CISSP® : devenir expert en sécurité des SI

Date et durée

Code formation : CIS01FR
Durée : 5 jours
Nombre d'heures : 35 heures

Formation avec certification

CISSP® : Certified Information Systems Security Professional

Description

La formation CISSP® (*Certified Information Systems Security Professional*)**,** s'adresse aux professionnels possédant un **haut niveau d'expertise en sécurité informatique**. Elle est notamment adaptée pour les responsables de la sécurité des systèmes d'information (RSSI) et pour les directeurs des systèmes d'information (DSI). Toutefois, cette formation certifiante est **utile dans plusieurs métiers**, puisqu'elle aborde des compétences spécifiques dans le domaine de la cybersécurité.
Pendant 5 jours intensifs, chaque cours CISSP est dispensé par **un formateur accrédité par l'ISC2** qui vous préparera à cette prestigieuse certification. Conformément aux exigences de certification, cette formation couvrira **les 8 domaines clés du corpus de connaissances (CBK)**. Ceux-ci incluent la sécurité et la gestion des risques, la sécurité des actifs, l'architecture et l'ingénierie de la sécurité, la sécurité des communications et des réseaux, la gestion des identités et des accès, l'évaluation et les tests de sécurité, les opérations de sécurité et la sécurité pour le développement des logiciels.
Grâce à **des quiz, des études de cas réels et des discussions interactives**, vous acquerrez les compétences dont vous avez besoin pour relever des défis complexes en matière de sécurité informatique. De plus, vous obtiendrez **le plus haut niveau de certification** en tant que professionnel de la sécurité des systèmes d'information.

Oo2 est un partenaire de formation (ATP), agréée par l'ISC². Les ATPs sont des organismes habilités à dispenser des formations certifiantes conforme aux normes de qualité rigoureuses de l'ISC². Une enquête récente démontre que plus de 80 % des organisations préfèrent travailler avec un organisme agréé.

Objectifs

A l'issue de cette **formation CISSP®**, vous devrez être capable de valider les objectifs de compétences suivants :

- connaître les 8 domaines du Common Body of Knowledge défini par l'(ISC)²;
- acquérir des compétences et des connaissances avancées en sécurité des systèmes d'information et en gestion des risques informatique ;
- passer l'examen officiel CISSP® et décrocher votre certification.

Points forts

Un formateur agréé par l'(ISC)², des supports de cours officiels, le passage de l'examen CISSP® compris dans l'offre, des conseils, des quiz d'évaluation et des études de cas.

Certification

Cette formation s'adresse aux professionnels de la sécurité de l'information disposant de connaissances techniques et managériales avancées et d'une solide expérience. Elle permet de passer **l'examen de certification CISSP disponible en ligne et en anglais** uniquement. (*un bon d'examen vous sera remis à l'issue de la formation*).
Pour obtenir votre certification CISSP®, vous devez remplir les conditions suivantes :

- avoir une expérience professionnelle cumulée de 5 ans minimum dans au moins 2 des 8 domaines du corpus de connaissances (CBK) de l'ISC2. Des dérogations peuvent être accordées aux personnes qui possèdent d'autres certifications en sécurité informatique ou des diplômes universitaires.
- créer un compte sur le site de l'ISC2, s'inscrire à l'examen et signer le code de déontologie ;
- passer et réussir l'examen CISSP qui consiste à répondre à un QCM entre 125 et 75 questions en 4 heures et obtenir un score de 700 points sur 1000;
- accepter un audit périodique de ses compétences et de ses connaissances.

A savoir : *une fois obtenue, la certification CISSP est valable 3 ans. Pour la renouveler, vous devrez suivre un minimum de 120 heures de formation continue en cybersécurité à la fin de cette période de validité.*

Modalités d'évaluation

Quiz / QCM
Etude de cas

Pré-requis

Suivre la **formation CISSP ®** nécessite les prérequis suivants :

- des compétences fondamentales sur les réseaux, les systèmes d'exploitation et sur les pratiques de la sécurité de l'information ;
- des notions élémentaires sur les normes d'audit et les normes internationales de gestion de continuité des activités.
- savoir lire et comprendre l'anglais afin de pouvoir consulter les supports de cours et passer l'examen CISSP®.

Public

Cette formation s'adresse aux publics suivants :

- les auditeurs informatiques souhaitant obtenir la certification CISSP® ;
- les professionnels de la sécurité informatique ou les gestionnaires de systèmes informatiques.

Cette formation s'adresse aux profils suivants

Administrateur système
Ingénieur système
Directeur des Systèmes d'Information (DSI)
Responsable sécurité informatique
Analyste cybersécurité
Auditeur interne / externe

Programme

Tour de table

- Introduction individuelle
- Exploration des attentes et des objectifs de chaque participant
- Introduction au cadre de la formation
- Alignement avec les objectifs et enjeux spécifiques
- Identification des attentes et des perspectives individuelles des participants

---

Domaine 1 : la sécurité et la gestion des risques

- Compréhension, respect et valorisation de l'éthique professionnelle.
- Compréhension et mise en œuvre des concepts de sécurité.
- Évaluation et mise en œuvre des principes de gouvernance de la sécurité.
- Définition des exigences en matière de conformité et d'autres aspects.
- Compréhension sur les aspects juridiques et règlementaires liés à la sécurité de l'information dans un contexte holistique.
- Compréhension des exigences relatives aux types d'enquêtes (administratives, pénales, civiles, etc.).
- Élaboration, documentation et mise en œuvre des politiques, des normes, des procédures et des lignes directrices en matière de sécurité.
- Identification, analyse et hiérarchisation des exigences en matière de continuité des activités.
- Contribution aux politiques et procédures de sécurité du personnel et mise en œuvre des mesures correspondantes.
- Compréhension et mise en œuvre des concepts de gestion des risques.
- Compréhension et mise en œuvre des concepts et des méthodologies de modélisation sur les menaces.
- Application des principes de gestion des risques pour la chaine d'approvisionnement.
- Création et maintien d'un programme de sensibilisation, d'éducation et de formation à la sécurité.

Domaine 2 : la sécurité des actifs

- Identification et classification des informations et des actifs.
- Définition des exigences en matière de gestion de l'information et des actifs.
- Mise à disposition des ressources de manière sécurisée.
- Gestion du cycle de vie des données.
- Mise en place de mesures de conservation des actifs (exemple : fin de vie et fin de support).
- Identification des contrôles de sécurité des données et des exigences de conformité.

Domaine 3 : l'architecture et l'ingénierie de sécurité

- Recherche, implémentation et gestion des processus d'ingénierie à l'aide de principes de conception sécurisés.
- compréhension des concepts fondamentaux des modèles de sécurité (Biba, Star Model, Bell-LaPadula, etc.).

- Sélection des mesures de contrôle en fonction des exigences de sécurité du système.
- Compréhension des capacités de sécurité des systèmes d'information (protection de la mémoire, Trusted Platform Module (TPM), cryptage et décryptage).
- Évaluation et atténuation des vulnérabilités des architectures, des conceptions et des éléments de solution en matière de sécurité.
- Sélection et mise au point de solutions cryptographiques.
- Compréhension des méthodes d'attaque par cryptographie.
- Mise en pratique des principes de sécurité dans la conception du site et de ses équipements.
- Conception des contrôles de sécurité du site et des équipements.

Domaine 4 : la sécurité des communications et des réseaux

- Évaluation et mise en œuvre des principes de conception sécurisés pour les architectures réseau.
- Sécurisation des composants du réseau.
- Mise en œuvre de canaux de communication sécurisés conformément à la conception.

Domaine 5 : la gestion des identités et des accès

- Contrôle de l'accès physique et logique des actifs.
- Gestion de l'identification et de l'authentification des personnes, des appareils et des services.
- Identification unifiée avec des services tiers.
- Implémentation et gestion des systèmes d'autorisation.
- Gestion du cycle de vie du provisionnement de l'identité et de l'accès.
- Mise en œuvre de système d'authentification.

Domaine 6 : l'évaluation et les tests de sécurité

- Conception et validation des stratégies d'évaluation, de test et d'audit.
- Réalisation de tests de contrôle pour la sécurité.
- Récupération de données à partir des processus de sécurité.
- Analyse des résultats des tests et rédaction de rapports.
- Réalisation et facilitation des audits de sécurité.

Domaine 7 : les opérations de sécurité

- Compréhension et acceptation des enquêtes.
- Réalisation d'activités de journalisation et de surveillance.
- Gestion de la configuration CM (approvisionnement, référencement, automatisation, etc.).
- Mise en œuvre des concepts fondamentaux des opérations de sécurité.
- Mise en œuvre des mesures de protection des ressources.
- Gestion des incidents.
- Utilisation et maintien des mesures de détection et de prévention.
- Mise en œuvre et suivi de la gestion des correctifs et des vulnérabilités.
- Compréhension des processus de gestion du changement et participation dans ces processus.
- Mise en œuvre de stratégies de récupération.
- Mise en œuvre des processus de reprise après sinistre.
- Évaluation des plans de reprise après sinistre.
- Participation à la planification et aux exercices de continuité des activités.
- Mise en œuvre et gestion de la sécurité physique.
- Gestion des problèmes de sureté et de sécurité du personnel.

Domaine 8 : la sécurité du développement logiciel

- Compréhension et intégration de la sécurité dans le cycle de développement des logiciels.
- Identification et application des contrôles de sécurité dans les écosystèmes de développement logiciel.

- Évaluation de l'efficacité de la sécurité des logiciels.
- Évaluation de l'impact sur la sécurité des logiciels achetés.
- Définition et application des lignes directrices et des normes de codage sécurisées.

Préparation à l'examen CISSP

- Conseils et astuces.
- Quiz d'évaluations.

Contenu de formation proposé en partenariat avec (ISC)²
CISSP® est une marque déposée par (ISC)²

Guide de certification
CISSP®
Télécharger la brochure