Date de publication : 02/05/2024

Formation : CISSO, Certified Information Systems Security Officer, certification MILE2

Formation pratique - 5j - 35h00 - Réf. CEF
Prix : 5010 CHF H.T.

4 / 5

Cette formation a pour but de préparer les candidats à l'examen du CISSO, la certification internationale délivrée par MILE2. La formation couvre l'ensemble des connaissances en sécurité de l'information réparties sur 19 domaines. Elle est alignée sur les objectifs des standards majeurs ISO 27001, NIST, CISM et CISSP.

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Acquérir les connaissances dans les 19 domaines du tronc commun nécessaires à la réussite des examens CISSO et CISSP
- Acquérir les connaissances pour conseiller une organisation sur les meilleures pratiques en management de la SSI

Public concerné

DSI, ingénieurs et chefs de projet, experts consultants sécurité, responsables sécurité, auditeurs.

Prérequis

Expérience dans le domaine des réseaux, des systèmes et de la sécurité. Compréhension de l'anglais technique.

Vérifiez que vous avez les prérequis nécessaires pour profiter pleinement de cette formation en faisant ce test.

Certification

Examen de certification en ligne sur le site de MILE2 (durée 2 heures/100 questions). Condition de réussite : au moins 70% de bonnes réponses.

PARTICIPANTS

DSI, ingénieurs et chefs de projet, experts consultants sécurité, responsables sécurité, auditeurs.

PRÉREQUIS

Expérience dans le domaine des réseaux, des systèmes et de la sécurité. Compréhension de l'anglais technique.

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.

Méthodes et moyens pédagogiques

Méthodes pédagogiques

Ensemble d'exposés couvrant chaque domaine du programme de l'examen. Ensemble de questions/réponses à la fin de chaque domaine. Support et animation en Français.

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.

Programme de la formation

1 Management des Risques et de la Sécurité, IAM et Contrôle d'Accès

- Risk Management : gestion des risques, évaluations et réponses.
- Security Management : SMSI, rôles et responsabilités, frameworks, ressources humaines.
- Identification and Authentication : identity Management, authentification, Access Control Monitoring.
- Access Control : types contrôles d'accès, information classification, modèles Contrôle d'Accès et méthodes.

2 Opérations de Sécurité et Cryptographie

- Security Models and Evaluation Criteria : mécanisme de protection, modèles de Sécurité.
- Operations Security : incidents et menaces opérationnels, responsabilités.
- Sym. Cryptography and Hashing : définition, historique, fondamentaux de cryptographie, algorithmes symétriques.
- Asym. Cryptography and PKI : crypto hybride et signature digitale, PKI, usages, attaques crypto.

3 Sécurité des Réseaux et Communications, Architecture de Sécurité

- Network connections : sécurité réseau et communication, topologies, transmissions réseaux, câblage, LAN/WAN.
- Network Protocols and Devices : modèle OSI, protocoles, ports & services.
- Telephony, VPNs and Wireless : téléphonie, VPNs, WiFi, attaques basées sur le réseau.
- Security Architecture and Attacks : modèles d'architecture, attaques systèmes.

4 Sécurité du Développement Logiciel, Sécurité des Bases de Données, Malwares

- Soft Development Security : processus de développement logiciel, sécurité Web, conformité PCI-DSS.
- DB Security and System Development : modèles et terminologies, sécurité base de données.
- Malware and Software Attacks : virus, Worm, Logic Bomb, Trojan Horse, Timing Attack, Spyware.

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 formations pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
- À l'issue de chaque formation 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 participant 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

Pour toute question ou besoin relatif à l'accessibilité, vous pouvez joindre notre équipe PSH par e-mail à l'adresse psh-accueil@orsys.fr.

5 BCP & DRP, Incidents de Sécurité, Lois et Ethique, Sécurité Physique

- BCP & DRP : BIA, stratégies, plan de développement, test.
- Incident Management, Law and Ethics : Computer Crime, gestion des preuves, éthique et confidentialité.
- Physical Security : locaux et construction bâtiments, protection périmétrique, menaces électricité et feu.

Examen
Passage de l'examen de certification CISSO.

Dates et lieux

CLASSE À DISTANCE
2026 : 18 mai, 12 oct., 16 nov.