Cyber sécurité, certification CISSP

Certified Information Systems Security Professional

Introduction

Cette formation s'adresse aux professionnels qui vivent et travaillent dans la sécurité de l'information et qui souhaitent être à l'avant-garde pour assurer la sécurité de leur entreprise. Elle prépare à l'examen de certification CISSP (Certified Information Systems Security Professional). Cette certification a été développée par l'ISC2 (International Information Systems Security Certification Consortium) pour valider les connaissances des experts en sécurité et pour assurer que leurs compétences restent à jour. Elle démontre que son titulaire possède les connaissances et compétences pour concevoir, développer, mettre en oeuvre et gérer un programme de sécurisation de l'information. Elle est une mesure objective de l'excellence dans le domaine.

La formation se base sur le programme défini par l'ISC dans l'ouvrage CBK (Common Body of Knowledge). Il représente les savoirs spécifiques que tous les professionnels du domaine de la sécurité ont en commun et qu'ils utilisent continuellement dans l'exercice de leur profession. La certification CISSP permet d'étalonner son niveau de compétences tant au niveau des connaissances techniques qu'au niveau de l'analyse des risques et de l'audit des systèmes dans une optique de gouvernance des systèmes d'informations.

Pour obtenir la certification CISSP, il faut :

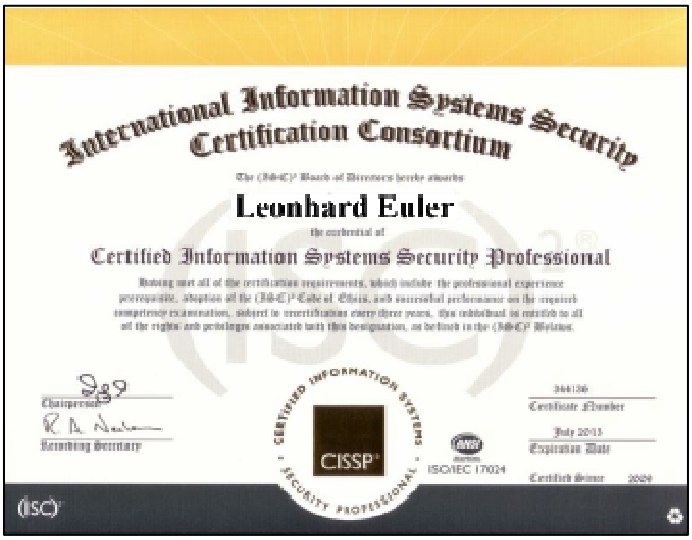
- réussir l'examen de certification
- faire valoir une expérience d'au moins 5 ans dans au moins 2 des 8 domaines présentés dans le CISSP CBK (Common Body of Knowledge) ou être titulaire d'un diplôme d'études supérieures d'une durée de 4 ans et faire valoir une expérience d'au moins 1 an dans au moins 2 des 8 domaines présentés dans le CISSP.

Le candidat qui ne répondrait pas à l'une de ces 2 conditions peut passer l'examen et sa réussite lui permettra d'obtenir la désignation Associate of (ISC) désignation. Il aura alors jusqu'à 6 ans pour faire valoir de l'expérience exigée pour obtenir la certification CISSP.

L'examen de certification, d'une durée de 3 heures, est en anglais. Il comprend 150 questions à choix multiple adaptatives, c'est-à-dire que les questions dépendent des questions et réponses précédentes. Il faut obtenir au moins 700 points sur 1000 pour le réussir. L'examen se déroule à l'ISEIG un jeudi à convenir. Sa préparation se fait sur la base d'examens à blanc à effectuer en dehors des heures de cours et discutés et corrigés dans le cadre du cours.

Pour qui

- professionnels qui vivent et travaillent dans la sécurité de l'information et qui souhaitent être à l'avant-garde pour assurer la sécurité de leur entreprise



Objectifs

- connaître le fonctionnement de la sécurité
- savoir gérer le contrôle des accès
- connaître les bases de la cryptographie
- connaître l'architecture et la conception de la sécurité
- savoir gérer la sécurité des télécommunications et des réseaux
- savoir gérer la sécurité des applications
- savoir concevoir, mettre en place et administrer la continuité de l'exploitation
- connaître le cadre légal et éthique
- savoir assurer la sécurité physique
- comprendre les modèles et architectures de la sécurité
- se préparer à l'examen de certification CISSP

Prérequis

- anglais technique écrit, la documentation pédagogique et les examens étant en anglais

Programme

- Domaine 1 : sécurité et management des risques
  - appliquer les principes de gouvernance de la séc.
  - comprendre et appliquer les concepts de confidentialité, intégrité , disponibilité et conformité

Suite au verso

- comprendre les questions légales et réglementaires concernant la sécurité de l'information dans un contexte global
- comprendre l'éthique professionnelle
- développer et implémenter une politique de sécurité, des standards, des procédures et des guidelines
- comprendre les exigences de continuité d'activité
- contribuer aux politiques de sécurité du personnel
- comprendre et appliquer les concepts de management des risques
- comprendre et appliquer le modèle de menace
- intégrer les considérations de risque de sécurité dans la stratégie d'acquisition
- établir et gérer la sensibilisation, la formation et l'éducation à la sécurité de l'information

- Domaine 2 : sécurité des actifs
  - classification de l'information et support des actifs
  - déterminer et maintenir la propriété
  - protéger la confidentialité
  - assurer la rétention appropriée
  - déterminer les mesures de sécurité des données
  - établir les exigences de manipulation
- Domaine 3 : ingénierie de la sécurité
  - implémenter et gérer les processus d'engineering en utilisant les principes de conception sécurisée
  - comprendre les concepts fondamentaux des modèles de sécurité
  - sélectionner les mesures et contre -mesures sur la base des modèles d'évaluation de la sécurité des systèmes
  - comprendre les possibilités de sécurités offertes par les systèmes d'information
  - évaluer et réduire les vulnérabilités de sécurité des architectures, des conceptions, des solutions
  - évaluer et réduire les vulnérabilités de sécurité des systèmes web
  - évaluer et réduire les vulnérabilités de sécurité des systèmes mobiles
  - évaluer et réduire les vulnérabilités de sécurité des systèmes embarqués
  - a ppliquer la cryptographie
  - appliquer les principes de sécurité au site et à la conception de l'installation
  - concevoir et implémenter la sécurité physique
- Domaine 4 : sécurité des réseaux et communications
  - appliquer les principes de conception sécurisée à l'architectures réseau
  - sécuriser les composants réseau
  - concevoir et établir des canaux de com. sécurisés
  - prévenir ou limiter les attaques réseau
- Domaine 5 : management des identités et des accès
  - contrôle d'accès physique et logique aux actifs
  - gérer l'identification et l'authentification des personnes et des équipements
  - intégrer l'identité en tant que service
  - intégrer des services d'identité tiers
  - intégrer et gérer les mécanismes d'autorisation
  - prévenir les attaques au contrôle d'accès
  - gérer le cycle de vie des identités et du provisioning des accès
- Domaine 6 : évaluation de la sécurité et test
  - concevoir et valider les stratégies d'évaluation et de test de sécurité
  - conduire des tests de mesures de sécurité
  - collecter les données des processus de sécurité
  - analyser et reporter les résultats des tests
  - conduire ou faciliter les audits internes ou externes
- Domaine 7 : sécurité des opérations
  - comprendre et supporter les investigations
  - comprendre les exigences des types d'investigations
  - réaliser les activités de monitoring et de logging
  - sécuriser le provisioning des ressources
  - c omprendre et appliquer les concepts fondamentaux de sécurité des opérations
  - utiliser les techniques de protection de ressources
  - gérer les incidents
  - opérer et maintenir des mesures de sécurité préventives
  - implémenter et supporter le management des patchs et vulnérabilités
  - c omprendre et participer aux processus de gestion des changements
  - implémenter des stratégies de reprise après sinistre
  - tester les plans de reprise après sinistre
  - participer au Plan de Continuité d'Activité et aux exercices
  - implémenter et manager la sécurité physique
  - sensibiliser le personnel aux problèmes de sécurité
- Domaine 8 : sécurité du développement logiciel
  - comprendre et appliquer la sécurité dans le cycle de vie de développement logiciel
  - appliquer les mesures de sécurité dans les environnements de développement
  - évaluer l'efficacité de la sécurité du logiciel
  - évaluer l'impact la sécurité du logiciel acquis
- Préparation à l'examen de certification

Durée, prix :

Formation	Jours	Prix	Prix/j
Cyber sécurité, certification CISSP - Certified Information Systems Security Prof.	5	2750'	

.