CISSO, Certified Information Systems Security Officer, certification

★★★★★

PL-40 **5 Jours (35 Heures)**

Description

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.

À qui s'adresse cette formation ?

Pour qui

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

Prérequis

Aucune

Les objectifs de la formation

- 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

Programme de la formation

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.

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.

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.

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.

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.