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

Durée: 5 Jours **Réf de cours: GK9803** **Méthodes d'apprentissage: Classe à distance**

Résumé:

Acquérir les connaissances et l'expérience nécessaires pour mettre en œuvre et gérer avec succès les programmes de sécurité et se préparer à la certification CISSP 2024.
Ce cours mis à jour en 2024 est la révision la plus complète des concepts de sécurité de l'information et des meilleures pratiques de l'industrie, en se concentrant sur les huit domaines du CISSP-CBK (Common Body of Knowledge) qui sont couverts par l'examen CISSP.
Vous développerez des connaissances en matière de sécurité de l'information qui vous permettront de mettre en œuvre et de gérer avec succès des programmes de sécurité dans n'importe quelle organisation ou entité gouvernementale.
En plus d'un manuel, vous avez également accès à l'environnement d'apprentissage interactif en ligne de Sybex qui comprend :
Plus de 900 questions d'examen pratique avec des explications complètes des réponses.
Plus de 1000 Flashcards électroniques
Un glossaire consultable en PDF pour vous donner un accès instantané aux termes clés que vous devez connaître.

Mis à jour le 18 06 2024

Public visé:

Ce cours est destiné à:
Toute personne dont le poste exige une certification CISSP
Les personnes qui souhaitent progresser dans leur carrière actuelle en sécurité informatique ou se diriger vers une carrière similaire

Objectifs pédagogiques:

- Ce cours couvre en détail les huit domaines requis pour réussir l'examen CISSP :
- Gestion des identités et des accès (IAM)
- Évaluation et test de la sécurité
- Gestion de la sécurité et des risques
- Opérations de sécurité
- Sécurité des actifs
- Sécurité du développement de logiciels
- Architecture et ingénierie de la sécurité
- Sécurité des communications et des réseaux

Pré-requis:

Pour pouvoir suivre ce cours avec succès, vous devez avoir au moins cinq ans d'expérience dans le domaine de l'infrastructure informatique et de la cybersécurité.

Avez-vous les compétences requises pour cette formation ?
Testez vos connaissances !

- 9701 - Cybersecurity Foundations
- G013 - Formation CompTIA Security+

Test et certification

Ce cours vous prépare à l'examen 2024 ISC(2) CISSP.
L'examen lui-même ne fait pas partie de ce cours.
Nous recommandons de passer l'examen peu de temps après avoir terminé le cours, en réservant au moins 2 semaines pour que votre préparation à l'examen soit compatible avec votre charge de travail et vos horaires habituels.

Vous pouvez également utiliser les questions pratiques qui vous seront fournies au début du cours pour évaluer votre niveau de préparation.

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

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

Contenu:

Chapitre 1 La gouvernance de la sécurité à travers les principes et les politiques

- Sécurité 101
- Comprendre et appliquer les concepts de sécurité
- Les limites de la sécurité
- Évaluer et appliquer les principes de gouvernance de la sécurité
- Gérer la fonction de sécurité
- Politique de sécurité, normes, procédures et lignes directrices
- Modélisation des menaces
- Gestion des risques de la chaîne d'approvisionnement

Chapitre 2 Concepts de sécurité du personnel et de gestion des risques

- Politiques et procédures de sécurité du personnel
- Comprendre et appliquer les concepts de gestion des risques
- Ingénierie sociale
- Établir et maintenir un programme de sensibilisation, d'éducation et de formation à la sécurité

Chapitre 3 Planification de la continuité des activités

- Planification de la continuité des activités
- Portée et planification du projet
- Analyse de l'impact sur l'entreprise
- Planification de la continuitéApprobation et mise en œuvre du plan

Chapitre 4 Lois, réglementations et conformité

- Catégories de lois
- Lois nationales sur la protection de la vie privée
- Conformité
- Contrats et marchés publics

Chapitre 5 Protection de la sécurité des actifs

- Identifier et classer les informations et les biens
- Établir les exigences en matière de traitement des informations et des biens
- Méthodes de protection des données
- Comprendre les rôles des données
- Utilisation des lignes de base de sécurité

Chapitre 6 Cryptographie et algorithmes à clé symétrique

- Fondements de la cryptographie
- Cryptographie moderne
- Cryptographie symétrique
- Cycle de vie de la cryptographie

Chapitre 8 Principes des modèles, de la conception et des capacités de sécurité

- Principes de conception sécurisée
- Techniques pour garantir la CIA
- Comprendre les concepts fondamentaux des modèles de sécurité
- Sélectionner les contrôles sur la base des exigences de sécurité des systèmes
- Comprendre les capacités de sécurité

Chapitre 9 Vulnérabilités, menaces et contre-mesures en matière de sécurité

- Responsabilité partagée
- Localisation et souveraineté des données
- Évaluer et atténuer les vulnérabilités des architectures de sécurité, des conceptions et des éléments de solution
- Systèmes basés sur les clients
- Systèmes basés sur des serveurs
- Systèmes de contrôle industriel
- Systèmes distribués
- Systèmes de calcul à haute performance (HPC)
- Systèmes d'exploitation en temps réel
- Internet des objetsInformatique en périphérie et Fog Computing
- Dispositifs embarqués et systèmes cyber-physiques
- Microservices
- Infrastructure en tant que code
- Architecture immuable
- Systèmes virtualisés
- Conteneurisation
- Dispositifs mobiles
- Mécanismes essentiels de protection de la sécurité
- Défauts et problèmes courants de l'architecture de sécurité

Chapitre 10 Exigences en matière de sécurité physique

- Appliquer les principes de sécurité à la conception du site et de l'installation
- Mettre en œuvre les contrôles de sécurité du site et de l'installation
- Mettre en œuvre et gérer la sécurité physique

Chapitre 11 Architecture et composants d'un réseau sécurisé

- Modèle OSI
- Modèle TCP/IP
- Analyse du trafic réseau
- Protocoles communs de la couche application
- Protocoles de la couche transport
- Système de noms de domaine
- Protocole Internet (IP)
- Problèmes liés à l'ARP

Chapitre 15 Évaluation et test de la sécurité

- Mise en place d'un programme d'évaluation et de test de la sécurité
- Évaluer les vulnérabilités
- Tester vos logiciels
- Formation et exercices
- Mise en œuvre des processus de gestion de la sécurité et collecte des données relatives aux processus de sécurité

Chapitre 16 Gestion des opérations de sécurité

- Appliquer les concepts fondamentaux des opérations de sécurité
- Assurer la sécurité du personnel
- Fournir des informations et des actifs en toute sécurité
- Services gérés dans le cloud
- Effectuer la gestion de la configuration (CM)
- Gérer les changements
- Gérer les correctifs et réduire les vulnérabilités

Chapitre 17 Prévenir les incidents et y répondre

- Gestion des incidents
- Mise en œuvre de mesures de détection et de prévention
- Journalisation et surveillance
- Automatisation de la réponse aux incidents

Chapitre 18 Planification de la reprise après sinistre

- La nature du sinistre
- Comprendre la résilience des systèmes, la haute disponibilité et la tolérance aux pannes
- Stratégie de reprise
- Élaboration d'un plan de reprise
- Formation, sensibilisation et documentation
- Tests et maintenance

Chapitre 19 Enquêtes et éthique

- Enquêtes
- Principales catégories de délits informatiques
- Éthique

Chapitre 20 Sécurité du développement de logiciels

- Introduction des contrôles de développement de systèmes
- Mise en place de bases de données et d'entrepôts de données
- Menaces sur le stockage

Chapitre 7 ICP et applications cryptographiques

- Cryptographie asymétrique
- Fonctions de hachage
- Signatures numériques
- Infrastructure à clé publique
- Gestion des clés asymétriques
- Cryptographie hybride
- Cryptographie appliquée
- Attaques cryptographiques

- Protocoles de communication sécurisés
- Implications des protocoles multicouches
- Segmentation
- Réseaux périphériques
- Réseaux sans fil
- Communications par satellite
- Réseaux cellulaires
- Réseaux de distribution de contenu (CDN)
- Composants des réseaux sécurisés

Chapitre 12 Communications sécurisées et attaques sur les réseaux

- Mécanismes de sécurité des protocoles
- Communications vocales sécurisées
- Gestion de la sécurité de l'accès à distance
- Collaboration multimédia
- Surveillance et gestion
- Équilibrage de charge
- Gestion de la sécurité du courrier électronique
- Réseau privé virtuel
- Commutation et réseaux locaux virtuels
- Traduction d'adresses de réseau
- Connectivité avec des tiers
- echnologies de commutation
- Technologies WAN
- Liaisons par fibre optique
- Prévenir ou atténuer les attaques du réseau

Chapitre 13 Gestion de l'identité et de l'authentification

- Contrôler l'accès aux ressources
- Le modèle AAA
- Mise en œuvre de la gestion des identités
- Gestion du cycle de vie du provisionnement des identités et des accès

Chapitre 14 Contrôle et surveillance des accès

- Comparaison des modèles de contrôle d'accès
- Mise en œuvre des systèmes d'authentification
- Application de la politique d'accès de confiance zéro
- Comprendre les attaques de contrôle d'accès
- Comprendre les systèmes basés sur la connaissance

Chapitre 21 Attaques contre les codes malveillants et les applications

- Les logiciels malveillants
- Prévention des logiciels malveillants
- Attaques d'applications
- Vulnérabilités d'injection
- Exploitation des vulnérabilités d'autorisation
- Exploitation des vulnérabilités des applications Web
- Contrôles de sécurité des applications
- Pratiques de codage sécurisées

Méthodes pédagogiques :

Un support de cours est 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