CISSP, sécurité des SI, préparation à la certification

Cours Pratique de 5 jours - 35h
Réf : CIS - Prix 2024 : 3 990CHF HT

Ce stage détaille les concepts de sécurité pour l'obtention de la certification CISSP. Il vous préparera au passage de l'examen en couvrant l'ensemble du Common Body of Knowledge (CBK), le tronc commun de connaissances en sécurité défini par l'International Information Systems Security Certification Consortium (ISC)².

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Connaître le Common Body of Knowledge de la sécurité IT

Développer une vision globale des enjeux de sécurité IT

Approfondir les connaissances des huit domaines du CISSP

Se préparer à l'examen de certification du CISSP

CERTIFICATION

Pour passer la certification, vous devez vous inscrire sur le site de l'ISC2 et déposer un dossier d'éligibilité.

LE PROGRAMME

dernière mise à jour : 09/2018

1) Sécurité du SI et le CBK de l'(ISC)²

- La sécurité des Systèmes d'Information.
- Le pourquoi de la certification CISSP.
- Présentation du périmètre couvert par le CBK.

2) Gestion de la sécurité et sécurité des opérations

- Pratiques de gestion de la sécurité. La rédaction de politiques, directives, procédures et standards en sécurité.
- Le programme de sensibilisation à la sécurité, pratiques de management, gestion des risques, etc.
- Sécurité des opérations : mesures préventives, de détection et correctives, rôles et responsabilités des acteurs.
- Les meilleures pratiques, la sécurité lors de l'embauche du personnel, etc.

3) Architecture, modèles de sécurité et contrôle d'accès

- Architecture et modèles de sécurité : architecture de système, modèles théoriques de sécurité de l'information.
- Les méthodes d'évaluation de systèmes, modes de sécurité opérationnels, etc.
- Systèmes et méthodologies de contrôle d'accès. Les catégories et types de contrôles d'accès.
- Accès aux données et aux systèmes, systèmes de prévention des intrusions (IPS) et de détection d'intrusions (IDS).
- Journaux d'audit, menaces et attaques reliés au contrôle des accès, etc.

4) Cryptographie et sécurité des développements

- Cryptographie. Les concepts, cryptographie symétrique et asymétrique.
- Les fonctions de hachage, infrastructure à clé publique, etc.

PARTICIPANTS

Responsables de la sécurité des SI ou toute autre personne jouant un rôle dans la politique de sécurité des SI.

PRÉREQUIS

Connaissances de base sur les réseaux et les systèmes d'exploitation ainsi qu'en sécurité de l'information. Connaissances de base des normes en audit et en continuité des affaires.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

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 pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• 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.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

- Sécurité des développements d'applications et de systèmes. Les bases de données, entrepôts de données.
- Le cycle de développement, programmation orientée objet, systèmes experts, intelligence artificielle, etc.

5) Sécurité des télécoms et des réseaux

- Sécurité des réseaux et télécoms. Les notions de base, modèle TCP/IP, équipements réseaux et de sécurité.
- Les protocoles de sécurité, les attaques sur les réseaux, sauvegardes des données, technologies sans fil, VPN...

6) Continuité des activités, loi, éthique et sécurité physique

- Continuité des opérations et plan de reprise en cas de désastre.
- Le plan de continuité des activités, le plan de rétablissement après sinistre.
- Les mesures d'urgence, programme de formation et de sensibilisation, communication de crise, exercices et tests.
- Loi, investigations et éthique : droit civil, criminel et administratif, propriété intellectuelle.
- Le cadre juridique en matière d'investigation, règles d'admissibilité des preuves, etc.
- La sécurité physique. Les menaces et vulnérabilités liées à l'environnement d'un lieu, périmètre de sécurité.
- Les exigences d'aménagement, surveillance des lieux, protection du personnel, etc.

LES DATES

CLASSE À DISTANCE
2024 : 10 juin, 17 juin, 02 sept., 14 oct., 16 déc.