CISSP-Certified Information Systems Security Professional - Préparation à la Certification sécurité

Durée: 5 Jours **Réf de cours: GK9803** **Méthodes d'apprentissage: Intra-entreprise & sur-mesure**

Résumé:

Acquérir les connaissances et l'expérience essentielles pour mettre en œuvre et gérer avec succès des programmes de sécurité et se préparer à la certification CISSP. Cette formation est la revue la plus complète des concepts de sécurité de l'information et des meilleures pratiques du secteur, et se concentre sur les huit domaines du CISSP CBK (Common Body of Knowledge) qui sont couverts par l'examen CISSP. Les participants acquerront des connaissances en matière de sécurité de l'information qui leur permettront d'accroître leur capacité à mettre en œuvre et à gérer avec succès des programmes de sécurité dans toute organisation ou entité gouvernementale.
Pourquoi suivre le cours de préparation à la certification CISSP ?
L'examen CISSP est difficile, mais les avantages sont immenses. En raison de sa portée globale, CISSP est la certification de facto pour démontrer la compétence dans les rôles cybernétiques. C'est également l'une des certifications les mieux rémunérées dans le domaine de l'informatique.
Mise à jour : 06.11.2023

Public visé:

Cette formation aux personnes qui cherchent à établir les meilleures pratiques en matière de sécurité de l'information au sein de leur organisation ou celles qui cherchent à faire progresser leur carrière dans le domaine de la sécurité de l'information.

Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
- Comprendre de façon approfondie les six domaines requis pour réussir l'examen CCSP :
- Sécurité et gestion des risques
- Sécurité des actifs
- Architecture et ingénierie de la sécurité
- Sécurité des communications et des réseaux
- Gestion des identités et des accès (IAM)
- Évaluation et test de la sécurité
- Opérations de sécurité
- Sécurité du développement logiciel

Pré-requis:

Les participants doivent remplir les conditions préalables suivantes :

- Un minimum de 5 ans d'expérience dans le domaine des infrastructures informatiques et de la cybersécurité
- 9701 - Cybersecurity Foundations
- G013 - Formation CompTIA Security+

Test et certification

Recommandé comme préparation aux examens suivants :

- CISSP - Professionnel certifié en sécurité des systèmes d'information

Pour obtenir cette certification en cybersécurité, vous devez réussir l'examen et avoir au moins cinq ans d'expérience professionnelle cumulée et rémunérée dans au moins deux des huit domaines du (ISC)² CISSP Common Body of Knowledge (CBK).

Il est possible de satisfaire à l'exigence d'une année d'expérience professionnelle en obtenant un diplôme universitaire pertinent de quatre ans ou en détenant un titre approuvé.

Même si vous n'avez pas le niveau d'expérience requis, vous pouvez passer l'examen CISSP et devenir un Associate of (ISC)² tout en acquérant l'expérience professionnelle requise.

Après cette formation, nous vous conseillons le(s) module(s) suivant(s):

- GK1642 - SSCP-Systems Security Certified Practitioner - Préparation à la Certification sécurité

Contenu:

Sécurité et gestion des risques (p. ex., sécurité, risques, conformité, lois, règlements, continuité des activités)

- Comprendre et appliquer les concepts de confidentialité, d'intégrité et de disponibilité.
- Appliquer les principes de gouvernance de la sécurité
- Conformité
- Comprendre les questions juridiques et réglementaires relatives à la sécurité de l'information dans un contexte mondial.
- Développer et mettre en œuvre une politique, des normes, des procédures et des directives documentées en matière de sécurité.
- Comprendre les exigences en matière de continuité des activités
- Contribuer aux politiques de sécurité du personnel
- Comprendre et appliquer les concepts de gestion des risques
- Comprendre et appliquer la modélisation des menaces
- Intégrer les considérations relatives au risque de sécurité dans la stratégie et les pratiques d'acquisition.
- Établir et gérer l'éducation, la formation et la sensibilisation à la sécurité

Sécurité des actifs (protection de la sécurité des actifs)

- Classifier les informations et les biens de soutien
- Déterminer et maintenir la propriété
- Protéger la vie privée
- Assurer une conservation appropriée
- Déterminer les contrôles de sécurité des données
- Établir les exigences de manipulation

Ingénierie de la sécurité (ingénierie et gestion de la sécurité)

- Mettre en œuvre et gérer un cycle de vie d'ingénierie en utilisant les principes de conception de la sécurité
- Comprendre les concepts fondamentaux des modèles de sécurité
- Sélectionner les contrôles et les contre-mesures en fonction des normes de sécurité des systèmes d'information
- Comprendre les capacités de sécurité des systèmes d'information
- Évaluer et atténuer les vulnérabilités des architectures, conceptions et éléments de solution de sécurité
- Évaluer et atténuer les vulnérabilités des systèmes basés sur le Web
- Évaluer et atténuer les vulnérabilités des systèmes mobiles
- Évaluer et atténuer les vulnérabilités des

Sécurité des communications et des réseaux (conception et protection de la sécurité des réseaux)

- Appliquer les principes de conception sécurisée à l'architecture des réseaux
- Sécuriser les composants du réseau
- Concevoir et établir des canaux de communication sécurisés
- Prévenir ou atténuer les attaques de réseau

Gestion des identités et des accès (Contrôle des accès et gestion des identités)

- Contrôler l'accès physique et logique aux actifs
- Gérer l'identification et l'authentification des personnes et des appareils
- Intégrer l'identité en tant que service (IDaaS)
- Intégration de services d'identité tiers
- Mettre en œuvre et gérer les mécanismes d'autorisation
- Prévenir ou atténuer les attaques de contrôle d'accès
- Gérer le cycle de vie du provisionnement des identités et des accès

Évaluation et tests de sécurité (conception, exécution et analyse des tests de sécurité)

- Concevoir et valider les stratégies d'évaluation et de test
- Effectuer des tests de contrôle de sécurité
- Collecte de données sur les processus de sécurité
- Mener ou faciliter les audits internes et tiers

Opérations de sécurité (par exemple, concepts de base, enquêtes, gestion des incidents, reprise après sinistre)

- Comprendre et soutenir les enquêtes
- Comprendre les exigences relatives aux types d'enquêtes
- Mener des activités de journalisation et de surveillance
- Sécuriser le provisionnement des ressources par la gestion de la configuration
- Comprendre et appliquer les concepts de base des opérations de sécurité
- Utiliser des techniques de protection des ressources
- Effectuer une réponse aux incidents
- Exploiter et maintenir des mesures préventives
- Mettre en œuvre et soutenir la gestion des correctifs et des vulnérabilités
- Participer aux processus de gestion du changement et les comprendre
- Mettre en œuvre des stratégies de récupération
- Mettre en œuvre des processus de reprise après sinistre
- Tester le plan de reprise après sinistre
- Participer à la planification de la continuité des activités
- Mettre en œuvre et gérer la sécurité physique
- Participer à la sécurité du personnel

Sécurité du développement logiciel (comprendre, appliquer et faire respecter la sécurité logicielle)

- Comprendre et appliquer la sécurité dans le cycle de vie du développement logiciel
- Appliquer les contrôles de sécurité dans l'environnement de développement
- Évaluer l'efficacité de la sécurité des logiciels
- Évaluer la sécurité de l'acquisition des logiciels

dispositifs embarqués et des systèmes cyber-physiques.
- Appliquer la cryptographie
- Appliquer les principes de sécurité à la conception des sites et des installations
- Concevoir et mettre en œuvre la sécurité des installations

Méthodes pédagogiques :

Support de cours officiel remis aux participants
Les participants réalisent un test d'évaluation des connaissances en amont et en aval de la formation pour valider les connaissances acquises pendant la formation.

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.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera 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 cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement