CISSP

Certified Information Systems Security Professional

Informations générales

- **Public visé** : Experts de la sécurité des systèmes d'information qui souhaitent se préparer à la certification professionnelle délivrée par l'(ISC²), le CISSP®.
- **Méthodes pédagogiques :** Théorie, demonstrations, retour d'experience.
- **Contenu du kit de formation :** Cours officiel ISC2 CISSP (format papier + contenus numériques). Livre officiel ISC2 CISSP Practice Exams (+ de 250 questions pratiques couvrant les 8 domaines, des questions concrètes avec des réponses expliquées et détaillées).
- **Prérequis** : Justifier de 5 ans d'expérience professionnelle dans au moins 2 des 8 domaines du CBK® (possible de passer l'examen sans cette expérience, un titre intermédiaire temporaire sera alors délivré). Maitrise de l'anglais technique pour supports de formation.
- **Accessibilité** : Formation accessible à tout public. N'hésitez pas à nous faire part de toutes demandes spécifiques afin que l'on adapte au mieux nos modalités de formation (aménagement des horaires, des lieux, des supports…)
- **Evaluation** : Certification incluse (mais non obligatoire) en centre pearsonvue. QCM 100 à 150 questions environ. Durée variable, jusqu'à 3 heures (en anglais).
  Score habituellement requis : 70%

Objectifs pédagogique

- Maîtriser les huit chapitres du Common Body of Knowledge (CBK) de la sécurité IT pour garantir une compréhension complète des meilleures pratiques et des normes en matière de sécurité
- Évaluer les enjeux de sécurité IT à l'échelle organisationnelle pour développer une vision globale des risques et des impacts potentiels sur l'entreprise
- Approfondir les connaissances des huit domaines du CISSP afin de pouvoir appliquer ces concepts à des scénarios réels de gestion de la sécurité
- Préparer de manière stratégique à l'examen de certification du CISSP en développant des compétences d'étude et en révisant les matières clés du CBK
- Analyser les politiques de sécurité et les réglementations afin d'identifier les lacunes et de recommander des améliorations pour une meilleure conformité
- Appliquer des frameworks de gestion des risques pour évaluer les menaces et vulnérabilités au sein d'un environnement IT complexe

Programme détaillé

Jour 1
Domaine 1 Security and Risk Management
Domaine 2 Asset Security
Domaine 3 : Security Architecture and Engineering

Jour 2
Domaine 4 : Communication and Network Security
Domaine 5 : Identity and Access Management (IAM)

Programme détaillé

Jour 3
Domaine 6 Security Assessment and Testing

Jour 4
Domaine 7 : Security Operations

Jour 5
Domaine 8: Software Development Security

Prix H.T	Stagiaires	Conditions	Durée	Langue
4 190 € Par personne	Groupe de 3 à 10 pers.	Présentiel ou Distanciel	35h sur 5 jours	Formateur Francophone

DEVENSYS CYBERSECURITY SAS, SIRET 790 746 952, enregistrée sous le numéro d'enregistrement d'activité 76-34-10238-34
Certifiée Qualiopi pour la catégorie : actions de formation [Certificat n°2200682].
Document non contractuel - version 1.0
Dernière version : Décembre 2024