SECURIDAY

PRÉSENTIEL/ DISTANCIEL

CISSP PRÉPARATION

Préparez-vous à la Certification mondialement reconnue en Cybersécurité - Sécurité des Systèmes d'Information

Notre cours de formation est une expérience d'apprentissage adaptable et unique avec +1300 questions et 8 domaines nécessaires pour réussir l'examen. La plateforme e-learning de Securiday vous aidera à maîtriser chaque domaine grâce à des examens pratiques, des quiz et du coaching personnalisé.

LIEUX (2024) :

- ✓ Annecy 09 Sept, 07 Oct.,04 Nov., 02 Déc.
- ✓ Grenoble 23 Sept., 21 Oct., 18 Nov., 16 Déc.
- ✓ Paris/Lyon: 16 Sept.,14 Oct.,09 Déc
- ✓ Chamonix 30 Sept., 25 Nov.

A distance : 09 Sept., 16 Sept., 23 Sept., 30 Sept., 07 Oct., 14 Oct., 21 Oct., 04 Nov., 25 Nov., 02 Déc, 09 Déc., 16 Déc.

Contact : info@securiday.io www.securiday.io

PARTICIPANTS

Responsables "Cyber" ou toute autre personne jouant un rôle dans la sécurité des TI.

PRÉREQUIS

La certification CISSP® n'est pas destinée aux nouveaux entrants dans le secteur de la cybersécurité informatique et des systèmes d'information.

Les candidats doivent avoir au moins cinq ans ou plus d'expérience de travail global avant de passer la certification CISSP®.

Les candidats doivent également avoir une expérience de travail pertinente dans au moins deux des huit domaines couverts par la certification.

COMPÉTENCES DU FORMATEUR

Directeur de la Cybersécurité/TI, MBA en Sécurité des Systèmes d'Information, validé par les équipes pédagogiques des organismes de formation tant sur le plan des connaissances métiers que sur celui de la pédagogie.

Votre formateur a plus de vingt années d'expérience dans le domaine et occupe des postes à responsabilité en entreprise.

MODALITÉS ET DÉLAIS D'ACCÈS

Pour vous inscrire à cette formation, il vous suffit de remplir le formulaire en fonction des lieux et dates souhaitées disponibles en ligne : https://www.securiday.io/8-domaines-a-connaitre-pour-reussir-la-certification-CISSP-avec-SECURIDAY.html

MOYENS PÉDAGOGIQUES ET TECHNIQUES

Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices, études de cas ou présentation de cas réels dispensés en présentiel ou via la plateforme d'apprentissage en ligne.

À l'issue de chaque stage ou séminaire, SECURIDAY fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé.

Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez-nous, à l'adresse suivante info@securiday.io pour étudier au mieux votre demande et sa faisabilité.

Contact : info@securiday.io www.securiday.io

GESTION DE LA SÉCURITÉ ET DES RISQUES (D1)

Ce domaine vaut 16 % de la note à atteindre. Il comprend :

- Éthique professionnelle
- Concepts de sécurité
- Principes de gouvernance de la sécurité
- Conformité et les autres exigences
- Questions juridiques et réglementaires liées à la sécurité de l'information dans un contexte holistique
- Exigences relatives aux types d'enquête
- Politiques, des normes, des procédures et des lignes directrices
- Exigences en matière de continuité des opérations (BC)
- Politiques et procédures de sécurité du personnel
- Concepts de gestion des risques
- Concepts et les méthodologies de modélisation des menaces
- Gestion des risques de la chaîne d'approvisionnement (SCRM)
- Programme de sensibilisation, d'éducation et de formation en matière de sécurité

SÉCURITÉ DES BIENS (D2)

Ce domaine vaut 10 % de la note à atteindre. Il comprend :

- Identifier et classer l'information et les biens
- Établir des exigences en matière d'information et de gestion des biens
- Fournir des ressources en toute sécurité
- Gérer le cycle de vie des données
- Assurer une rétention appropriée des actifs
- Déterminer les contrôles de sécurité des données et les exigences de conformité

SÉCURITÉ DES COMMUNICATIONS ET DES RÉSEAUX (D4)

ARCHITECTURE DE SÉCURITÉ ET INGÉNIERIE (D3)

Ce domaine vaut 13 % de la note à atteindre et comprend :

- Recherche, mise en œuvre et gestion des processus d'ingénierie utilisant des principes de conception sécurisés
- Comprendre les concepts fondamentaux des modèles de sécurité
- Sélectionner les contrôles basés sur les exigences des Systèmes de Sécurité
- Comprendre les capacités de sécurité des systèmes d'information
- Évaluer et atténuer les vulnérabilités de sécurité d'architectures, conceptions, et éléments de solution
- Sélectionner et déterminer les solutions cryptographiques
- Comprendre les méthodes des attaques cryptanalytiques
- Appliquer les principes de sécurité à la conception du site et des installations
- Contrôles de sécurité des sites de conception et des installations

Ce domaine vaut 13 % de la note à atteindre et comprend :

Évaluer et appliquer des principes de conception sécurisés dans les architectures de réseau

Composants réseau sécurisés

- Mettre en œuvre des canaux de communication sécurisés selon la conception

Contact : info@securiday.io www.securiday.io

GESTION DES IDENTITÉS ET DES ACCÈS (D5)

Ce domaine vaut 13 % de la note à atteindre et comprend :

- Contrôler l'accès physique et logique aux biens
- Gérer l'identification et l'authentification des personnes, des appareils et des services
- Identité fédérée avec un service tiers
- Mettre en œuvre et gérer les mécanismes d'autorisation
- Gérer le cycle de vie du provisionnement des identités et des accès
- Mettre en place des systèmes d'authentification

EVALUATION ET TEST DE LA SÉCURITÉ (D6)

Ce domaine vaut 12 % de la note à atteindre. Il comprend :

- Concevoir et valider des stratégies d'évaluation, de test et de vérification
- Effectuer des essais des contrôles de sécurité
- Recueillir des données sur les processus de sécurité (par exemple techniques et administratives)
- Analyser la sortie du test et générer un rapport
- Effectuer ou faciliter des audits de sécurité

SÉCURITÉ DU DÉVELOPPEMENT DES LOGICIELS (D8)

Ce domaine vaut 10 % du la note à atteindre. Il comprend :

Comprendre et intégrer la sécurité dans le cycle de vie du développement logiciel(SDLC)
Identifier et appliquer des contrôles de sécurité dans les écosystèmes de développement logicielcosystems)

-

SÉCURITÉ OPÉRATIONNELLE (D7)

Ce domaine vaut 13 % du la note à atteindre. il comprend :

Comprendre et respecter les enquêtes
Mener des activités d'enregistrement et de surveillance
Effectuer la gestion de la configuration (CM) (par exemple, provisioning, baselining, automatisation)
Appliquer les concepts fondamentaux des opérations de sécurité
Appliquer la protection des ressources
Gérer les incidents
Appliquer et maintenir des mesures de détection et de prévention
Implémenter et gérer les correctifs et les vulnérabilités
Comprendre les processus de gestion du changement et y participer
Mettre en œuvre des stratégies de rétablissement
Mettre en œuvre des processus de reprise après sinistre
Mise à l'essai des plans de reprise après sinistre
Participer à la planification et aux exercices de continuité des activités
Mettre en œuvre et gérer la sécurité physique
Répondre aux préoccupations en matière de sécurité et de sûreté du personnel

Évaluer l'efficacité de la sécurité des logiciels
Évaluer l'impact sur la sécurité des logiciels acquis
Définir et appliquer des lignes directrices et des normes de codage sécurisées.

Contact : info@securiday.io www.securiday.io