CISSP Préparation à la Certification sécurité

Durée: 5 Jours **Réf de cours: GK9840** **Version: 2021**

Résumé:

La formation GK9840 constitue une excellente préparation à la Certification sécurité CISSP. **En 2020, notre formation de préparation CISSP a recueilli la note de satisfaction de 4,9 sur 5!**
L'international Information Systems Security Certification Consortium – l'ISC2 a développé **la certification CISSP, certification internationale reconnue mondialement par les experts en sécurité informatique,** dans le but de valider les connaissances des experts et d'assurer qu'ils continuent leur formation. L'ISC2 définit un tronc commun de connaissances en sécurité (CBK = Common Body of Knowledge) qui représente les savoirs spécifiques que tous les professionnels du domaine ont en commun et qu'ils utilisent couramment dans l'exercice de leurs tâches. 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.

Public visé:

Cette formation s'adresse aux consultants IT, managers, administrateurs réseaux et ingénieurs sécurité.

Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
- Expliquer comment assurer la sécurité et gérer les risques
- Expliquer comment assurer la sécurité des biens
- Décrire l'Engineering de la sécurité et la cryptographie
- Expliquer comment assurer la sécurité des réseaux et des communications
- Décrire la gestion des accès et des identités
- Définir l'évaluation de la sécurité et des tests
- Expliquer coment assurer la sécurité des Opérations
- Définir la sécurité dans le cycle de vie du développement logiciel

Pré-requis:

Avoir une expérience d'au minimum 5 ans, dans au moins deux des huit domaines couverts par la formation.

Test et certification

Cette formation intensive prépare au passage de la certification CISSP, Certified Information Systems Security Professional .

Contenu:

Sujets du test et techniques de travail

- Préparer l'examen CISSP
- Transférer les documents requis
- Ressources et aides diverses

Gestion de la sécurité et des risques

- Confidentialité, intégrité et concepts de disponibilité
- Principes de la gouvernance de la sécurité
- Conformité
- Problèmes légaux et réglementaires
- Stratégies de sécurité, standards, procédures et lignes directrices

Sécurité des biens

- Information et classification des biens
- Propriétaires des données, prorpriétaires des systèmes
- Protection de la vie privée
- Rétention appropriée
- Contrôles de la sécurité des données
- Tenir compte des exigences (stockage, marquage, étiquettage)

Engineering de la sécurité

- Process d'engineering via des principes sécurisés de conception
- Concepts fondamentaux des modèles de sécurité
- Modèles d'évaluation de la sécruité
- Possibilité de sécurisation des systèmes d'information
- Architecture sécurisée, conceptions et vulnérabilités des éléments de la solution
- Vulnérabilités des systèmes basés sur le Web
- Vulnérabilités des systèmes mobiles
- Périphériques embarqués et vulnérabilités des systèmes cyber-physiques
- Cryptographie
- Site et principes de conception sécurisée
- Sécurité physique

Sécurité des réseaux et des communications

- Conception d'une architecture réseau sécurisée
- Sécuriser les composants réseaux
- Sécrire les canaux de communications
- Attaques réseaux

Gestion des accès et des identités

- Contrôle des biens logiques et physiques
- Identification et authentification des personnes et des périphériques
- Identity as a Service (Identité dans le cloud)
- Services d'identité tierce peresonne (sur site)
- Attaques de contrôle d'accès
- Cycle de vie des accès et des identités

Evaluation de la sécurité et des tests

- Evaluation et stratégies de tests
- Données de processus de sécurité
- Tests de contrôle de sécurité
- Tests automatisés, tests manuels
- Vulnérabilités des architectures de sécurité

Sécurité des Opérations

- Support et exigences
- Connexion et surveillance des activités
- Fournir des ressources
- Concepts de base de sécurité des opérations
- Techniques de protection des ressources
- Gestion des incidents
- Mesures préventives
- Patch et gestion des vulnérabilités
- Changer la gestion des process
- Stratégies de récupération
- Process de récupération d'urgenceet plans
- Planning de continuité du Business et exercices
- Sécurité physique
- Problèmes de sécurité personnelle

Sécurité du dévelopement logiciel

- Sécurité dans le cycle de vie du développement logiciel
- Contrôles de sécurité de l'environnement de développement
- Efficacité de la sécurité logicielle
- Impact sur la sécurité logicielle

Rappels et Questions / réponses

Méthodes pédagogiques :

Supports de cours remis aux participants

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• Modalités d'évaluation : le participant est invité à s'auto-évaluer par rapport aux objectifs énoncés.
• Chaque participant, à l'issue de la formation, répond à un questionnaire de satisfaction qui est ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

•Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
•Votre place sera confirmée à la réception d'un devis ou ""booking form"" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
•Attention, si vous utilisez votre Compte Personnel de Formation pour financer votre inscription, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés.