Formation Préparation à la Certification CISSP (Information Systems Security Profesionnal)

La certification des professionnels de la Sécurité de l'information

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

La certification de référence CISSP® (Certified Information Systems Security Professional) est indépendante, pragmatique et internationalement reconnue. Créée et maintenue par des professionnels de la sécurité informatique en exercice, elle permet d'étalonner son niveau de compétence selon 3 axes : les connaissances techniques, les capacités d'analyse des risques et les aptitudes à l'audit des systèmes. La certification CISSP n'atteste pas seulement d'une bonne connaissance des technologies, elle démontre surtout une réelle capacité à les imbriquer et à les assembler pour répondre au mieux aux besoins des entreprises en matière de sécurité.
Cette formation prépare au test CISSP et entre en jeu dans le cursus de certification Certified Information Systems Security Professional (CISSP).

Référence	MGR211
Durée	5 jours (35h)
Tarif	3 850 €HT

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 17 au 21 juin 2024
du 19 au 23 août 2024
du 21 au 25 octobre 2024
du 9 au 13 décembre 2024

PARIS

du 17 au 21 juin 2024
du 19 au 23 août 2024
du 21 au 25 octobre 2024
du 9 au 13 décembre 2024

VOIR TOUTES LES DATES

Objectifs

| Connaître les thèmes, les domaines et rubriques du Common Body of Knowledge (CBK®)
| Maîtriser les fondamentaux de la sécurité des SI
| Se préparer à l'examen de certification CISSP

Public

| RSSI, DSI
| Consultants / Auditeurs
| Administrateurs Système et réseaux

Prérequis

| Justifier de cinq ans d'expérience professionnelle minimum dans au moins 2 des 8 domaines du CBK®

Programme de la formation

1 - Sécurité des informations et gestion des risques
| Les concepts de confidentialité, intégrité et disponibilité
| Les principes de gouvernance de la sécurité
| La conformité
| Les questions légales et réglementaires concernant la sécurité de l'information dans un contexte global
| L'éthique professionnelle
| La politique de sécurité, les standards, les procédures et les guidelines
| Les exigences de continuité d'activité
| Les politiques de sécurité du personnel
| Les concepts de management des risques
| Le modèle de menace
| Les considérations de risque de sécurité dans la stratégie d'acquisition
| La sensibilisation, la formation et l'éducation à la sécurité de l'information

2 - La sécurité des assets
| Classification de l'information et support des assets
| Le maintien de la propriété
| Protéger la confidentialité
| Assurer la rétention appropriée
| Les mesures de sécurité des données
| Les exigences de manipulation

3 - Ingénierie de la sécurité
| Les processus d'engineering et les principes de conception sécurisée
| Comprendre les concepts fondamentaux des modèles de sécurité
| Les mesures et contre-mesures
| Les possibilités de sécurités offertes par les systèmes d'information
| Les vulnérabilités de sécurité des architectures, des conceptions, des solutions
| Evaluer et réduire les vulnérabilités de sécurité des systèmes web, mobiles et des systèmes embarqués
| La cryptographie
| Les principes de sécurité au site et à la conception de l'installation
| La sécurité physique

4 - Sécurité des télécommunications et des réseaux
| Les principes de conception sécurisée à l'architectures réseau
| Sécuriser les composants réseau
| Concevoir et établir des canaux de communication sécurisés
| Prévenir ou limiter les attaques réseau

5 - La gestion des identités et des accès
| Contrôle d'accès physique et logique aux assets
| Gérer l'identification et l'authentification des personnes et des équipements
| L'identité en tant que service
| Les services d'identité tiers
| Les mécanismes d'autorisation
| Les attaques au contrôle d'accès
| Le cycle de vie des identités et du provisionnement des accès

6 - Évaluation de la sécurité et tests
| Les stratégies d'évaluation et de test de sécurité
| Tests de mesures de sécurité
| Les données des processus de sécurité
| Les résultats des tests
| Les audits internes ou third-party

7 - Continuité des opérations et plan de reprise
| Les investigations
| Les exigences des types d'investigations
| Les activités de monitoring et de logging
| Le provisionnement des ressources
| Les concepts fondamentaux de sécurité des opérations
| Les techniques de protection de ressources
| La gestion de incidents
| Opérer et maintenir des mesures de sécurité préventives
| La gestion des patchs et vulnérabilités
| Les processus de gestion des changements
| Les stratégies de reprise
| Les stratégies de reprise après sinistre
| Les plans de reprise après sinistre
| Le Plan de Continuité d'Activité
| La gestion de la sécurité physique
| Les problèmes de sécurité du personnel

8 - La sécurité du développement logiciel
| La sécurité dans le cycle de vie de développement logiciel
| Les mesures de sécurité dans les environnements de développement
| L'efficacité de la sécurité du logiciel
| Evaluer l'impact de la sécurité d'un logiciel acquis

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.