Certified Information Systems Security Professional – CISSP

Description

Allez plus loin dans vos connaissances relatives à la sécurité de l’information

Ce cours enseigne les concepts de sécurité de l’information et des meilleures pratiques de l’industrie, et couvre les huit domaines du CISSP officiel CBK (Common Body of Knowledge).
Vous acquerrez des connaissances en sécurité de l’information qui augmenteront votre capacité à implémenter et à gérer avec succès des programmes de sécurité dans n’importe quelle organisation ou entité gouvernementale.

Nous vous préparons à l’examen CISSP : Certified Information Systems Security Professional

Cette formation, en 5 jours vous prépare efficacement à l’examen CISSP (Certified Information System Security Professional). Ce cours abordera entre autres la sécurité et la gestion des risques, l’ingénierie de sécurité et l’évaluation de l’efficacité de la sécurité existante.

Contenu du cours
Module 1 : Sécurité et gestion des risques (p. Ex., Sécurité, risques, conformité, droit, réglementation, continuité des activités)

- Comprendre et appliquer les concepts de confidentialité, d'intégrité et de disponibilité
- Appliquer les principes de gouvernance de la sécurité
- Conformité
- Comprendre les questions juridiques et réglementaires qui se rapportent à la sécurité de l'informationdans un contexte mondial
- Élaborer et mettre en œuvre une politique de sécurité documentée, des normes, des procédures et des lignes directrices
- Comprendre les exigences de continuité des affaires
- Contribuer aux politiques de sécurité du personnel
- Comprendre et appliquer les concepts de gestion des risques
- Comprendre et appliquer la modélisation des menaces
- Intégrer les facteurs de risque de sécurité dans la stratégie et la pratique d'acquisition
- Établir et gérer l'éducation, la formation et la sensibilisation à la sécurité

Module 2 : Sécurité des biens (protection de la sécurité des biens)

- Classer les informations et soutenir les ressources
- Déterminer et maintenir la propriété
- Protéger la vie privée
- Assurer une rétention appropriée
- Déterminer les contrôles de sécurité des données
- Établir les exigences de manutention

Module 3 : Ingénierie de la sécurité (Ingénierie et gestion de la sécurité)

- Implémentation et gestion d'un cycle de vie d'ingénierie à l'aide des principes de conception de sécurité
- Comprendre les concepts fondamentaux des modèles de sécurité
- Sélectionner les contrôles et les contre-mesures en fonction des normes de sécurité des systèmes d'information
- Comprendre les capacités de sécurité des systèmes d'information
- Évaluer et atténuer les vulnérabilités des architectures de sécurité, des conceptions et des éléments de solution
- Évaluer et atténuer les vulnérabilités dans les systèmes Web
- Évaluer et atténuer les vulnérabilités dans les systèmes mobiles
- Évaluer et atténuer les vulnérabilités dans les dispositifs embarqués et les systèmes cyber-physiques
- Appliquer la cryptographie
- Appliquer des principes sécurisés à la conception du site et de l'installation
- Conception et implémentation de la sécurité des installations

Module 4 : Communications et sécurité réseau (Conception et protection de la sécurité réseau)

- Appliquer des principes de conception sécurisés à l'architecture de réseau
- Sécuriser les composants réseau
- Concevoir et établir des canaux de communication sécurisés
- Prévenir ou atténuer les attaques réseau

Module 5 : Gestion des identités et des accès (Contrôle de l'accès et gestion de l'identité)

- Contrôler l'accès physique et logique aux ressources
- Gérer l'identification et l'authentification des personnes et des périphériques
- Intégrer l'identité en tant que service (IDaaS)

- Intégrer les services d'identité tiers
- Implémenter et gérer les mécanismes d'autorisation
- Prévenir ou atténuer les attaques de contrôle d'accès
- Gérer le cycle de vie du provisionnement d'identité et d'accès

Module 6 : Évaluation et test de sécurité (Conception, exécution et analyse des tests de sécurité)

- Concevoir et valider des stratégies d'évaluation et de test
- Effectuer des tests de contrôle de sécurité
- Collecter les données du processus de sécurité
- Mener ou faciliter les vérifications internes et externes

Module 7 : Opérations de sécurité (par exemple, Concepts de base, enquêtes, gestion des incidents, reprise après sinistre)

- Comprendre et soutenir les enquêtes
- Comprendre les exigences pour les types d'enquête
- Diriger les activités d'exploitation forestière et de surveillance
- Sécuriser le provisionnement des ressources via la gestion de la configuration
- Comprendre et appliquer les concepts fondamentaux des opérations de sécurité
- Employer des techniques de protection des ressources
- Intervenir en cas d'incident
- Exploiter et maintenir les mesures préventives
- Implémenter et prendre en charge le correctif et la gestion des vulnérabilités
- Participer et comprendre les processus de gestion du changement
- Implémenter des stratégies de récupération
- Implémenter les processus de récupération après sinistre
- Tester les plans de catastrophe
- Participer à la planification de la continuité des activités
- Implémenter et gérer la sécurité physique
- Participer à la sécurité du personnel

Module 8 : Sécurité du développement logiciel (Comprendre, appliquer et appliquer la sécurité logicielle)

- Comprendre et appliquer la sécurité dans le cycle de vie du développement logiciel
- Appliquer les contrôles de sécurité dans l'environnement de développement
- Évaluer l'efficacité de la sécurité logicielle
- Évaluer la sécurité de l'acquisition de logiciels

Documentation

- Support de cours numérique inclus

Examen

- Ce cours prépare à la certification CISSP : Certified Information Systems Security Professional. Si vous souhaitez passer cet examen, merci de contacter notre secrétariat qui vous communiquera son prix et s’occupera de toutes les démarches administratives nécessaires pour vous

Profils des participants

- Toute personne dont la position nécessite une certification CISSP
- Les personnes qui souhaitent progresser dans leur carrière actuelle en sécurité informatique ou changer de poste

Connaissances Préalables

- Cinq ans d'expérience dans l'infrastructure informatique et la cybersécurité

Objectifs

- Sécurité et gestion des risques
- Sécurité des actifs
- Ingénierie de sécurité
- Communications et sécurité réseau
- Identité et gestion de l'accès
- Évaluation de la sécurité et tests
- Opérations de sécurité
- Sécurité du développement logiciel

Description
Formation Préparation à la Certification CISSP
Niveau
Avancé
Prix de l'inscription en Présentiel (CHF)
4900
Prix de l'inscription en Virtuel (CHF)
4650
Durée (Nombre de Jours)
5
Reference
ISC-CISSP