendre et déployer la sécurité dans le cycle de vie de développement des logiciels (SDLC) ;
2. Renforcer les contrôles de sécurité au niveau des environnements de développement ;
3. Analyser la robustesse de la sécurité au niveau des applications ;
4. Analyser l'impact sur la sécurité globale des logiciels nouvellement acquis.

4. Session de préparation approfondie à la certification CISSP (Suite et fin)

Section 9 : Préparation à l'Examen CISSP

Examen Blanc

FORMAT

La formation est donnée en français sous forme d' interactions entre les participants et le formateur et d'ateliers pratiques entre les participants dont :
- 3 supports de cours en anglais (langue recommandée pour le passage de l'examen) seront remis à chaque participant.
- Chaque session est limitée à un maximum de 12 personnes

INTERVENANT

Hafedh BEN HAMIDA

• Tunisien résident en France, ingénieur certifié CISSP®, Expert Senior en sécurité des systèmes d'information. Avec plus de 17 ans d'expérience en conseil stratégique, tactique et opérationnel en sécurité pour des grands groupes internationaux et de nombreuses PME/PMI, M.BEN HAMIDA est aujourd'hui l'un des formateurs africains les plus reconnus

Pour avoir plus de détails sur les contenus de la formation veuillez cliquer ici : Formation CISSP